جمهورية مصر العربية

معهد التخطيط القومي

سلسـلـة قضايـا التخطيـط والتنميـة

الأبعاد التنموية والاستراتيجية للأمن السيبرانى ودوره في دعم الاقتصادات الرقمية والمشفرة – مسارات التجربة المصرية فى ضوء التجارب العالمية

رقـم (٣٢٦) – أغسطس ٢٠٢١

جمهورية مصر العربية
معهد التخطيط القومي

سلسلة قضايا التخطيط والتنمية
رقم (326)

الأبعاد التنموية والاستراتيجية للأمن السيبرانى ودوره في دعم الاقتصادات الرقمية والمشفرة – مسارات التجربة المصرية في ضوء التجارب العالمية

2021

الأبعاد التنموية والاستراتيجية للأمن السيبرانى ودوره في دعم الاقتصادات الرقمية والمشفرة – مسارات التجربة المصرية في ضوء التجارب العالمية

جمهورية مصر العربية
معهد التخطيط القومي
الإدارة العامه للبحوث

رئيس المعهد
أ.د . علاء زهران

نائب رئيس المعهد
لشئون البحوث والدراسات العليا
أ.د . خالد عطية

خشبة، محمد ماجد وآخرون

الأبعاد التنموية والاستراتيجية للأمن السيبرانى ودوره في دعم الاقتصادات الرقمية والمشفرة – مسارات التجربة المصرية في ضوء التجارب العالمية،
سلسلة قضايا التخطيط والتنمية، القاهرة، معهد التخطيط القومي، 2021، 177 ص.

الكلمات الدالة: التكنولوجيات البازغة، المخاطر السيبرانية، الأمن السيبرانى، الإقتصادات الرقمية والمشفرة.

رقم الإيداع: 2020/13047
ISBN: 978-977-6641-58-7

مدينة نصر- طريق صلاح سالم-
القاهرة- جمهرية مصر العربية
https://inp.edu.eg
معهد التخطيط القومي
res.unit@inp.edu.eg
الهاتف/22627372-22634040 (202+)
الفاكس/22634747-24011398 (202+)

الطباعة والتنفيذ: معهد التخطيط القومي
الطبعة الاولى: 2021

تقديم

تعتبر سلسلة قضايا التخطيط والتنمية أحد القنوات الرئيسية لنشر نتاج معهد التخطيط القومى من دراسات وبحوث جماعية محكمة فى مختلف مجالات التخطيط والتنمية. يضم المعهد مجموعة من الباحثين والخبراء متنوعى ومتعددى التخصصات، مما يضيف إلى قيمة وفائدة مثل هذه الدراسات المختلفة التى يتم إجراؤها من حيث شمولية الأخذ فى الاعتبار الأبعاد الاقتصادية، الاجتماعية، البيئية، المؤسسية، والمعلوماتية وغيرها لأي من القضايا محل البحث.

تضمنت الإصدارات المختلفة لسلسلة قضايا التخطيط والتنمية منذ بدئها فى عام 1977 عدداً من الدراسات التى تناولت قضايا مختلفة تفيد الباحثين والدارسين، وكذا صانعى السياسات ومتخذى القرارات فى مختلف مجالات التخطيط والتنمية، منها على سبيل المثال لا الحصر: السياسات المالية والنقدية، الإنتاجية والأسعار والأجور، الاستهلاك والتجارة الداخلية، المالية العامة، التجارة الخارجية، التكتلات الدولية، قضايا التشغيل والبطالة وسوق العمل، التنمية الإقليمية والنمو الاحتوائي، آفاق وفرص الاستثمار، السياسات الصناعية، السياسات الزراعية والتنمية الريفية، المشروعات الصغيرة والمتوسطة، مناهج وأساليب النمذجة التخطيطية، قضايا البيئة والموارد الطبيعية، التنمية المجتمعية، قضايا التعليم والصحة والمرأة والشباب والأطفال وذوي الإعاقة، ...إلخ

تتنوع مصادر وقنوات النشر لدى المعهد إلى جانب سلسلة قضايا التخطيط والتنمية، والمتمثلة فى التقارير العلمية، والكتب المرجعية، المجلة المصرية للتنمية والتخطيط، والتى تصدر بصفة دورية نصف سنوية، وكذلك كتاب المؤتمر الدولى السنوي وسلسلة أوراق السياسات في التخطيط والتنمية المستدامة، وكراسات السياسات، إضافة إلى ما يصدره المعهد من نشرات علمية تعكس ما يعقده المعهد من فعاليات علمية متنوعة.

وفق الله الجميع للعمل لما فيه خير البلاد، والله من وراء القصد...

رئيس المعهد

أ . د . علاء زهران

موجز البحث

تهدف هذه الدراسة إلى التعرف على آليات وسبل التوظيف التنموى للأمن السيبرانى لدعم التنمية المستدامة واقتصاد المعرفة الرقمي الوطني والأمن القومي، بالإضافة إلى دعم التحول الرقمي وحماية الأصول الوطنية الرقمية.

ولم يأت الاهتمام بالأمن السيبرانى عالمياً ومحلياً من فراغ فقد أشار تقرير (إستشراف مستقبل المعرفة) إلى التكنولوجيات الأربعة الحاكمة فى تشكيل مستقبل البشرية على أنها : الذكاء الاصطناعي –AI، سلسلة الكتل – Block Chain، الأمن السيبرانى – Cyber security ثم التكنولوجيا الحيوية –Biotechnology، كما أشار المنتدى الاقتصادي العالمي WEF إلى أن عام 2020 يعتبر نقطة تحول فى الاهتمام العالمي بالأمن السيبرانى خاصة فى ضوء تزايد مستخدمي الإنترنت عالمياً (4.7 مليار نسمة فى يناير 2021)، وتصاعد الهجمات الإليكترونية، والتحول نحو الأخذ بأسباب الثورة الصناعية الرابعة فى دول العالم، وفى موازاة هذا الاهتمام العالمي ، تصاعد هذا الاهتمام عربياً من خلال مبادرات متعددة منها : تأسيس المركز العربي الإقليمي للأمن السيبرانى ARCC الذى بدأ نشاطه عام 2013 لتعزيز ممارسات الأمن السيبرانى فى المنطقة العربية بالتعاون مع الإتحاد الدولي للاتصالات – ITU.

وقد تنبهت الدولة المصرية مبكراً إلى أهمية (الأمن السيبرانى) فقامت بتأسيس المركز المصري للاستجابة للطوارئ المعلوماتية عام 2009، ثم المجلس الأعلى للأمن السيبرانى التابع لمجلس الوزراء عام 2015، واطلاق إستراتيجية وطنية للأمن السيبرانى (2017–2021)، كما تم عقد (المؤتمر الوطني الأول للأمن السيبرانى) في ديسمبر عام 2019.

وقد أكد وزير الإتصالات وتكنولوجيا المعلومات فى المؤتمر على أن الأمن السيبرانى يعتبر الركيزة الأساسية لبناء (إستراتيجية مصر الرقمية)، كما أنه ركيزة بناء الاقتصاد القائم على المعرفة فى مصر، كما نبه إلى أن توسع الرقمنة فى المجتمع والاقتصاد يزيد من مخاطر وتكلفة الهجمات الإليكترونية، وهو الأمر الذى يواجه مصر كغيرها من دول العالم.

وقد جاءت مصر فى المركز 23 عالمياً على مؤشر الأمن السيبرانى العالمي – GCI فى تقرير عام 2018، وحافظت على نفس الترتيب فى تقرير عام 2020 الصادر فى يونيو 2021، مقابل المركز 14 فى تقرير عام 2017.

وقد أشارت مسودة تحديث إستراتيجية التنمية المستدامة : رؤية مصر 2030 إلى الارتباط والتشابك بين (الأمن المعلوماتى / السيبرانى) وقضايا التحول نحو الاقتصاد الرقمي والاقتصاد القائم على

المعرفة وتطوير البنية التحتية الرقمية فى مصر، ويضيف إليها فريق البحث قضايا الاقتصاد المشفر بعد الاتجاهات العالمية للتوسع في استخدام العملات الرقمية والمشفرة.

فى إطار الاهتمام بالتطورات التكنولوجية الحاكمة، فقد قام مركز الأساليب التخطيطية بمبادرة من قسم الدراسات المستقبلية بإعداد دراسة علمية حول الذكاء الاصطناعي وسلسلة الكتل عام 2020، كما يتناول قضايا الأمن السيبرانى للعام الأكاديمي الحالي 2020 / 2021.

يتناول البحث قضايا الأمن السيبرانى في أبعادها التنموية المختلفة خاصة العلاقات الترابطية بين الأمن السيبرانى / الرقمي وتنمية الاقتصادات الرقمية والمشفرة والقائمة على المعرفة في مصر، كما يتناولها في سياقاتها المرتبطة بالتحول الرقمي في القطاعات الحكومية، وسياقات الأمن القومي والحروب السيبرانية التي تعتبر من أهم مهددات الأمن القومي في العقود القادمة، والتي يمكن أن تعصف بنتائج وثمار التنمية.

الكلمات الدالة: التكنولوجيات البازغة، المخاطر السيبرانية، الأمن السيبرانى، الاقتصادات الرقمية والمشفرة.

فريق البحث

م	فريق الدراسة	الاسم	الدرجة العلمية	التخصص
1	**الباحث الرئيسي**	أ.د. محمد ماجد خشبة	أستاذ متفرغ	إدارة أعمال
2	**البـــاحثون من داخل المعهد**	أ.د. أماني حلمى الريس	أستاذ	علوم حاسب
3		د. عصام محمد السيد احمدالجوهري	أستاذ مساعد	نظم معلومات
4		د. داليا أحمد على ابراهيم	مدرس	محاسبة
5		د. هبة جمال الدين محمد العزب	مدرس	علوم سياسية
6		د. حسن محمد ربيع حسن	مدرس	نظم معلومات
7		أ. آية ابراهيم محمد مليجى	معيدة	رياضيات بحتة وعلوم الحاسب
8	**البـــاحثون من خارج المعهد**	م. أحمد محمد يوسف الدسوقى	باحث– شركة خدماتي للدفع الإلكتروني	نظم معلومات
9		أ. أيمن سعد الدين	باحث– وزارة الإتصالات وتكنولوجيا المعلومات	نظم معلومات

المحتويات

قائمة الجداول

قائمة الأشكال

مقدمة

تشير العديد من التقارير والأدبيات العالمية إلى أن الأمن السيبرانى Cybersecurity وما يرتبط به من قضايا التهديدات السيبرانية للدول والمنظمات على السواء يظل مطلباً مطروحاً على قوائم الأولويات الرئيسية لدى معظم الدول والمنظمات فى العالم عام 2021 وما بعدها، وترافق هذا الاهتمام مع صعود تطبيقات موازية للتكنولوجيات البازغة مثل: تطبيقات الجيل الخامس 5G، تطبيقات الذكاء الاصطناعي AI، تطبيقات الحوسبة السحابية Cloud Computing، وهى التطبيقات التي يلازم توسعها تنامى أنواع متعددة من التهديدات السيبرانية.

وقد أشار تقرير المخاطر العالمية الأخير الصادر عام 2021 إلى أن فشل الأمن السيبرانى يأتى فى المرتبة الرابعة ضمن أبرز المخاطر التى تهدد العالم فى الآونة الراهنة وإلى أجل قريب، كما أشارت تقارير أخرى إلى خسائر فادحة تتعرض لها القطاعات المالية والصناعية والخدمية عبر العالم جراء الهجمات السيبرانية بأنواعها. وقد أشارت تلك التقارير إلى تكبد العالم لخسائر تصل إلى 5 تريليون دولار عام 2020 جراء تلك الهجمات، ويتوقع أن ترتفع إلى 6 تريليون دولار بنهاية عام 2021 خاصة مع التوسع فى التحول الرقمى.

وقد نبهت تلك المخاطر العديد من دول العالم– ومن بينها مصر– إلى التداعى لإتخاذ خطوات جدية للتعامل مع المهددات السيبرانية خاصة مع تنامى اتجاهات التحول نحو الاقتصادات الرقمية ورقمنة الخدمات العامة، كما أكدت ذلك نتائج أعمال المؤتمر الدولي للاقتصاد الرقمى والتنمية المستدامة بمعهد التخطيط القومى فى أبريل عام 2021، كما تنبهت الأمم المتحدة ووكالاتها المتخصصة إلى أن هذا النوع من المهددات السيبرانية يمكن أن يهدد أو يهدر جهود انجاز أهداف التنمية المستدامة العالمية، وأهداف التنمية المستدامة الوطنية فى العديد من دول العالم.

وقد انعكس الاهتمام العالمي بالمهددات السيبرانية والأمن السيبرانى فى مبادرات وجهود الأمم المتحدة والإتحاد الدولي للإتصالات ITU فى سياقات القمم العالمية لمجتمع المعلومات وبرامجها التنفيذية، وفى العديد من المبادرات العالمية والإقليمية، بما فيها الأوروبية والعربية والأفريقية، والهادفة إلى وضع أطر تعاونية عالمية وإقليمية لإستباق ورصد وتقييم ومواجهة المهددات السيبرانية وتعزيز الأمن السيبرانى العالمي والإقليمي، وتعزيز الثقة فى البنية التحتية الرقمية الوطنية.

وانعكس هذا الاهتمام العالمي والإقليمي بدوره على المستوى الوطنى / القطرى حيث تبنت العديد من دول العالم المتقدمة والناهضة والنامية، ومن بينها مصر، استراتيجيات وخطط وطنية للأمن السيبرانى تتفاوت فى مجالاتها ودوائر إهتمامها، لكنها تركز بالدرجة الأولى على حماية الاقتصادات

والخدمات وسلاسل القيمة الرقمية الصاعدة فى كافة دول العالم من المخاطر السيبرانية التى يمكن أن تهدر جهود التنمية فى تلك الدول، وفى هذا السياق برزت نماذج الإستراتيجيات السيبرانية للولايات المتحدة الأمريكية، والصين، والهند، وكوريا الجنوبية، والسعودية، ودولة الإمارات العربية المتحدة، بالإضافة إلى التجربة المصرية.

في ضوء ذلك، تهتم الدراسة بتسليط الأضواء على المفاهيم الرئيسية وذات الصلة بالأمن السيبرانى والمخاطر السيبرانية، كما تضع الاهتمام بالأمن السيبرانى فى سياقات صعود الاقتصادات الرقمية والتكنولوجيات البازغة عالمياً وإقليمياً وقطرياً، وتسلط أيضاً الأضواء على بعض الجهود العالمية والإقليمية التعاونية فى هذا الخصوص.

كما تتناول الدراسة بالتحليل بعض خبرات الاستراتيجيات والخطط الوطنية السيبرانية فى بعض التجارب العالمية والإقليمية، ومن بينها تجربة الولايات المتحدة الأمريكية، والصين، والهند وبعض التجارب العربية لإستخلاص أفضل الممارسات والخبرات المستفادة.

وتتناول الدراسة تفصيلاً ملامح التجربة المصرية فى التعامل مع قضايا الأمن السيبرانى، والمداخل الدستورية والتشريعية والتنظيمية والإجرائية ذات الصلة، كما تتناول بالتحليل الأدوار المؤسسية الحاكمة فى منظومة الأمن السيبرانى المصري بما فيها ريادات الأعمال فى تفاعلاتها الداخلية وعبر الحدود إقليمياً ودولياً، وتنتهى الدراسة بطرح خارطة طريق لتعزيز الأمن السيبرانى المصري فى ضوء الخبرات المستفادة من التجربة المصرية والخبرات العالمية والإقليمية على السواء.

1. أهمية البحث والفئات المستفيدة:

1.1. أهمية البحث:

تأتى أهمية البحث في ضوء ما يلى:

- تعاظم الاهتمام بقضايا الأمن السيبرانى وانعكاساتها على قضايا التنمية والأمن القومي في كافة دول العالم، وقد أشار مؤتمر ميونيخ للأمن 2020، ومؤتمر معهد التخطيط القومى حول الاقتصاد الرقمي فى أبريل 2021 إلى أن عدد الأجهزة المرتبطة بالإنترنت في العالم يصل إلى 20 مليار جهاز عام 2020 يتوقع أن تصل إلى 27 مليار جهاز بنهاية عام 2021، بما يعزز أهمية الأمن السيبرانى خاصة على عتبات تطبيقات الجيل الخامس.
- دور محوري للحكومات في التعامل الإستراتيجى مع قضايا الأمن السيبرانى، وأمن وحوكمة التكنولوجيات الجديدة البازغة، فالقضية أكبر من أن تترك للقطاع الخاص بمفرده.

- مراجعة وتقييم أدوار ومداخل تعظيم الاستفادة من (الأمن السيبرانى) في تعزيز الاقتصادات الرقمية والتنمية المستدامة من جهة، وتعزيز حصانة الدولة وأمنها القومي من جهة أخرى.
- دور المعهد، كبيت خبرة وطني ومركز للتفكير الاستراتيجي، في تشبيك الجهود والأطراف الوطنية المعنية بقضايا الأمن السيبرانى لدعم استدامة التنمية والأمن القومى.

1.2. الفئات المستهدفة من البحث:

- **المخطط ومتخذ القرار وصناع السياسات العامة** في مصر على مستويات تخطيطية واقتصادية وسياسية متعددة، ومنها: وزارة التخطيط والتنمية الاقتصادية، وزارة التعليم العالي والبحث العلمي، أكاديمية البحث العلمي والتكنولوجيا، البنوك والمؤسسات المالية، وغيرها.
- **التنظيمات المهنية للقطاع الخاص**، وتشمل الغرف التجارية، إتحاد الصناعات، إتحاد البنوك المصرية، جمعيات رجال الأعمال وجمعيات المستثمرين، جمعيات تكنولوجيا المعلومات
- البرلمان المصري ولجانه المعنية، والأحزاب السياسية، ومراكز الفكر ومنظمات المجتمع المدني المعنية بشئون التنمية العلمية على وجه الخصوص.
- **الباحثون في مجالات التنمية والتخطيط الاستراتيجي**، خاصة ما يرتبط بها من قضايا العلم والتكنولوجيا والاقتصادات الرقمية والمشفرة، وأنشطة البحوث والتطوير ذات الصلة.

2. أهداف البحث

تقديم سياسات وبدائل تدعم دور الأمن السيبرانى في تعزيز التنمية المستدامة ودعم جهود التحول الرقمي فى القطاع الحكومي وقطاعات الأعمال وفرص تطوير اقتصادات المعرفة، وتحسين حصانة الدولة والأمن القومي ضد المهددات السيبرانية بأنواعها في المستقبل المنظور من خلال:

- مراجعة وتقييم المفاهيم والتطبيقات والاتجاهات الراهنة والمستقبلية الخاصة بالأمن السيبرانى في بعض التجارب العالمية والإقليمية مقارنة بالتجربة المصرية.
- استشراف انعكاسات الأمن السيبرانى على تنمية اقتصادات المعرفة الرقمية والمشفرة في مصر
- استشراف انعكاسات الأمن السيبرانى على حالة ومهددات الأمن القومي في مصر.
- مراجعة وتقييم أدوار الحكومات، قطاعات الأعمال، والتجمعات والتنظيمات المهنية والأهلية المعنية، الجامعات ومراكز ومعاهد الفكر والبحوث.

3. منهجية البحث

- **المنهج الوصفي التحليلي** Descriptive Analytical Methodology: لإستعراض كافة الجوانب المتعلقة بالدراسة واستعراض الأدبيات والمعلومات ذات الصلة، واستخلاص النتائج التي تدعم أهداف الدراسة.
- **لقاءات الخبراء** Expert Panels من خلال ورشة عمل متخصصة مع الخبراء المعنيين بقضايا الأمن السيبرانى فى مصر **– (ملحق الدراسة).**
- **تحليل الاتجاهات** Trend Analysis.
- **تحليل السياسات** Policy Analysis.
- **دراسات الحالة المقارنة** Comparative Case-Study.

الفصل الأول

الأمن السيبرانى: المفاهيم الرئيسية والأهمية العالمية فى سياق الثورة الصناعية الرابعة والاقتصادات الرقمية والتنمية المستدامة

يشير التقرير الأخير حول الإتجاهات الرقمية فى العالم (Digital 2021) الصادر عن الإتحاد الدولي للإتصالات –والذى سنعرض له لاحقاً– إلى حقيقة توسع مساحات الرقمنة والتحولات الرقمية فى العالم؛ حيث تجاوز مستخدموا الإنترنت عتبة 4.7 مليار نسمة فى يناير 2021 ويمثلون حوالى 59.5 من سكان العالم (7.8 مليار نسمة)، كما أن 53% من سكان العالم يستخدمون مواقع التواصل الإجتماعي فى نفس التاريخ.

ويرتبط بهذا التوسع الرقمى الكبير والمتزايد العديد من القضايا وعلى رأسها قضايا تأمين الشبكات والأنظمة والأجهزة والبرمجيات من خلال نظم وخطط متكاملة للأمن السيبرانى على نحو يضمن كبح التهديدات السيبرانية لحياة البشر وللاقتصادات الرقمية الوطنية الصاعدة على حد سواء، خاصة وقد تجاوزت تكلفة الهجمات السيبرانية 5 تريليون دولار عام 2020 ويتوقع أن ترتفع إلى 6 تريليون عام 2021، وأن يتكبد العالم خسائر سيبرانية سنوية تصل إلى 10.5 تريليون دولار بحلول عام 2025 وفق تقرير حديث لمركز المعلومات ودعم اتخاذ القرار– سنتعرض له لاحقًا.

وفى ظل الحقائق السابقة لم تعد قضايا الأمن السيبرانى والتهديدات السيبرانية قضايا وطنية الطابع، بل تعولمت هذه القضايا فى ظل إدراك عالمى واقليمى متصاعد لخطورة المهددات السيبرانية على أمن الدول وحياة البشر وعلى جودة الحياة وفعالية الاقتصادات الرقمية، وإدراك جمعي عالمي بالحاجة إلى الجهود الجماعية العابرة للحدود للتعامل مع هذه المهددات.

يُلقى الفصل الحالي أضواء مفاهيمية مختصرة حول الأمن السيبرانى، كما يرصد بعض تطورات عالمية وإقليمية بارزة حول التعامل مع المهددات السيبرانية، وعلاقة الأمن السيبرانى بنمو الاقتصادات الرقمية والتحول الرقمى فى الإدارة العامة والخدمات العامة، وعلاقتها بتحقيق أهداف التنمية المستدامة العالمية SDGs، كم تصاعدت أهمية الأمن السيبرانى فى ظل جائحة كورونا COVID-19.

يعرض الفصل الحالي للقضايا السابقة على النحو التالى:

المبحث الأول: المفاهيم والملامح الرئيسية للأمن السيبرانى

المبحث الثاني: عولمة مهددات ومخاطر الأمن السيبراني – النظام العالمي والقطاع المالي

المبحث الثالث: مؤشرات الأمن السيبرانى والعلاقة مع الاقتصادات الرقمية والمشفرة

المبحث الأول

المفاهيم والملامح الرئيسية للأمن السيبرانى

يُلقى المبحث الحالي بعض الأضواء على مفاهيم وأبعاد أساسية للأمن السيبرانى، والتعرف على أنواع المهددات والمخاطر السيبرانية وأدوات التعامل معها.

أولاً: مفاهيم وأبعاد ومؤشرات الأمن السيبرانى والاقتصادات الرقمية والمشفرة

1. عن المفاهيم الرئيسية:

1.1. الأمن السيبرانى Cybersecurity

ويعرف بالنشاط أو العملية أو القدرة أو الحالة التي يتم بموجبها ومن خلالها حماية أنظمة المعلومات والإتصالات والمعلومات الواردة فيها، والدفاع عنها ضد الضرر أو الاستخدام غير المصرح به أو التعديل أو الاستغلال،[1] ويرى موقع (كسبارسكى – Kaspersky) أن الأمن السيبرانى يتضمن ستة مجموعات: [2]

- **أمن الشبكات Network Security**، فى مواجهة مخاطر هجمات متعمدة أو عابرة.
- **أمن التطبيقاتApplication Security**، لتحصين البرمجيات والأجهزة سيبرانياً.
- **أمن المعلومات Information Security**، ويرتبط بترتيبات ضمان سلامة وخصوصية البيانات فى التخزين والتداول.
- **الأمن العملياتي Operational Security**، وترتبط بقواعد حفظ وتداول البيانات
- **أمن التعافى وإستمرارية الأعمال Disaster Recovery and Business Continuity**، ويرتبط بتعزيز قدرات الجهات فى إدارة التعامل مع، والتعافى من الخطر السيبرانى.
- **أمن التعلم وتركيم الخبرات End User Education**، بما يعزز قدرات الأشخاص والمنظمات التى تعرضت للهجمات فى استباق وتجنب المخاطر السيبرانية.

---

[1] لمزيد من التفاصيل حول هذه المصطلحات، يراجع موقع المبادرة الوطنية لوظائف ودراسات الأمن السيبرانى: https://niccs.cisa.gov/

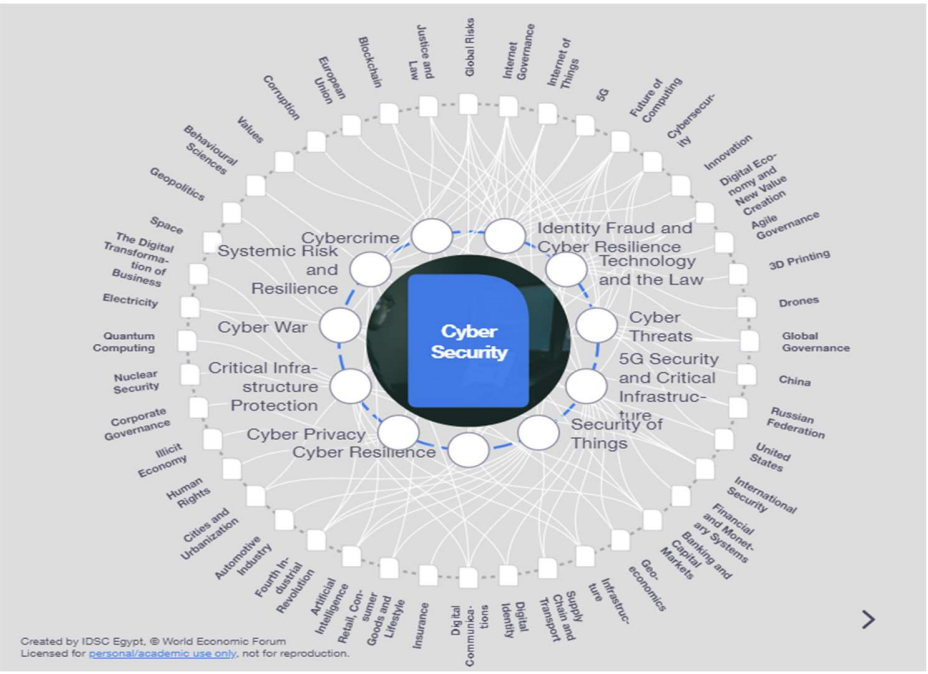
[2] Kaspersky (2021). What is cybersecurity.pp.1-5. www.kaspersky.com/

ويمكن أن يتسع نطاق التعريف ليشمل: الاستراتيجيات والسياسات والمعايير المتعلقة بأمن الفضاء الإلكتروني والعمليات فيه، ويشمل الأطر الكفيلة بالحد من التهديدات السيبرانية، والحد من الضعف السيبرانى، وتطوير آليات الردع السيبرانى، والمشاركة الدولية، والإستجابة للحوادث السيبرانية، والمرونة، وسياسات وأنشطة التعافي، بما في ذلك عمليات شبكة الكمبيوتر، وضمان المعلومات، وإنفاذ القانون، والدبلوماسية، والأنشطة العسكرية والإستخباراتية ذات الصلة من حيث صلتها بأمن واستقرار البنية التحتية العالمية للمعلومات والإتصالات. [1]

وفى هذا السياق الأوسع، يقدم المنتدى الاقتصادى العالمي رؤية شاملة للمحاور الرئيسية والفرعية المرتبطة بالأمن السيبرانى كما يوضحها الشكل رقم (1-1)، والذى يشير إلى المحاور المباشرة المرتبطة بالأمن السيبرانى وتشمل: الأطر التشريعية، الجرائم السيبرانية، المخاطر والمهددات السيبرانية، الحرب السيبرانية، البنية التحتية للحماية السيبرانية، الخصوصية والمرونة السيبرانية، أمن انترنت الأشياء، الأمن السيبرانى لتكنولوجيا الجيل الخامس 5G، وغيرها.

شكل (1-1)

المحاور المباشرة وغير المباشرة المرتبطة بالأمن السيبرانى



المصدر: موقع المنتدى الإقتصادى العالمى

-WEF. https://www.weforum.org/

[1] .Kaspersky (2021).,**Op.cit**.

1.2. لفضاء السيبرانى Cyberspace

ويعبر عن بيئة تفاعلية رقمية تتكون من عناصر مادية وغير مادية تشمل الأجهزة الرقمية، أنظمة الشبكات والبرمجيات، كما تشمل المستخدمين سواء مشغلين أو مستعملين.[1]

1.3. الهجمات السيبرانية Cyber Attacks

وتعرف على أنها كافة الأفعال التى يمكن أن تقوض من قدرات ووظائف شبكات الحاسبات لغرض شخصي أو أعمالي أو سياسي من خلال استغلال ثغرات أو جوانب ضعف معينة تتضمن التلاعب بالأنظمة.[2]

1.4. الجرائم السيبرانية Cybercrimes

تعبر عن الأفعال والتصرفات غير القانونية التى تتم من خلال معدات وأجهزة اليكترونية عبر شبكة الإنترنت وتتضمن قصد إحداث أضرار بأجهزة الحاسبات ونظم المعلومات يعاقب عليها القانون.

1.5. الردع السيبرانى Cyber Deterrence

وتشمل الإجراءات التى تهدف لمنع الأفعال الضارة بالأصول الوطنية فى الفضاء الرقمي.

1.6. الاقتصاد الرقمي Digital Economy

ويعبر عن النشاط الاقتصادي الذي ينتج عن مليارات الإتصالات اليومية عبر الإنترنت بين الأشخاص والشركات والأجهزة والبيانات والعمليات، حيث يعتبر الاتصال الفائق hyperconnectivity والمتواصل والمستمر هو العمود الفقرى للاقتصاد الرقمي، وهو الإتصال الذى يعبر عن زيادة وتوسع الترابط والتشبيك بين الأشخاص والمؤسسات والآلات الناتج عن الإنترنت وتكنولوجيا الهاتف المحمول وإنترنت الأشياء (IOT) وهى اتصالات وتفاعلات تتطلب أنواع جديدة من الحماية السيبرانية.[3]

ويقدم الاقتصاد الرقمى مفاهيم جديدة حول هياكل وعمليات وإدارة الأعمال والأنشطة الاقتصادية والتجارية، وآليات وأشكال التفاعل بين الأطراف المعنية سواء بين منظمات الأعمال بعضها البعض، أو فى علاقتها ببيئات الأعمال المحلية والخارجية، مع أدوار جديدة للآلات والنظم الذكية فى هذا التفاعل.

---

(1) شبكة هيكل ميديا المعرفية – هارفرد بزنس ريفيو (2021). المفاهيم الإدارية – الأمن السيبرانى.
- https://hbrarabic.com/

(2) المرجع السابق مباشرة.

(3) Damian Heath and Ludwicg Micallef (2021). What is digital economy – Unicorns, transformation and the internet of things. Malta: Deloitte.pp, 1- 2.

1.7. الاقتصـاد المشـفر Economy Crypto (اقتصـاد سلسـلة الكتـل Blockchain Economy)

ويعد الاقتصاد المشفر أو اقتصاد سلسلة الكتل أحد النتائج المنطقية لثورة العملات الرقمية المشفرة وخاصة البيتكوين، حيث تحل العملات الرقمية الأكثر شيوعاً وتطوراً محل الأنظمة النقدية التقليدية، فقد فتح دفتر الأستاذ الموزع غير القابل للتغيير في سلسلة الكتل مساراً شفافاً ومفهوماً لعملات رقمية جديدة وأصول مالية رقمية جديدة خاصة لو تم اعتمادها وحوكمتها من جانب الحكومات الوطنية وقطاعات الأعمال بحيث يكون هناك نوع من التتبع الرقمى الجديد والآمن للأصول المالية الرقمية دون غموض أو تستر.[1]

وقد أدى صعود وتوسع مثل هذه التطبيقات الرقمية المشفرة إلى تغيير مفاهيم الملكية والحيازة فى العالم والتى لم تعد تتمثل فى أموال أو أوراق مالية للعملاء أو صلاحية الحصول عليها، بل أصبحت حيازة أنواع مغايرة من الأصول المعقدة يطلق عليه (الأصول المشفرة – Assets Crypto) والمرتبطة فى الأغلب الأعم بنظام لسلسلة الكتل– Blockchain يجعل من ملكية هذه الأصول أو امكانية الوصول اليها مرتبط بمن يملك كود أو شفرة أو رمز دون الحاجة إلى وجود أية اثباتات أو سجلات ملكية أخرى كما هو الحال فى ملكية الأصول التقليدية. [2]

وقد أكدت عديد من المنظمات الدولية الصعود القادم لهذا النوع من التطبيقات المشفرة فى كافة مجالات الحياة ودعم التنمية المستدامة فى العالم، وفى هذا الصدد فقد أشار مؤتمر الأمم المتحدة للتجارة والتنمية UNCTAD، إلى إمكانيات واسعة لإستخدام تطبيقات البلوك تشين فى التأمين على المحاصيل، سلاسل توريد اللقاحات، جمع التبرعات، ودعم أنشطة وكالات الأمم المتحدة الأخرى مثل اليونيسف وغيرها.[3]

ولم يقتصر الاهتمام بالاقتصادات المشفرة على الدول المتقدمة، ولكن يتواصل هذا الاهتمام فى الدول النامية أيضاً، حيث ناقش المؤتمر الأخير (سلاسل الكتل فى أفريقيا Blockchain Africa) بمشاركة حوالى 40 دولة بجانب العديد من الشركات العالمية، مبادرات التحول الكبير فى الدول

---

(1) يراجع عن ذلك، وعن سلسلة الكتل وآفاقها العالمية وفى مصر:

-Techopedia (2021). Blockchain Economy://www.techopedia.com/definitio.

- محمد ماجد خشبة وآخرون –بحث جماعى (2020). "استشراف الآثار المتوقعة لبعض التطورات التكنولوجية على التنمية في مصر وبدائل سياسات التعامل معها - بالتطبيق على الذكاء الاصطناعي: AI - وسلسلة الكتل: Blockchain القاهرة: معهد التخطيط القومى. سلسلة قضايا التخطيط والتنمية رقم 315.ص ص: 5-75.

(2) بول كيروز (2020). التحديات التي تواجه قضية تنظيم الأصول المشفرة.

(3). UNCTAD (2021). Harnessing the promise of blockchain to change lives.

الأفريقية نحو توسيع تطبيقات سلسلة الكتل – البلوك تشين فى الأعمال خاصة: القطاعات المالية، التأمين، اللوجيستيات، الخدمات والمرافق العامة.[1]

2. أنواع المهددات السيبرانية وطرق التعامل معها:

2.1. نواع المهددات / الهجمات السيبرانية:

تتزايد الهجمات السيبرانية مع توسع الأعمال عن بعد التى تعتمد بصورة شاملة أو جزئية على التقنيات الرقمية، ويوضح الجدول التالى أبرز أنواع المهددات السيبرانية بما فى ذلك الخمسة أنواع الأبرز التى شهدها عام 2020.

جدول (1-1)

أنواع المهددات والهجمات السيبرانية

المهددات	إضاءات حول المهددات – الهجمات
الهندسة الاجتماعية Social Engineering	- جاءت ثلث الهجمات عام 2020 من خلال أدوات هندسة اجتماعية - 90% من الهجمات المذكورة تمت من خلال أداة التصيد – Phishing
هجمات الفدية Ransomware	- برامج لتشفير البيانات data-encrypting program، وطلب فدية لتحريرها - وصلت مبالغ الفدية المطلوبة عام 2020 إلى 1.4 مليار دولار، وتكلفة إصلاح الأضرار فى حدود 1.45 مليار دولار.
هجمات حجب الخدمات DDoS attacks	- تجاوز عددها فى النصف الأول من عام 2020 حوالى 4.8 مليون هجمة - يستخدم المهاجمون حالياً تقنيات الذكاء الإصطناعى AI فى هذه الهجمات
برامج الطرف الثالث Third party software	- تنتشر فى أنشطة التجزئة، بمهاجمة الطرف الخارجى الأضعف على سلاسل التوريد الخاصة بالعميل الرئيس، ومن خلاله يمكن مهاجمة الطرف الأصلى
هجمات الحوسبة السحابية Cloud computing vulnerabilities.	- يتنامى سوق السحابة عالمياً بمعدل 17% سنوياً، وقد وصل إلى 227.8 مليار دولار، مع زيادة فى استخداماته فى الاقتصاد تصل إلى 50%. - نفذ القراصنة أكثر من 7.5 مليون هجوم على حسابات سحابية، وزادت الهجمات بنسبة تصل إلى 250% مقارنة بعام 2019.

[1] وقد شارك فى المؤتمر خبراء من أمريكا الشمالية وأوروبا وآسيا واستراليا، يراجع:
- https://blockchainafrica.co/

المهددات	إضاءات حول المهددات – الهجمات
هجمات الوسيط Man in the Middle	- يتسلل المهاجم بين محاورين فى الشبكة دون علم كل منهم، ويعمل على اعتراض الإتصال الحقيقى من خلال اتصال آخر عبر جهازه.
حقن قواعد البيانات SQL Injection	- يعتمد على ارسال المهاجم جمل نصية لقواعد البيانات الرئيسية وصفحات المواقع المرتبطة بها.
المهاجم الداخلى Internal Attacker	- يعمل داخل المنظمة وبالتالى يعتبر أخطر من المهاجم الخارجى - يستخدم أدوات تصيد للتعرف على كلمات المرور ووسائل الحماية وغيرها.
هجمات كلمات المرور Password Attacks	- يعتمد على تخمين ومن ثم كسر وتغيير كلمات المرور لاستخدامها فيما بعد للدخول غير الشرعى أو غير المصرح به للنظم.
التعدين الخبيث Crypto jacking	- ويتم من خلال اختراق حاسوب أحد الأشخاص وتنزيل أحد البرامج الخبيثة عليه، ثم استغلاله لتعدين العملات الرقمية المشفرة.
التصيد Phishing	- وتعتمد على خداع المستخدم بتمويه ارسال برامج ضارة متخفية فى شكل مستند هام أو غيره، وتستغل للحصول على معلومات حساسة بمجرد فتحها.
البرامج الضارة Malware	- ومصممة لإلحاق الضرر بالأجهزة، أو الخوادم أو الشبكات على نحو يمكن المهاجم من التحكم فيها عن بعد.

Source: Juta Gurinaviciute (2021). "5 biggest cybersecurity threats – How hackers utilize remote work and human errors to steal corporat data". www.securitymagazine.com

المصدر: قيصر بهاء (2020). "أشهر الهجمات السيبرانية – آلية عملها وطرق تجنبها". بغداد: الفريق الوطنى للإستجابة للأحداث السيبرانية.

2.2. طرق وأدوات التعامل مع الهجمات السيبرانية

يُعد الأمان ضد البرامج والهجمات السيبرانية أحد أهم المشكلات التى يواجهها الأمن السيبرانى اليوم، وسيظل كذلك مع تطور البرامج الضارة، و تعمل حزم برامج مكافحة الفيروسات على مكافحة أي نشاط مشبوه، كما تتضمن هذه الحزم عادة أدوات تقوم بكل شيء بدءاً من التحذير من المواقع المشبوهة وحتى الإبلاغ عن رسائل البريد الإلكتروني التي قد تكون ضارة.

من جهة أخرى تعتبر الهواتف المحمولة (أكثر من 5 مليار مستخدم) أيضاً واحدة من أكثر الأجهزة المعرضة لخطر الهجمات السيبرانية، وبالتالي يوجد العديد من أدوات الأمن السيبرانى لحماية المعلومات والبيانات على هذه الأجهزة، كما توجد أدوات تقوم بغلق جميع استخدامات الهواتف المحمولة في حالة فقدانه، وكذلك توجد أدوات لمكافحة تطبيقات الأجهزة المحمولة التي تتطلب

الكثير من الامتيازات أو إدخال فيروسات أحصنة طروادة أو تسريب معلومات شخصية، حيث تعمل هذه الأدوات على التنبيه فى حالة الأنشطة المشبوهة أو تحظرها تماماً، كذلك فإن التوسع فى استخدام شبكة Wi-Fi العامة يزيد من خطر التعرض لمجموعة متنوعة من الهجمات الإلكترونية عبر الإنترنت، وللحماية من هذه الهجمات، يجب استخدام أحدث البرامج، وتجنب المواقع المحمية بكلمة مرور والتي تحتوي على معلومات شخصية.

ومن التطورات المستجدة فى مجال مواجهة هجمات الأمن السيبرانى استخدام الذكاء الاصطناعي لإحباط مجموعة واسعة من الجرائم الإلكترونية الخبيثة، حيث تقوم شركات الأمن بتطويع أدوات الذكاء الاصطناعي للتنبؤ بانتهاكات البيانات، والتنبيه لمحاولات التصيد في الوقت الفعلي وكشف عمليات الاحتيال في الهندسة الاجتماعية قبل أن تصبح خطيرة، ويلقى الجدول رقم (1-2) الأضواء على بعض الطرق والأدوات التى تستخدم فى مجال الأمن السيبرانى للدفاع عن الشبكات والأنظمة:

جدول (1-2)

بعض أدوات الحماية ضد الهجمات السيبرانية

الأدوات	إضاءات حول الأدوار والإستخدامات
أدوات الدفاع عن الشبكة	
نتستومبلر Netstumbler	- أداة مجانية مصممة للأنظمة التي تعمل على نظام التشغيل Windows فقط تستخدم لأغراض القيادة، وتمكن من تحديد نقاط الضعف في الشبكة.
ايركراك-أنجي Aircrack-ng	- أداة شاملة مناسبة لتعزيز أمن الشبكة وتحسينه، حيث يضم مجموعة شاملة من الأدوات المساعدة المستخدمة لتحليل نقاط الضعف في أمان شبكة Wi-Fi. - يستخدم لفحص حزم البيانات التي يتم توصيلها عبر شبكة للمراقبة المستمرة.
كيسماك KisMAC	- يستخدم لأمان الشبكة اللاسلكية في نظام التشغيل MAC OS X، - يقوم بالمسح الضوئى للشبكات اللاسلكية على بطاقات Wi-Fi المدعومة، ويستخدم تقنيات مختلفة لاختراق أمان مفاتيح WPA وWEP، حيث يعنى الاختراق الناجح أن المفاتيح ليست آمنة، وأن الشبكة عرضة للهجمات.
أدوات لفحص ثغرات الويب	
أن ماب Nmap	- يعرف باسم مخطط الشبكة، هو أداة أمان إلكتروني مجانية ومفتوحة المصدر تُستخدم لفحص الشبكات الكبيرة أو الصغيرة وأنظمة تكنولوجيا المعلومات لتحديد نقاط الضعف الأمنية الحالية.
نيكتو Nikto	- من أفضل أدوات الأمن السيبراني لاكتشاف الثغرات الأمنية على الويب، حيث

الأدوات	إضاءات حول الأدوار والإستخدامات
	يحتوي على قاعدة بيانات بها أكثر من 6400 نوع مختلف من التهديدات ويتم مقارنتها بنتائج فحص ثغرات الويب.
نكسبوز Nexpose	- تزود المتخصصين بعمليات في الوقت الفعلي لفحص الثغرات الأمنية وإدارتها في البنية التحتية المحلية. - يدعم اكتشاف نقاط الضعف المحتملة على النظام وتقليلها، وتقدير درجة مخاطر نقاط الضعف بحيث يتم ترتيبها وفقاً لمستويات الخطورة المتوقعة.
نيســـــوس بروفيشـــــنال Nessus Professional	- برنامج لتحسين تكامل الشبكة، ويتم استخدامه أيضًا في تصحيح الأخطاء مثل تطبيق تصحيحات الأمان الخاطئة، وغيرها. - يدعم اكتشاف الثغرات الأمنية وإدارتها بشكل مناسب، وتحديد الثغرات
بيـرب سـويت Burp Suite	- أداة تستخدم لإجراء عمليات مسح في الوقت الفعلي على الأنظمة، وتركز على اكتشاف نقاط الضعف الحرجة من خلال المحاكاة.

Source: Software Testing Help. (2020). Top 11 Most Powerful Cybersecurity Software Tools in 2021. pp.1-8 www.softwaretestinghelp.com/cybersecurity-software-tools.

المبحث الثاني

عولمة مهددات ومخاطر الأمن السيبرانى- النظام العالمي والقطاع المالي

كما سبقت الإشارة فإن الإمن السيبرانى فى ارتباطه بالتحولات الرقمية فى العالم لا تقتصر تأثيراته فقط على بعض القطاعات الحيوية وخاصة القطاعات المالية فى العالم، بل إن تأثيراته تطال قواعد وآليات عمل هيكل النظام العالمي ذاته، وهو الأمر الذى نلقى عليه الضوء فيما يلي.

أولاً: الأمن السيبرانى والنظام العالمي ومخاطر الأمن القومى:

جاءت ثورة المعلومات والتحولات الرقمية فى العالم لتتحدي الافتراض الأساسي للمدرسة الواقعية فى العلوم السياسية في أن الدول هي أقوى الجهات الفاعلة فى العلاقات الدولية والنظام العالمي والسياسة الدولية بوجه عام، فقد ظهرت مشاركات جديدة لجهات فاعلة غير حكومية، وقد شهد المجال السيبرانى تحولات هامة فى هذه الخصوصية حيث يمكن للمجرمين من الأفراد والمنظمات والجماعات الإرهابية الاستفادة من إمكانية الوصول إلى الإنترنت لتهديد هيمنة الدولة، نعرض فيما يلى لبعض قضايا الأمن السيبرانى فى علاقته بالنظام العالمي.

1. التحول الرقمى والأمن السيبرانى والتداعيات على النظام العالمي والسياسة الدولية

أنشغل علماء السياسة فى هذا السياق بالوقوف على ماهية الوحدات الفاعلة في ظل النظام العالمي الجديد الذي يحتل فيه مفهوم الأمن السيبراني ثقلاً جديداً على الصعيد الدولي. فهناك من اعتبر أن التحول الرقمي والأمن السيبراني له تأثير على الفاعلين العاملين بالنسق الدولي، وهناك من اعتبره محفزاً لظهور فاعلين جدد، وهناك من اعتبره ذاته فاعلاً في التنظيم الدولي. ويوضح الشكل التالى أبرز الوحدات الدولية التي تلعب دوراً في النظام الدولي بفعل الأمن السيبراني.

شكل (1-2)

أبرز الوحدات الدولية الفاعلة في النظام الدولي

Source: Anthony Craig and Brandon Valeriano, (2018). Realism and Cyber Conflict: Security in the Digital Age, Feb 3, 2018, pp.3-5. https://www.e-ir.info/2018/

ويوضح الشكل أن (التحول الرقمى Digital Transformation) أضحى قوة عالمية رئيسة[1] مفروضة على دول العالم ككل، ولها انعكاسات سياسية / اقتصادية واضحة مرتبطة بالمخاوف والتهديدات ذات الطابع السيبرانى ومنها: التجسس السيبرانى Cyber-espionage، التخريب السيبرانىCyber-sabotage، الإرهاب السيبرانى Cyber-terrorism، بالإضافة إلى التأثير السيبرانى المرتبط بنفوذ خارجي foreign influence Cyber [2].

ونظرت مراكز فكر عالمية كمركز "بلفر" وكلية "هارفارد كيندي" للأمن السيبرانى باعتباره طاقة إلكترونية عالمية تتطلب وجود إستراتيجية لتوطين الإنترنت وحماية المصالح التجارية والصناعية جنباً إلى جنب مع حماية الأمن القومي والصحة الإلكترونية للمواطنين، ومراجعة دور القوة الإلكترونية فى تعزيز ثقة الجمهور فى نظم الحكم[3].

وقد أختلف علماء السياسة حول تأثير الأمن السيبراني على سيادة الدولة، فيرى "دانيال لامباش" أن الفضاء السيبراني ساهم في تعزيز سيادة الدولة عبر دعم "السيادة الإلكترونية" أو "السيادة على البيانات"، أو ما يسمى بـ"السيادة الرقمية"، أي فرض السيادة الوطنية بالفضاء السيبراني، وتعنى السيادة الرقمية تشكيل مناطق ذات سيادة وطنية في الفضاء السيبراني، استنادًا إلى نظرية الممارسة والمفاهيم المزدوجة لإعادة التوطين وهو ما يُعرف بـ"الأنطولوجيا الإقليمية " عبر طرق ووسائل تمارِس من خلالها الجهات الفاعلة (الدول أو غير ذلك) السيطرة على الفضاء السيبراني، كقيام الحكومات بقطع الإنترنت في أوقات الأزمات السياسية، أو التحكم في التعليمات البرمجية والخوارزميات بتقنيات الذكاء الاصطناعي، أو فرض الرقابة الصارمة على المحتوى، وهو ما تفعله تركيا وتايلاند، إضافة إلى اللجوء للقرصنة الوطنية أو فرض قوانين "توطين البيانات" التي تحظر نقل البيانات عبر الحدود كالحالة الروسية والحالة الصينية، الأمر الذي يدعم إظهار قوة الدولة بشكل منتظم. وهناك العديد من الأدوات المتاحة للدول التي تسعى إلى إعادة إنشاء أراضيها الوطنية في الفضاء السيبراني، كحجب IP، والبحث عن الكلمات الرئيسية لمراقبة المناقشات حول الموضوعات الحساسة، ومنع الوصول إلى مواقع الويب التي تعتبر تخريبية. وهو ما تم تطبيقه في العديد من

---

[1] Borrett, Amy and Corbineau, Georges (2020). Cybersecurity rankings reveal leading global cyber powers, Techmoinitor, 27 Nov, pp.1-7. https://translate.google.com/

[2] وهي تهديدات تعززها التكنولوجيات البازغة وقدراتها المهددة للدولة والقطاع الخاص على السواء، وهو مادفع الحكومة الكندية لإعتبار الأمن السيبرانى جزء لا يتجزء من ضمان الرفاهية والإبتكار للدولة الكندية، يراجع:

- Canadian Security Intelligence Service-CSIS (2021). CSIS public report 2020.Canada: CSIS.pp.24-25.

[3] JuliaVoo.et.al. (2020). National Cyber power index 2020-Methodology and analytical considerations. USA: HARVARD Kenedy School.p.5-8.

الدول، كالجدار الناري العظيم في الصين، ونظم الرقابة الحكومية الصارمة على الإنترنت في كوريا الشمالية على سبيل المثال. [1]

وعلى الرغم من ذلك نجد هناك من اعتبر أن الأمن السيبراني يحمل في طياته تهديداً لسيادة الدولة، وبسط نفوذها بسبب عمليات الاختراق والهجمات السيبرانية؛ كهجمات وسطاء الظل والثغرات الإلكترونية، واسعة المدى التي تتعدي حدود الدول. [2]

2. <u>الأهداف السيبرانية الوطنية فى عالم متحول ومتغير رقمياً وسياسياً</u>

قدم مركز "هارفرد بلفر" سبعة أهداف رئيسة كأهداف وطنية تتطلع الدول لتحقيقها لحماية أمنها السيبراني تمثل في بعضها خرقاً مباشراً لمواثيق حقوق الإنسان العالمية، بل وقد ترتقي إلى حد تهديد ركائز النظام والسلم الدولي فبدل أن تتسم بالرشادة لدعم السلم والأمن الدوليين أضحت تهدد السلم العالمي، وهذه الأهداف على النحو التالى: [3]

- **الهدف الأول: مسح ومراقبة المجموعات المحلية**، بقيام الدولة – لدواعى الأمن القومى- بالمراقبة الالكترونية لرصد واكتشاف وجمع المعلومات الاستخبارية عن التهديدات المحلية والجهات الفاعلة داخل حدودها.
- **الهدف الثاني: تقوية وتعزيز الدفاعات السيبرانية الوطنية**، بتعزيز الدولة لدفاعاتها الوطنية لحماية أصولها الرقمية الحكومية وغير الحكومية.
- **الهدف الثالث: التحكم في بيئة المعلومات ومعالجتها**، بتحكم الدول في المعلومات باستخدام الوسائل الإلكترونية في الداخل والخارج ومحاولة حماية خصوصية الإنترنت وحرية التعبير لمواطنيها.
- **الهدف الرابع: جمع المعلومات الاستخبارية من دول أخرى لحماية الأمن القومي**، من خلال قيام دولة ما بانتزاع أسرارًا وطنية من خصم أجنبي كالمعلومات السرية عن الاتفاقيات، والخطط العسكرية السرية وسرقة الملفات وغيرها.

---

[1] دانيال لامباش (2020) عرض هدير أبو زيد. السيادة الإلكترونية: اتجاهات تشكيل مناطق سيبرانية تحت سيطرة الدول والشركات.أبوظبى: مركز المستقبل للأبحاث والدراسات المتقدمة. صص1-2.

[2] فاطمة الزهراء عبد الفتاح (2017). قراصنة " الويندوز:" كيف كشفت هجمات "الفدية الخبيثة" ثغرات الأمن السيبراني، أبو ظبي: مركز المستقبل للأبحاث والدراسات المتقدمة. ص ص،1-3.

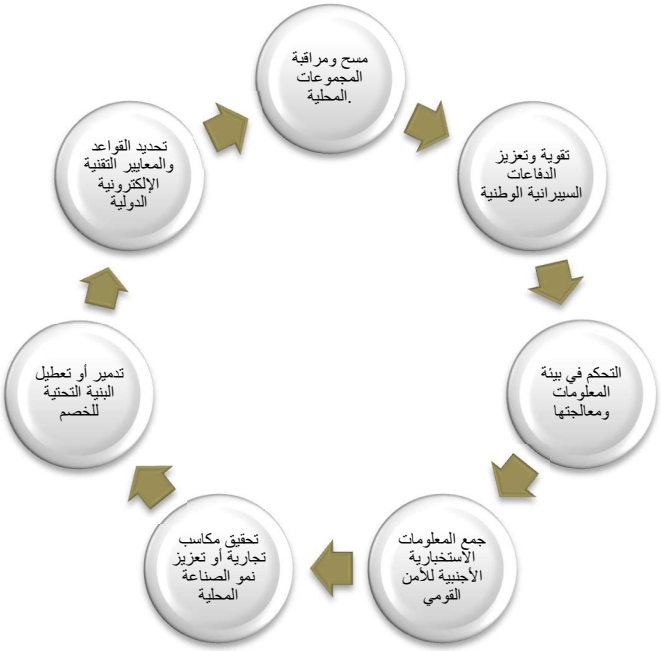
[3] Julia Voo. et.al. **Op. cit**. p.21.

- **الهدف الخامس: تحقيق مكاسب تجارية أو تعزيز نمو الصناعة المحلية؛** حيث يسخر النشاط السيبرانى لتنمية صناعة التكنولوجيا المحلية وتطوير صناعات محلية أخرى عبر وسائل مشروعة أو غير مشروعة كالتجسس الصناعي ضد الشركات الأجنبية.
- **الهدف السادس: السعى لتدمير أو تعطيل البنية التحتية للخصم وقدراته،** كاستخدام الدولة لتقنيات وتكتيكات إلكترونية مدمرة لردع أو إضعاف قدرة الخصم في المجالات الإلكترونية أو التقليدية كشكل من أشكال الدفاع الشرعي عن النفس.
- **الهدف السابع: تحديد القواعد والمعايير التقنية الإلكترونية الدولية،** من خلال مشاركة الدولة في المناقشات القانونية والسياسية والفنية الدولية حول المعايير الإلكترونية.

ويمكن اعتبار الهدف السابع أكثر الاهداف مثالية لدعم ركائز النظام العالمي ودعم السلم والأمن الدوليين، كما يوضح الشكل التالى الذى يعرض الأهداف السبعة.

شكل (1-3)

الأهداف السيبرانية للدول وفقاً للمؤشر العالمي للقوى السيبرانية الوطنية



source: Julia Voo.et.al. (2020), National Cyber Power Index 2020 Methodology and Considerations, USA: Harvard Kennedy School, p21.

ويتضح من الطرح السابق للمؤشر العالمي للقوى السيبرانية الوطنية أن بعض هذه الأهداف يمكن أن يعد مشروعاً، ومنها الذي يغلب عليه عدم المشروعية على نحو يهدد السلم والأمن الدوليين، من هنا

ينبغي التساؤل حول ما إذا كان من الممكن اعتبار هذه الأهداف بداية ردة على التنظيم الدولي الذي قامت مبادئه على عدم شرعية التدخل في الشأن الداخلي، وعدم التهديد باستخدام القوة، وعدم شرعية تهديد السلم والأمن الدوليين، فهذه الأهداف والمقومات تتسم بالتعدي على أمن وسيادة وخصوصية الدول الأخري والفاعلين الدوليين، كما إنها تمثل خرقاً للإعلان العالمي لحقوق الانسان الذي يكفل حماية الخصوصية الافراد.

3. خطورة وأبعاد أدوار الأطراف من غير الدول فى المشهد السيبرانى العالمي

تتنوع تصنيفات الفاعلين الدوليين بهذه الفئة ما بين وسطاء الظل، والجماعات الإرهابية، والأشخاص الاعتياديين علاوة على قوى غير دولية أقرب للكيانات الأممية كما يوضح الشكل التالى:

شكل (1-4)

تعدد الأطراف الضالعة فى الهجمات السيبرانية وتعدد دوافعها وأهدافها

A closer look at cyberattacks

The actors behind these incidents include not only increasingly daring criminals but also states and state-sponsored groups, with diverse goals and motivations.

THREAT ACTOR	MOTIVATIONS	GOALS	EXAMPLES
Nation-states, state-sponsored groups	Geopolitical, ideological	Disruption, destruction, damage, theft, espionage, financial gain	Permanent data corruption, targeted physical damage, power grid disruption, payment system disruption, fraudulent transfers, espionage
Cybercriminals	Enrichment	Theft/financial gain	Cash theft, fraudulent transfers, credential theft
Terrorist groups, hacktivists, insider threats	Ideological, discontent	Disruption	Leaks, defamation, distributed denial-of-service attacks

Source: European Systemic Risk Board. 2020. "Systemic Cyber Risk." https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

Source: Time Maurer and Arthur Nelson (2021). Cyber threats to the financial system are growing, and the global community must cooperate to protect it. Washington: (IMF-FD Magazine, Spring 2021).

أ. **وسطاء الظل:** ويقومون بشن هجمات سيبرانية عبر قوى من الفاعلين من غير الدول وتمارس ضغوط لقرصنة المعلومات الأمنية الرقمية واختراق نظم التأمين وأمن المعلومات، بما يتطلب تعزيز التعاون الاقليمي والدولي لمكافحة الجريمة الإلكترونية. [1]

ب. **قوى غير دولية أقرب للكيانات الأممية،** وهى أصغر في مقدراتها من الدول، وقد تكون أقرب إلى الكيانات الأممية، وعادة ما يكون لهولاء أهدافا تخريبية، إلا أن قدرتهم على القيام بعمليات واسعة النطاق تعوزها مساعدة أجهزة استخبارات دولية.

ت. **الأشخاص الاعتياديين،** وبعضهم قادر على أن يبدل من حال العالم، والمثال على ذلك ما رأيناه في ظاهرة ويكليكس Wikileaks، حيث استطاع مخترق للأمن المعلوماتي الأميركي أن يهدد أكبر دولة في العالم، وهى الولايات المتحدة الأمريكية. [2]

ث. **الجماعات الارهابية،** وتنشط فى سرقة المعلومات وتسهيل كل ما هو غير مشروع من عينة تجارة البشر والسلاح، مستغلين السوق السوداء على الشبكة الدولية، ويعتبر الإرهاب السيبراني تهديداً رئيسياً يواجه جميع الدول مع صعوبات فى تتبع الهجمات وتحديد هوية الجناة، وهناك جهود دولية جماعية لمواجهة هذه الهجمات، حيث يعمل المركز الأوروبي للجرائم السيبرانية (EC3) الذى تأسس عام 2013 كمحور مركزي للمعلومات والاستخبارات الجنائية "الإلكترونية" للدول الأعضاء في الإتحاد الأوروبي. [3]

ج. **الشركات متعددة الجنسيات،** سيدعم الأمن السيراني دور الشركات متعددة الجنسيات في النسق الدولي، حيث تستخدم الشركات برامج إدارة الحقوق الرقمية والتراخيص المحدودة وملفات تعريف الارتباط، ومتطلبات التسجيل لإنشاء حدود تسمح بجمع البيانات، ومراقبة المستخدمين، وتحقيق الدخل من الوصول إلى المحتوى الرقمي، كما يمكن أن تعمل فى بعض الأحيان على تحدي سلطة الدولة الوطنية عبر جمع المعلومات الرقمية للمستخدمين مما يهدد الخصوصية ويمس الامن القومي للدول. [4]

---

[1] فاطمة الزهراء عبد الفتاح، مرجع سبق ذكره، ص5.

[2] اميل أمين (2020). الأمن السيبراني العالمي - حروب خلفية ومساحات إرهابية: 5 قوى تهدد استقرار المجتمعات عبر شبكة الإنترنت وبتقنيات عالية جداً-https://www.independentarabia.com /

[3] وينشر المركز تقريراً سنوياً عن الجريمة المنظمة عبر الإنترنت:IOCTA ، والذي يعتبر مرجعاً هاماً للدول الأوروبية حول التهديدات السيبرانية وفق موقع المركز https://www.europol.europa.eu/

[4] دانيال لامباش، مرجع سابق مباشرة،.

ح. **وسائل التواصل الاجتماعي العالمية الكبرى،** أضحت وسائل التواصل الاجتماعي فاعلا رئيساً في النظام العالمي عبر ما تمتلكه من بيانات وقدرات؛ مثل "فيسبوك" و"جوجل" وتويتر" حيث تمتلك قدراً من المعلومات يوفر لها قدرات تفوق في واقع الحال قدرات بعض الدول، فمن خلال تلك المعلومات تستطيع اختراق الأسواق السيبرانية، بل وتوجيه المجتمعات والمزاحمة فى تشكيل الرأى العام العالمي والوطنى.[1]

من هنا يتضح أن الأمن السيبراني والتقدم التكنولوجي قد أثرا معاً على تحديد ماهية الوحدات الدولية الفاعلة بل أضحى نفسه فاعلاً على الساحة الدولية، وييسر لفاعلين قائمين بالفعل على زيادة فاعليتهم وقدراتهم لتحقيق أهدافهم بطرق مشروعة وغير مشروعة يمكن أن تؤثر بدورها على مقدرات وتوجهات السياسة الدولية.

4. <u>الأمن السيبرانى ومعضلات الحوكمة العالمية والإقليمية</u>

يمتد تأثير الهجمات السيبرانية على مسافات تتعدي الحدود الوطنية للدول، فعلى سبيل المثال لم يقف الهجوم السيبراني الذي تعرضت إليه الولايات المتحدة في 13 ديسمبر 2020 على حد الدولة ذاتها كمؤسسات فيدرالية وشركات عالمية، ولكنه امتد ليشمل مواطنين بدول أخرى حيث أعلنت شركة "مايكروسوفت" تضرر أكثر من 40 عميلاً لها من البرنامج الذي استعمله القراصنة، ويتواجد نحو 80% من هؤلاء العملاء في الولايات المتحدة بالإضافة إلى دول أخرى مثل: كندا والمكسيك وبلجيكا وإسبانيا والمملكة المتحدة وإسرائيل والإمارات، وتتوقع الشركة أن عدد الضحايا في الدول المتضررة سيواصل الارتفاع، الأمر الذي "يخلق هشاشة تكنولوجية خطيرة في الولايات المتحدة والعالم"، مما يؤكد أن الضربة تعدت حدود الهدف المبتغي من الهجمة السيبرانية التي تمت، خاصة أن الحالة المطروحة كانت قد تعرضت إلى القوة العظمي الأولي في العالم بدفاعتها السيبرانية القوية، ولكنها تغلبت عليها وتعدت حدودها لما هو أبعد من المستهدف. [2]

ويطرح هذا الهجوم السيبرانى وغيره من الهجمات السيبرانية العابرة للحدود قضية (الحوكمة العالمية للأمن السيبرانى والفضاء السيبرانى) الذى يتشكل فى حقيقة الأمر من مجموعة أقاليم غير حصرية ومتداخلة ومتقاطعة، مع محاولات متعددة للسيطرة عليها.

---

[1] اميل امين، مرجع سبق ذكره.

[2] أشار موقع فرنسا 24 – ديسمبر 2020، الى أن قائمة ضحايا الهجوم السيبرانى المذكور آخذة فى التوسع خارج حدود الولايات المتحدة، https://www.france24.com/ar، - متوفرة بتاريخ 19 يناير 2021

وينتج عن هذه المحاولات فى الأغلب (مناخ تنافسي) حيث تتجسد المعضلة الأمنية المتمثلة في محاولة كل دولة استخدام عدة وسائل لزيادة أمنها حتى لو تطلب الأمر تقويض أمن الأخرين المنافسين وبناء التحالفات المناسبة لتعزيز أمنها، وذلك في ظل افتقار المجال السيبراني للحوكمة المؤسسية العالمية الفعالة، مما يدفع الدول لزيادة التوتر الدولي وسباق تسلح متصارع وزيادة احتمالية سوء التقدير والصراع. [1]

من هنا، يمكنا القول أن المشهد السيبرانى العالمي يجسد حالة صراع وحالة حرب وفق نموذج (الكل ضد الكل)، وانتشار الفوضي، وعلى ذلك أصبح الأمن السيبراني مصدر قلق رئيسي لواضعي السياسات، ومصدر إهتمام كبير لعلماء العلاقات الدولية بسبب الخسائر المالية للشركات من خلال الجريمة الإلكترونية، أو سرقة البيانات الحكومية السرية، أو استهداف البنية التحتية الحيوية، حيث يشكل الأمن السيبراني تحديًا كبيرًا للأمن الاقتصادي والوطني للبلدان على مستوى العالم، كما يعتبر الفضاء الإلكتروني الآن المجال الخامس للحرب بعد الأرض والبحر والجو والفضاء. [2]

وفى سياق هذه الحالة من الصراع، تسعى الجماعة الدولية لمحاولة الاتفاق على قواعد منظمة لاستخدام الفضاء السيبراني، عبر طرح القضية في العديد من المحافل الدولية ومنها:

- **مؤتمر دافوس الاقتصادي لعام 2021**، حيث احتلت القضية صدارة أجندة المؤتمر [3]، والذى شخص التحديات السيبرانية العالمية فى خمسة تحديات: تحديات الرقمنة المتصاعدة والمعقدة، تشظّى وتعقد القواعد الحاكمة، تعدد وتداخل الأطراف على سلاسل الأعمال، نقص خبراء الأمن السيبرانى، وصعوبة تتبع والتحقق من المجرم / الفاعل السيبرانى.
- جهود للحوكمة السيبرانية فى قطاعات الأعمال –المنتدى الاقتصادى العالمي –2021: من خلال اقتراح ستة مبادىء لإدارة المخاطر السيبرانية لدى منظمات الأعمال. [4]
- **قمة ميونخ للأمن 2020**، والتي أكدت بالدرجة الأولى على أهمية الدور الذي تلعبه الحكومات في مجال الأمن السيبراني.

---

[1] Anthony Craig and Brandon Valeriano, Op. cit. pp.2-6.
[2] Ibid.pp,4-11.
[3] Look at :
-WEF (2021). These are the top cybersecurity challenges of 2021. https://www.weforum.org/agenda
[4] WEF (2021). Principles for board governance of cyber risk. Geneva. WEF. Insight Report., pp.1-13.

- **قمـة مجموعـة العشـرين – فبرايـر 2020**، وتوصـلت إلـى الحاجـة إلـى وجـود السياسـات الملائمة لتخفيف أثر الهجمات السيبرانية ومواجهة التحديات عبر سياسات منسجمة وموحدة تتضمن –أيضاً– المنشآت الصغيرة والمتوسطة التي تحتاج إلى مساعدة.[1]
- جهود الإتحاد الدولي للإتصالات، ونعرض جانب منها فيما بعد.

وتأتى هذه الجهود العالمية الجارية للتكامل مع جهود سابقة للمجتمع الدولي أسفرت من قبل على اتفاقية بودابست لمكافحة الجرائم المعلوماتية في 23 نوفمبر عام 2001. ورغم ذلك تظل الاشكالية قائمة في ظل غياب هوية الفاعل في الفضاء السيبراني، ويمكن أن تصبح إرادة الدول للالتزام ببنود أي اتفاق قد يوقع مستقبلا محل شك وتظل محاذير الفوضى حاضرة فى هذا الملف.

كما تظل القضية الحاضرة وبقوة هى علاقة ملف الأمن السيبرانى بملفات حقوق الإنسان فى العالم والتى كرسها الاعلان العالمي لحقوق الانسان سنة 1948 ثم العهدين الدوليين لحقوق الانسان سنة 1966. ومع ظهور الأمن السيبراني تثور عدة اشكاليات حول احترام الخصوصية وحقوق الانسان، حيث يظهر اتجاهين:

الاتجاه الأول: يعتبر قضايا الأمن السيبرانى تحمل في طياتها تهديداً لحقوق الانسان بفعل القدرات التي يوفرها الأمن السيبراني للدول وغيرها من الفاعلين من غير الدول، والتى يمكن أن تستخدم للجور على بعض هذه الحقوق.

الاتجاه الثاني: يعتبر الآليات السيبرانية مدخلاً لشن حركات مطالبة بتكريس حقوق الإنسان، والسعى لتحقيقها على أرض الواقع العالمي والإقليمي وفق مقررات الإعلان العالمي لحقوق الإنسان الذى غضت بعض الدول الطرف عنها، بل هى فرصة لنشر هذه الحقوق في العالم.

5. <u>الأمن السيبرانى والنظام العالمي – وماذا بعد ؟</u>

فى ظل التحديات السابق الإشارة اليها فإن فريق الدراسة والعديد من المعنيين بقضية الأمن السيبرانى يطرحون العديد من البدائل والإتجاهات، ومن بينها:

الاتجاه الأول: الأمن السيبراني مدخلا لزيادة سلطة الدولة على حساب حقوق الانسان:

حيث يدعو بعض الساسة إلى توسيع سلطة الأجهزة الأمنية على حساب حقوق الانسان داخل الدول لحماية الأمن القومي كدعوة بعض المسؤولين بالولايات المتحدة لزيادة سلطات وزارة الدفاع الامريكية لمراقبة الإنترنت على حساب بعض الحريات المدنية التي أقرها الاعلان العالمي لحقوق الانسان

---

[1] وأكد بيان وزراء الاقتصاد الرقمي للمجموعة على أهمية البنى التحتية الرقمية الآمنة القوية. يراجع نص البيان على موقع وزارة الإتصالات وتقنية المعلومات بالسعودية:https://www.mcit.gov.sa/

والمواثيق الدولية نظرا لطبيعة الهجمات الإلكترونية شديدة الخطورة. وفى هذا السياق تطلق تحذيرات حول إمكانية اختراق أنظمة الدفاع والبنية التحتية العامة وأنظمة الشركات والأنظمة الاقتصادية لإحداث الفوضى وإعاقة البلاد. [1] والجدير بالذكر أن هذا الاقتراح يأتي من الولايات المتحدة التي تعتبر نفسها حامية المبادئ الديموقراطية وحقوق الانسان بالعالم.

الاتجاه الثاني: آلية لدعم التعبير عن الراي والاحتجاج ودعم المثل العليا بالعالم:

تطرح الممارسة نماذج مختلفة لدعم المطالبات بحماية حقوق الانسان، فوجدت القوى الفاعلة من غير الدول الهجمات السيبرانية آلية للتعبير عن الرأي والاحتجاج بل ربما أداة للدفاع والمناصرة ودعم القيم المثلي في العالم. ففي 10 فبراير 2010 نفذت Anonymous هجمات في أستراليا أسقطت مواقع حكومية وبرلمانية احتجاجًا على التشريع الأسترالي المقترح للرقابة على الإنترنت، وبالمثل تورطت الجماعة في احتجاجات حزب الخضر على الانتخابات الإيرانية لعام 2009.

لم تتخذ Anonymous أي موقف سياسي، لكنها انضمت إلى المعركة لحماية سلامة المعلومات وحرية التعبير بعد أن أمر الرئيس أحمدي نجاد برقابة صارمة على مواقع التواصل لشل قدرة المحتجين على التنظيم، فوجدوا أبوابا خلفية مبرمجة ممثلة في جدران الحماية الإيرانية وإنشاء خوادم وكيلة حتى يتمكن الإيرانيون من التهرب من الحصار المجازي والوصول إلى مواقع مثل Gmail و Facebook ومنافذ الأخبار الغربية لتنظيم احتجاجاتهم وإيصال المعلومات إلى بقية العالم.

كما شاركت Anonymous نفسها في جدل WikiLeaks بدافع من الرغبة في حماية حرية التعبير، وقامت بعمل نسخة مطابقة لموقع WikiLeaks أكثر من 1241 مرة حتى لا يمكن إزالته من الإنترنت، كما لجأت المجموعة إلى الدفاع عن خوادم ويكيليكس من الهجمات الإلكترونية المستقبلية، كما أطلقت حملة انتقامية ضد الشركات التي قطعت علاقاتها التجارية مع ويكيليكس مثل أمازون وماستركارد، مما أدى إلى اضطرابات كبيرة في الخدمة، في حالة MasterCard كان الهجوم ناجحًا للغاية لدرجة أن مواقع شركة بطاقات الائتمان في جميع أنحاء العالم كان يتعذر الوصول إليها تمامًا لعدة ساعات وتعرضت العديد من الخوادم لأضرار بالغة.[2]

الإتجاه الثالث: مبدأ التعاون الدولي لإقرار السلم:

قدم علماء السياسة عدد من الأفكار مثلت امتدادا للجدل الدائر بين المدارس الفكرية المختلفة،

---

[1]Tim Maure, & Hannesebert, (2017). International Relations and Cyber Security: Carnegie Contribution to Oxford Bibliographies, Carnegie Endowment for International Peace, Oxford University Press, January 11, pp.1-10.

[2]Ibid.

ولكنهم اتفقوا في رغبتهم لتعزيز السلم والأمن الدوليين عبر تخفيف الهجمات السيبرانية، وتكاتف الجهود معا تعزيزاً لمبدأ التعاون الدولي في إقرار السلم والتنمية ومواجهة الكوارث، ولكن عبر طرح آليات جديدة قد تحتاج المنظمة الأممية للوقوف على ما تضمنته لتطوير ما أقرته بشأن هذا المبدئ.

الاتجاه الرابع: التعاون الدولي وتفعيل الدبلوماسية السيبرانية Cyber Diplomacy والدبلوماسية الرقمية Digital Diplomacy لتعزيز السلم فى الفضاء السيبراني:

أكد بعض علماء السياسية على أهمية التعاون وتنشيط أساليب التواصل الدبلوماسي السيبرانى والرقمي عبر العالم سواء بصورة جماعية أو ثنائية، وسواء أمميًا أو إقليميًا للتخفيف من تهديد الهجمات الإلكترونية، وتعزيز التوافق حول دور الاقتصادات الرقمية فى تعزيز فرص التعاون الدولي الإيجابي من خلالها مع درء المخاطر المرتبطة بها، وقد أشار "إريكسون" و"جيوكوميلو" فى هذا الخصوص إلى أن "الحكومة وحدها لا تستطيع تأمين الفضاء الإلكتروني"، وهنا تعتبر المدرسة النيوليبرالية في العلوم السياسية أنه يمكن حل هذه المعضلة الأمنية السيبرانية من خلال إنشاء مؤسسات دولية مؤلفة من دول وجهات فاعلة غير حكومية على حد سواء، مكرسة للحفاظ على الأمن السيبراني من شأنها أن تقلل إلى حد كبير من حالة عدم اليقين التي تواجهها حاليًا كل دولة. فمن الناحية النظرية، سيكشف كل عضو عن قدراته، ويقدم طرقًا للأعضاء لتحديد نشاطه السيبراني، ومشاركة التقنيات الدفاعية المطورة لتحقيق السلام والأمن[1] . ولكن ومن المحتمل أن تتجنب العديد من القوى الكبرى الانضمام حتى لا تكون مسؤولة عن أنشطة الحرب السيبرانية القائمة بالفعل.

ومن أبرز المجالات التي يمكن التعاون في خلالها:

- **إعطاء الأولوية للأمن السيبراني كقضية وطنية:** نظرا لحداثة فرع العلم وما يتضمنه من مخاطر وتهديدات الأمر يحتاج إلى وضع القضية بشكل أكبر على أجندة صناع القرار بالعالم للانتباه لها فقد أثبتت الجرائم الإلكترونية الشخصية " وجود نقاط ضعف حقيقية في الأنظمة الحكومية". [2]
- **القيام بمراجعات ايديولوجية على الصعيد الدولي كمدخل للتعامل مع الهجمات السيبرانية:** يعتبر بعض الكتاب (Constantine J. Petallides) أن التعامل مع هجوم الفاعلين من غير الدول عبر الساحة السيبرانية قد يكون عبر المراجعة الايديولوجية، فلا يمكن مواجهة مجهول أو هزيمته

---

[1]. Petallides Constantine J., "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat", Inquiries, 2012, VOL. 4 NO. 03, http://www.inquiriesjournal.com/articles/

[2]. Noah, Gamer (2015). The intersection of politics and cyber secure, September 28, https://blog.trendmicro.com/the-intersection-of-politics-and-cyber-security/, accessed on 07/02/2021.

بالوسائل التقليدية. بدلاً من ذلك، يجب على صانعي السياسة محاولة فهم مثل هذه الجماعات والتفاعل معها على مستويات أيديولوجية لتعزيز الأمن وتعزيز مجتمع عالمي أقوى، وهنا يمكن للمنظمة الأممية والدول كفاعل دولي رئيسي تقديم مراجعات فكرية للتعامل مع مشاكل سياسية واقتصادية ملحة فى بعض الأقاليم والدول الأكثر توترًا في العالم، بما يساهم في احتواء أو تحييد الجماعات الرافضة والمعارضة ليس فقط لسياسات الدول ولكن أيضا لنهج المنظمة الأممية ذاتها. (1)

- **تكوين شراكات فعالة بين القطاعين العام والخاص:** لا تقتصر مكافحة الجريمة الإلكترونية على تعاون الدول فقط، بل تتطلب أيضًا العمل بين الحكومات ومنظمات الأعمال لجسر الفجوات وازالة الحواجز أمام مشاركة معلومات الأمن السيبراني بين الحكومة والقطاع الخاص، وتعزيز أفضل الممارسات للقطاع الخاص، بما في ذلك معايير الأمن السيبراني الطوعية.
- **تعزيز وتوسيع تبادل وتقاسم أفضل للمعلومات:** توجد حواجز ضرورية بين الشركات الخاصة والحكومة، وكذلك بين الصناعات المختلفة. وفي هذا السياق صدر في عهد الرئيس الأمريكي الأسبق باراك أوباما أمرًا تنفيذيًا "لتشجيع تطوير مؤسسات تبادل المعلومات وتحليلها (ISAOs). " للعمل كمراكز لمشاركة معلومات الأمن السيبراني الهامة وتعزيز التعاون لتحليل هذه المعلومات داخل وعبر قطاعات الصناعة."
- **إصدار قانون رئيسي للأمن السيبراني:** يجمع بين التنسيق الحكومي والدولي والقطاع الخاص والشركات العابرة للقوميات العاملة في المجال.
- **إنشاء منصة للمواهب السيبرانية لاستقطاب الكوادر البشرية:** يمكنها تتبع مهارات الأفراد، وتحديد المرشحين الذين يمكنهم الانتقال جيدًا إلى أدوار الأمن السيبراني، وتوفير التدريب المناسب لتنمية القدرات وتعزيز فرص الوصول إلى منصات تخطيط القوى العاملة ومنصات التعلم ذات القدرات التحليلية للمهارات، ولديها القدرة على تقديم مزيج من المحتوى التعليمي الموصى به للشركات بهدف تحديد المواهب وبناءها داخليًا.(2)
- **حوكمة أفضل للبيانات على المستويين العالمي والوطنى لدعم التنمية المستدامة،** حيث تساهم البنية التحتية الرقمية الجيدة والآمنة والموثوقة للبيانات:شكل 1-5 فى تعزيز دورها كأداة للتغيير الاقتصادى والإجتماعى وضمان العدالة ومواجهة الفقر وتعزيز فرص التمكين والتنمية المستدامة

(1) Constantine J. Petallides, “, **Op.cit**.p4
(2) Joanne Cheng, **Op.Cit**.pp3-8.

من خلال تطوير عناصر النظام الإيكولوجى للبيانات [1].

شكل (1-5)

توجهات حوكمة البيانات لتعزيز فرص التنمية المستدامة وطنياً وعالمياً

المصدر: مجموعة البنك الدولي(2021). البيانات من أجل عالم أفضل – تقرير عن التنمية فى العالم 2021. واشنطن: البنك الدولي: ص11.

ثانياً: الأمن السيبرانى فى القطاعات المالية عالمياً وإقليمياً

مع تزايد أهمية استخدام التقنيات الحديثة يواجه النظام المالي العالمي ومؤسساته المالية المتعددة مخاطر جديدة بسبب التهديدات الإلكترونية والهجمات السيبرانية، ومع النمو الكبير الذي تشهده التقنيات والخدمات المرتبطة فإنه لا يمكن السير في الابتكار على حساب سلامة ومتانة المؤسسات المالية وتعطيل الخدمات المالية الضرورية للأنظمة المالية وكذلك على حساب حماية المستهلك[2]. نلقى الضوء فيما يلى على بعض جوانب الأمن السيبرانى فى القطاع المالي.

([1]) محمد ماجد خشبة وآخرون (2018). تقرير النظام الإيكولوجى للبيانات فى مصر لدعم التنمية المستدامة. القاهرة: صندوق الأمم المتحدة للسكان والجهاز المركزى للتعبئة العامة والإحصاء. ص 3-6.

[2] وقد خصص الصندوق قسماً خاصاً فى التقرير حول التهديدات السيبرانية وانعكاساتها السلبية على القطاعات المالية العربية. يراجع:

- صندوق النقد العربي (2020) تقرير الاستقرار المالي فى الدول العربية. أبو ظبي: صندوق النقد العربي. صص.206-235.

1. خصوصية القطاع المالي العالمي والمخاطر السيبرانية:

يعتبر القطاع المالي بشكل خاص من أكثر القطاعات تعرضاً لخطر الهجمات الإلكترونية، حيث تعتبر مؤسساته هدفا جذابا لهذه الهجمات نظرا لدورها الحيوي في الوساطة المالية. وأي هجمة إلكترونية ناجحة على مؤسسة ما يمكن أن تنتشر سريعا في كل النظام المالي الذي يتسم بدرجة عالية من الترابط. ولا يزال كثير من المؤسسات يستخدم نظماً قديمة قد لا توفر الحماية المطلوبة من الهجمات الإلكترونية. وإذا نجحت أي هجمة من هذا النوع، يمكن أن تكون العواقب كبيرة ومباشرة من خلال الخسائر المالية، ناهيك عن التكاليف غير المباشرة كالإضرار بالسمعة، كما يشير إلى ذلك أوراق على مدونة البنك الدولي.[1]

وتقدم دراسة أصدرها صندوق النقد الدولي مؤخراً إطاراً لتقدير الخسائر المحتملة من الهجمات الإلكترونية، مع التركيز على القطاع المالي، وتركز الدراسة على الربط بين الهجمات السيبرانية وإدارة مخاطر الإستقرار المالي، حيث أدى التوسع فى الرقمنة فى هذا القطاع إلى زيادة التركيز على المخاطر الإلكترونية، والتي أصبحت من وجهة نظر المديرون التنفيذيون فى القطاع المالي بين أهم ثلاثة مخاوف لديهم فى مؤسساتهم المالية.[2]

وتشير دراسة الصندوق المذكورة إلى مجموعة من الحقائق الهامة فى هذا الخصوص:

- **تصاعد وتيرة الهجمات السيبرانية عالمياً مع استهداف القطاع المالي**، خاصة مع تصاعد القدرات التكنولوجية لدى المهاجمين، كما يوضح الشكل التالى.

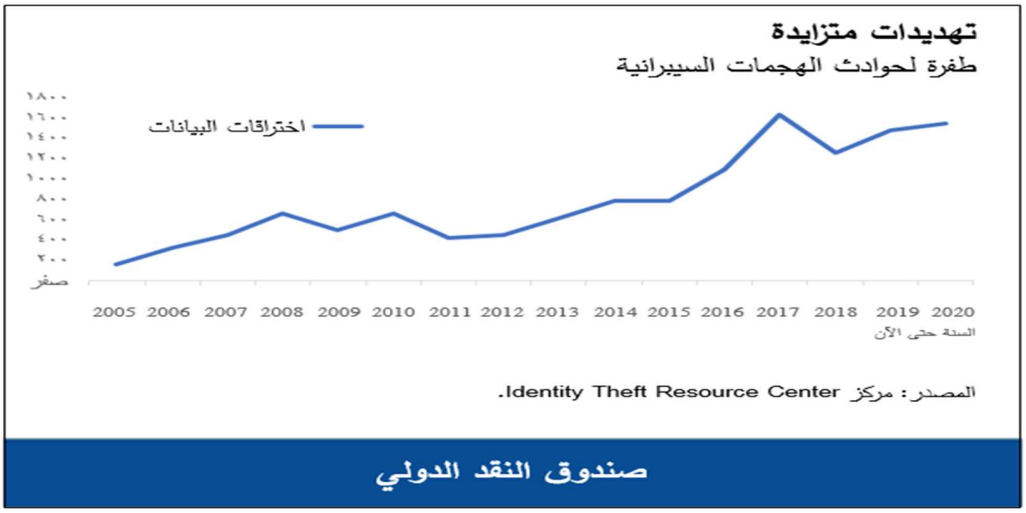
---

[1] Lagarde, C. (2018). Estimating cyber risk for the financial sector, IMF Blog, June. https://www.imf.org/ar/News/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector.

[2] IMF. (2020). Cyber Risk and Financial Stability: It's a Small World after AII.USA: IMF-(IMF Staff Discussion Note). pp.7-12.

شكل (1-6)

بيان التصاعد فى الهجمات السيبرانية بين عامى (2005-2020)



Source: Frank Adelman et.al. (2020). Cyber Risk and Financial Stability: It's a Small World After All. IMF Staff Discussion note. International Monetary Fund.p.7.

- **تعقد الهجمات وصعوبات الملاحقة**، خاصة مع تعدد قنوات التواصل والتعاون فى سوق الهجمات السيبرانية بين الأطراف المهاجمة (القراصنة) عبر العالم.
- **دوافع مالية وغير مالية للهجمات**، فكما سبق وأشرنا فإن بعض الهجمات قد تحركها دوافع جيوسياسية أو سياسية أو أيدولوجية.
- **الهجمات السيبرانية وتأثيرها السلبى على الإستقرار المالي**، حيث يمكن أن تؤدى لإهتزاز الثقة فى النظام المالي والمؤسسات المالية الوطنية أو الدولية.
- توقف أو انقطاع العمليات المالية وفقدان البيانات وتأثيراته السلبية على العملاء، حيث يؤدى أيضاً إلى اهتزاز ثقة العملاء فى القطاع المالي ومؤسساته.
- **التأثير على السيولة المالية عند اهتزاز الثقة**، كما يصعب على المؤسسات المالية إدارة الأزمة السيبرانية بكفاءة فى حالة فقدان الأصول أو صعوبة الوصول اليها.
- **تفاوت قدرات التعامل مع الأخطار السيبرانية فى القطاع المالي وجهود عالمية مبعثرة**، ويركز الصندوق على الحاجة لتوجيه إهتمام أكبر لتطوير قدرات منع واستباق الهجمات على القطاعات المالية، وسد الثغرات السيبرانية من جانب المؤسسات الوطنية، مع دور أكبر للمؤسسات المالية الدولية ومن بينها صندوق النقد الدولي لتعبئة الجهود العالمية فى هذا الصدد.

وفى ضوء ذلك، فإن هناك العديد من التحديات التى تواجه عمل المؤسسات المالية فى الفضاء السيبرانى، ومن أبرزها:[1]

أ. **التطور السريع في تقنية المعلومات** مع إعتماد متزايد عليها في العمليات المصرفية.

ب. **حداثة مفهوم الامن السيبراني** وضعف الثقافة السيبرانية فى المؤسسات المالية

ت. **وجود فجوات فى تطبيق ضوابط** أمن نظم المعلومات والفضاء السيبراني.

ث. الإرتفاع النسبي في تكلفة تطبيق تقنيات أمن المعلومات والفضاء السيبراني

وهنا تظهر الحاجة لطرف ثالث متخصص في تأمين نظم المعلومات للحد من عمليات القرصنة خاصة وأن الأخطار السيبرانية فى قطاع الخدمات المالية تأخذ صور مختلفة ومنها:

- **سرقة أو فقدان البيانات:** البيانات الشخصية والبيانات التجارية، وأي بيانات ذات قيمة بالسوق السوداء تعتبر خطر، وذلك بهدف تحقيق مكاسب مالية أو تنافسية.
- **تدمير البيانات:** مسح البيانات الالكترونية أو تشفيرها أو منع الوصول اليها.
- **انقطاع الإتصالات:** تعطيل الموقع الالكتروني أو تعطيل الشبكة؛ تشويه الموقع؛ الاستيلاء على صفحات وسائل التواصل الاجتماعي.
- **سرقة الأموال والأوراق المالية والصناديق وغيرها:** حيث تمتد الهجمات فى هذا النوع إلى ما وراء سرقة البيانات وهى سرقة المال والأوراق المالية والتى تعتبر هدفاً عالي القيمة سواء مادياً أو إلكترونياً.

2. نظرة عالمية حول تطور الهجمات السيبرانية فى القطاع المالي

تشير المسوح باستمرار إلى أن الهجمات الإلكترونية هي أكبر مصدر للقلق بالنسبة لمديري المخاطر وغيرهم من المسؤولين التنفيذيين في المؤسسات المالية. فوفقاً لتقديرات خبراء صندوق النقد الدولي، تواجه المؤسسات المالية على مستوى العالم خسائر محتملة من جراء الهجمات الالكترونية تتراوح بين 9% من صافى الدخل أو حوالي 100 مليار دولار أمريكي. وفي ظل السيناريو الحاد الذي يصل فيه تواتر الهجمات الإلكترونية إلى ضِعف ما كان عليه في السابق مع درجة أعلى من التمدد

[1] حسن، بهاء. 2020. الأمن السيبرانى للبنوك والمؤسسات المالية: التحديات وطرق المواجهة. عرض مقدم فى ندوة بعنوان " الأمن السيبرانى للبنوك والمؤسسات المالية". القاهرة: المنظمة العربية للتنمية الإدارية– جامعة الدول العربية، ص ص، 2–11

والإنتشار يمكن أن تتجاوز الخسائر هذا المقدار بنحو 2.5–3.5 ضِعفا، أو 270 إلى 350 مليار دولار أمريكي. [1]

وفى هذا الخصوص، قامت مؤسسة ديلويت العالمية بالتعاون مع مركز نشر وتحليل معلومات الخدمات المالية (FS-ISAC/ Deloitte 2020) بإجراء دراسة استطلاع رأى على مجموعة من المؤسسات المالية فى الدول المختلفة لدراسة اتجاهات المخاطر السيبرانية فى الخدمات المالية وكيف تتفاعل المؤسات المالية مع هذه المخاطر، وكذلك دراسة تأثير فيروس كورونا المستجد والتحول الرقمى على زيادة تسريع وتيرة الحاجه إلى الأمن السيبرانى فى المؤسسات المختلفة فى العديد من الدول. **وأسفر الاستبيان عن النتائج الرئيسية الآتية:**

- **زيادة الإنفاق على الأمن السيبرانى فى مختلف الخدمات المالية،** وتستحوذ إدارة الهوية والوصول، والمراقبة والعمليات السيبرانية، ونقاط النهاية وأمن الشبكة على النسبة الأكبر فى هذه الاستثمارات فى عام 2020. كما يوضح الشكل التالى.

شكل (1–7)

بيان الإنفاق على الأمن السيبرانى فى الخدمات المالية المختلفة

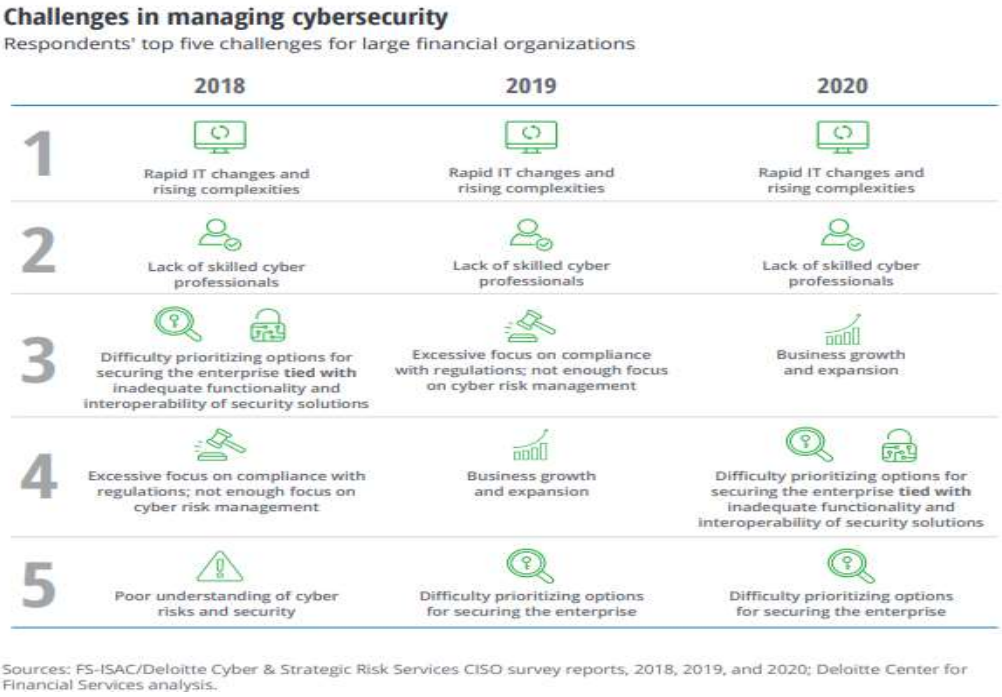
Source: Julie Bernard and Mark Nichloson. (2020). Reshaping the cybersecurity landscape: How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions. New York: Deloitte.p.3.

[1] Lagarde, C. (2018). Estimating cyber risk for the financial sector, IMF Blog, June. https://www.imf.org/ar/News/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector

- **التغيرات السريعة والمعقدة في تكنولوجيا المعلومات تمثل التحدي الأول للأمن السيبراني خاصة مع نقص المتخصصين**، وهو الأمر الذى يفرض على المؤسسات المالية العمل على تخفيف المخاطر السيبرانية الناشئة بشكل فعال من خلال تمكين الوظيفة السيبرانية مؤسسياً ضمن عملية تطوير خدمات تكنولوجيا المعلومات الأوسع فى المؤسسات المالية. ويوضح الشكل التالى أن هذا التوسع فى تكنولوجيا المعلومات بين 2018–2020 قد صاحبه نقص فى المتخصصين فى مجال الأمن السيبرانى فى المؤسسات المالية. كما يوضح الحاجة إلى التكامل الوظيفى والمؤسسى الوثيق بين تكنولوجيا المعلومات والأمن السيبرانى فى تلك المؤسسات.

شكل (1–8)

أهم التحديات فى إدارة الأمن السيبرانى فى المؤسسات المالية 2018–2020



Source: Julie Bernard and Mark Nichloson. (2020). Reshaping the cybersecurity landscape: How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions. New York: Deloitte.p.5.

- **أولويات هامة للمرحلة القادمة**، زيادة الإستثمار فى الجديد من التقنيات الناشئة مثل الحوسبة السحابيةCloud Computing، وتحليلات البيانات Data Analytics، وأتمتة العمليات الروبوتية، والاهتمام بالتكنولوجيات الوقائية الإستباقية وأمن البيانات.

وتشير دراسة حديثة لصندوق النقد الدولي إلى (التأمين ضد مخاطر الإنترنت) بإعتباره أحد الأدوات التى يمكن أن تلجأ اليها المؤسسات المالية لتحسين إدارة المخاطر السيبرانية والتخفيف من تداعياتها، حيث يتمثل دور التأمين في نقل المخاطر من المؤمن له وتجميع تلك المخاطر داخل شركة التأمين. وقد تأخر تبنى مثل هذه الحلول بسبب طبيعة المخاطر والفهم غير الناضج للمخاطر حاليًا، وقد قامت الرابطة الدولية لمشرفي التأمين بنشر ورقة قضايا حول المخاطر الإلكترونية (الرابطة الدولية لمشرفي التأمين 2016) وهي في طور إعداد ورقة تطبيق أيضًا (الرابطة الدولية لمشرفي التأمين 2018). [1] ورغم النمو الذي شهدته هذه السوق في الآونة الأخيرة، نجده لا يزال سوقا صغيرا حيث بلغت أقساط التأمين فيه حوالي 3 مليارات دولار على مستوى العالم في 2017. ومعظم المؤسسات المالية لا تملك تأمينا ضد المخاطر الإلكترونية أصلاً، كما أن التغطية محدودة وشركات التأمين تواجه تحديات في تقييم المخاطر نظرا لعدم اليقين بشأن التعرض للمخاطر الإلكترونية ونقص البيانات وآثار العدوى الممكنة.

3. جهود الحوكمة السيبرانية فى القطاعات المالية فى العالم

يعتبر تعزيز الأمن السيبراني في القطاع المالي من أولويات الإستقرار المالي، وكما سبقت الإشارة يُعد هذا القطاع هدفًا بارزًا في مجال التهديد السيبراني، وتشكل المخاطر السيبرانية تهديداً مباشراً لإستقرار الأنظمة المالية العالمية والوطنية خاصة فى ضوء إعتماد هذا القطاع المتزايد كما سبقت الإشارة على تكنولوجيا المعلومات والإتصالات (ICT)، حيث يمكن أن يؤدي الهجوم الإلكتروني إلى تعطيل توفير الوظائف الحيوية، وتهديد السيولة، وزعزعة استقرار وسلامة النظام المالي.

فى هذا الإطار اهتمت المنظمات والجهات التنظيمية والرقابية الكبرى فى العالم بدراسة أبعاد الأمن السيبرانى فى القطاع المالي وأصدرت فى ذلك تقارير ودراسات وإرشادات ومبادىء توجيهية.

3.1. المبادئ التوجيهية للمنظمات الدولية

3.1.1. وثيقة البنك الدولي - World Bank Digest 2020:

هى وثيقة تحتوى على ملخصات مجموعة حية ومحدثة بشكل دوري للقوانين واللوائح الحديثة والمبادئ التوجيهية وغيرها من الوثائق الهامة التى تصدرها الجهات والمنظمات الدولية حول الأمن السيبراني للقطاع المالي. [2]

---

[1] Christopher Wilson et.al. (2019). Cybersecurity Risk Supervision. USA: IMF-Monetary and Capital Markets Department. No. 19/15. pp.7-11.

[2] WB. 2020. Financial Sector's Cybersecurity: A Regulatory Digest.Washington: World Bank Group.pp.4-13.

3.1.2.وثيقة مجلس الإستقرار المالي - FSB 2020 [1]:

أصدر مجلس الإستقرار المالي (FSB) وثيقه استشارية حول الممارسات الفعالة للاستجابة للحوادث السيبرانية والتعافي منها بهدف بلورة مجموعة أدوات لمساعدة المنظمات في أنشطة CIRR الخاصة بهم. ويأتي هذا العمل بعد نشره لوائح الأمن السيبراني والتوجيه والممارسات الإشرافية في عام 2017 التى أعقبت قيامه بتقييم لوائح الأمن السيبراني للقطاع المالي والتوجيهات والممارسات الإشرافية، حيث خلصت النتائج إلى الحاجة إلى تعزيز الإتصالات بين السلطات والقطاع الخاص. لتسهيل التواصل الأكثر فعالية.

كما طور المجلس معجمًا إلكترونيًا في عام 2018 لدعم عمل المجلس وهيئات وضع المعايير، والسلطات والمشاركين من القطاع الخاص لمعالجة المرونة الإلكترونية للقطاع المالي.

ونظراً للترابط البينى لوحدات ومكونات القطاع المالي، وافق مجلس الإستقرار المالي في عام 2018 على تطوير مجموعة أدوات لتزويد المؤسسات المالية بمجموعة من الممارسات الفعالة للاستجابة للحوادث الإلكترنية والتعافي منه للحد من أي مخاطر تتعلق بالإستقرار المالي. كما أطلق المجلس فى يوليو 2019 مسحًا عبر الإنترنت لتطوير مجموعة أدوات للممارسات الفعالة المتعلقة باستجابة المؤسسات المالية للحوادث السيبرانة والتعافي منها.

3.1.3.بنك التسويات الدولية – BIS:

في ضوء زيادة حجم وتعقيد الهجمات السيبرانية وصعوبة تحديد تكاليفها، قام بنك التسويات الدولية Bank of International Settlement، باجراء دراسة تتناول تحليل لأكثر من 100.000 حدث إلكتروني عبر القطاعات لتوثيق خصائص الحوادث السيبرانية، وخلصت الدراسة إلى بعض خصائص الحوادث السيبرانية ومنها: [2]

- يتعرض القطاع المالي لعدد أكبر من الهجمات السيبرانية ولكنه يعاني من انخفاض التكاليف في المتوسط ، وذلك بفضل الاستثمار الأكبر نسبيًا في أمن تكنولوجيا المعلومات.

---

(1). FSB. (2020). Effective Practices for Cyber Incident Response and Recovery. Consultative Document. Financial Stability Board. Available online at: https://www.fsb.org/wp-content/uploads/P200420-1.pdf.

(2). Iñaki Aldasoro et al. (2020). Operational and cyber risks in the financial sector. Switzerland: BIS - Monetary and Economic Department Working Paper No. 840. pp.11-26. https://www.bis.org/publ/work840.pdf

- يرتبط استخدام الخدمات السحابية بانخفاض التكاليف على وجه الخصوص عندما تكون الحوادث الإلكترونية صغيرة نسبيًا.
- الأنشطة المتعلقة بالتشفير، والتي تعتبر غير منظمة إلى حد كبير تكون أكثر عرضة للهجمات الإلكترونية.

3.1.4.لجنة بازل للرقابة المصرفية [1]:

أصدرت تقريرًا عن الممارسات المختلفة للمرونة السيبرانية عام 2018، وتناولت الحوكمة السيبرانية فى البنوك فى بعض دول العالم، كما تناول مداخل إدارة المخاطر المصرفية السيبرانية والتنسيق والتعاون بين الشركاء فى هذا الخصوص، حيث خلص إلى مجموعة ملاحظات وتوجيهات للأطراف المعنية.

3-1. الخلاصات وأهم الخبرات المستفادة:

يقدم الجدول التالى تلخيصًا لجهود حوكمة الأمن السيبرانى من خلال المبادىء التوجيهية والإلزامية فى مجال الأمن السيبرانى فى القطاعات المالية لدى بعض المؤسسات والتكتلات الدولية المعنية والتى توضح الأهمية الكبيرة للحوكمة السيبرانية داخل هذه القطاعات التى تمثل عصب الأنشطة الاقتصادية والتجارية فى العالم.

جدول (3-1)

مبادىء توجيهية وإرشادية فى مجال الأمن السيبرانى فى القطاع المالي

الجهة	المبادىء التوجيهية
منظمة التعاون الاقتصادي والتنمية (OECD)	• تقترح منظمة التعاون الاقتصادي والتنمية أن تضع الدول الأعضاء إطارًا للمبادئ التوجيهية المتعلقة بالسياسات لإدارة الأمن السيبراني على المستويات المؤسسية. يجب أن تؤكد المبادئ التوجيهية على: 1. خلق الوعي بالمخاطر الإلكترونية وعواقبها، 2. تحديد الأطراف المسؤولة عن شبكات نظام المعلومات، 3. تحديد الفريق المسؤول للكشف عن التهديدات السيبرانية ومنع الحوادث، 4. ضمان المساءلة والأخلاقية ضمن معايير الأطراف المشاركة في إدارة الأمن السيبراني، 5. تطوير نظام أمني ضمن معايير الديمقراطية، 6. تطوير نظام شامل لتقييم المخاطر والتهديدات الأمنية سواء التقنية (ضعف النظام)

[1]Basel Committeeon Banking Supervision (2018). Cyber-resilience: Range of practices. Switzerland. BIS.pp.5-40.

الجهة	المبادىء التوجيهية
	وغير التقنية (العوامل البشرية والسياسة) 7. إعتماد "القلق الأمني" كمجال تركيز في جميع المجالات داخل المؤسسة، 8. تصميم نظام إدارة أمن شامل وديناميكي يتبنى نهج تقييم مخاطر استباقى إستشراف ى 9. إعادة تقييم وتعديل السياسات الأمنية جنبًا إلى جنب مع تطور التهديدات الأمنية
بنك التسويات الدولية (BIS)	• تقر اتفاقية بازل 2 مخاطر فقدان البيانات في الخدمات المصرفية القائمة على تكنولوجيا المعلومات ؛ وبالتالي ضرورة تواجد نظام يمكنه استباق وتخفيف المشكلة. • توضح اتفاقية بازل 3 مناهج إدارة المخاطر الإلكترونية من خلال مسئولية البنوك عن بناء وصيانة بنية البيانات والبنية التحتية لتكنولوجيا المعلومات لدعم قدرتها على جمع بيانات المخاطر وإعداد التقارير في الوقت المناسب • دور الإدارة العليا فى التأكد من أن إستراتيجية تكنولوجيا المعلومات تتضمن طرقًا لتحسين قدرات تجميع بيانات المخاطر وممارسات إعداد التقارير • مسئولية مجلس إدارة البنك عن الإبلاغ عن المخاطر المتعلقة بتكنولوجيا المعلومات
معهد الإستقرار المالي (FSI)	• من أجل تحسين الأمن السيبراني في المؤسسات المصرفية، يوصي باحثو FSI ببعض اعتبارات السياسة، مثل: 1. دمج مخاطر الأمن السيبراني في إطار نظام إدارة المخاطر على مستوى البنك، 2. تطوير إطار فعال للرقابة والإستجابة لإدارة مخاطر الأمن السيبراني في البنوك، 3. تعزيز الوعي بالأمن السيبراني بين موظفي البنك وأصحاب المصلحة الآخرين، 4. التعاون مع شركاء الصناعة ذوي الصلة لتعزيز نظام الأمن السيبراني الخاص، 5. ضمان التعاون عبر الحدود لتطوير نظام تنظيمي ورقابي متسق من أجل تعزيز المرونة الإلكترونية على مستوى البنوك.
صندوق النقد الدولي (IMF)	• بناء على بحث اجراه الصندوق عام 2018، فإن الإطار الفعال لتقييم المخاطر فى المؤسسات المالية يجب أن يتضمن عناصر المخاطر الرئيسية مثل: 1. مستوى التهديد الأمني ، 2. حالة ضعف النظام،

الجهة	المبادىء التوجيهية
	3. العواقب المالية لخرق أمني يمكن أن يؤثر على استقرار مؤسسة مالية. •إطار عمل تقييم المخاطر الثلاثى يمكن أن يمثل دليلاً لتوجيه المؤسسات المالية حول كيفية تحديد مستوى التعرض للمخاطر والعواقب المالية المترتبة على المؤسسة.
البنك الدولي(WB)	• يقترح البنك الدولي قيام البنوك المركزية الوطنية بجمع وتخزين معلومات عن الجرائم الإلكترونية من المؤسسات الخاضعة لولايتها. • تقوم المؤسسات بالإبلاغ عن جميع الحوادث الإلكترونية إلى البنوك المركزية الخاصة بها بمجرد أن تتمكن من اكتشافها. • يجب الإبلاغ عن المعلومات في شكل معين لرصد اتجاه الحوادث الإلكترونية داخل الدولة ومستوى المؤسسة. • تتفاعل المؤسسات المتأثرة على الفور لإعادة تقييم سياساتها الأمنية وتعديلها بما يتماشى مع التغييرات في متغيرات الأمن السيبراني
المنظمة الدولية لهيئات الأوراق الماليــة (IOSCO)	• يدرك مجلس إدارة المنظمة أن مخاطر الأمن السيبراني تشكل تهديدًا متزايدًا وهامًا لسلامة وكفاءة وسلامة الأسواق المالية العالمية. لذلك، 1. يجب تعيين منسق على مستوى مجلس الإدارة لضمان الاستخدام المتسق والفعال لموارد المنظمة الدولية لهيئات الأوراق المالية (IOSCO) وتوجيه المؤسسات المالية والمشاركين في السوق بشأن قضايا الأمن السيبراني. 2. توصي المنظمة بوجود إطار عمل منتظم ومستقل لإدارة مخاطر الأمن السيبراني لمعالجة السرقات الإلكترونية وخسائر البيانات الأخرى في المؤسسات المالية. **3.** تركيز إطار عمل إدارة المخاطر الإلكترونية على أولويات تحديد التهديدات، والحماية من المخاطر، واكتشاف ثغرات في النظام، والإستجابة للحوادث، وخطط التعافى

المصدر: مركب بمعرفة الفريق البحثى من مصادر متعددة بقائمة المراجع، ومصدر أساسى:

- Hamid Uddin et.al. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management (22):239–309. pp. 240-255.

4. حوكمة وإدارة المخاطر السيبرانية فى القطاع المالي العربي

أولى صندوق النقد العربي قضية الأمن السيبرانى فى القطاعات المالية العربية أهمية كبيرة فى الآونة الأخيرة، وقد تطرق العدد الرابع من سلسلة موجز السياسات للصندوق إلى قضية "**أمن الفضاء السيبراني في القطاع المصرفي**"، وأكد التقرير على مجموعة من الحقائق [1]:

[1] محمد اسماعيل (2019). الأمن السيبرانى في القطاع المصرفي. أبو ظبى، صندوق النقد العربي، موجز سياسات – العدد الرابع.ص ص. 1-8.

- **فرص وتحديات متعددة لتقنيات المعلومات فى القطاع المصرفى،** فمع الفرص المتعددة التى تخلقها تقنيات المعلومات والإتصالات فى هذا القطاع فإنها تولد تحديات ومخاطر جديدة، خاصة التقنية والإبتكارية منها، للمؤسسات المصرفية.
- **الاستخدام الضار لتقنية المعلومات والإتصالات يؤدي لتعطيل الخدمات المالية** الضرورية للأنظمة المالية الوطنية والدولية، وتقويض الأمن والثقة، وتعريض الإستقرار المالي للخطر.
- **الهجمات السيبرانية تشكل تهديدًا للنظام المالي بأكمله،** وهي حقيقة تؤكدها التقارير الصادرة في هذا الشأن على المستوى الدولي والإقليمي والمحلي، كما سبق وأشارت الدراسة.
- **المصارف المركزية العربية تواكب التوجهات العالمية فى التعامل مع المخاطر السيبرانية،** وفى هذا الصدد قامت المصارف المركزية العربية بإصدار التعليمات والتعاميم المصرفية التي تحث فيها البنوك على تعزيز قدراتها لمواجهة تلك الهجمات الإلكترونية.
- **آليات إستراتيجية لإدراج المخاطر السيبرانية ضمن مخاطر عمل المؤسسات المالية العربية،** حيث تلح الحاجة إلى وجود هيكل تنظيمي للتعامل مع الطبيعة الفريدة لتلك المخاطر، والعمل على تضمين الإستراتيجيات والسياسات الخاصة بالمصارف العربية جزء خاص بإدارة المخاطر السيبرانية، مع المراجعة المستمرة من قبل مجالس إدارات تلك المصارف مع زيادة حجم المخاطر السيبرانية وتنوع أشكالها وأدواتها.
- جوانب هامة تؤخذ فى الإعتبار لحوكمة إدارة المخاطر السيبرانية فى القطاعات المالية العربية
  - الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء السيبراني.
  - تنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت.
  - سرية وسلامة المعلومات، وطرق إثبات الهوية عبر الإنترنت.
  - الضوابط والتعليمات الرقابية الخاصة بإدارة كلمة السر (Password).
  - عمليات تحويل الأموال من خلال خدمات الإنترنت.
  - تأمين التطبيقات الإلكترونية في الخدمات والمعاملات البنكية من خلال شبكة الإنترنت.
  - توصيف وتحليل المخاطر المرتبطة بأمن نظم المعلومات والفضاء السيبراني.

- التعاون والتنسيق مع الأطراف المعنية بالأمن السيبرانى فى القطاع المالي عالميًا وإقليميًا، بالإضافة إلى الشركاء في صناعة تقنيات المعلومات.

وإدراك التزايد أهمية الأمن السيبراني في القطاع المالي والمصرفي ومواجهة التهديدات الإلكترونية في الدول العربية، والنمو الكبير والمتسارع الذي تشهده صناعة الأمن السيبراني والخدمات المرتبطة بها على مستوى العالم، تضمن الإستبيان الخاص بتقرير الإستقرار المالي في الدول العربية لعام 2020 لصندوق النقد العربي[1] فصلاً كاملاً يتعلق بالأمن السيبراني والتهديدات الإلكترونية وآثارها على الإستقرار المالي في الوطن العربي وإلقاء الضوء على أهمية الأمن السيبراني في القطاع المالي العربي ومؤسساته المصرفية والمالية المختلفة.

ومن أبرز النتائج التى توصل اليها الصندوق وتستحق التسجيل:

- **أهمية توافر إستراتيجيات وطنية للأمن السيبرانى،** والتى توفر مظلة لإستراتيجيات نوعية للأمن السيبرانى فى بعض القطاعات الهامة وعلى رأسها القطاعات المالية.
- **الأبعاد غير التقنية للأمن السيبرانى،** فلم تعد قضية الأمن السيبرانى قضية تكنولوجية / أو تقنية فقط لكنها تتضمن أبعاداً أخرى لا تقل أهمية مثل: ثقافة الأمن السيبرانى، نوعية الموارد البشرية اللازمة، الأبعاد السياسية للأمن السيبرانى وتأثيرات فجوات الأمن السيبرانى على الأمن الوطنى.
- **أهمية بناء القدرات،** نظراً لحداثة هذا النوع من المخاطر السيبرانية وارتباطه بالتطور والتوسع السريع فى تقنية المعلومات والإتصالات والتكنولوجيات البازغة مثل الذكاء الإصطناعى، الحوسبة السحابية، انترنت الأشياءوغيرها، والتى يستغلها المهاجمون، بما يتطلب تأهيل كوادر محترفة للتعامل مع تلك الأخطار وتطوراتها.
- **أهمية تبادل الخبرات والشراكات،** وذلك على مستويات متعددة، سواء على مستوى القطاع المالي الوطنى ذاته، أو القطاعات المالية الإقليمية والعالمية.

ويلقى الجدول (1-4) بعض الأضواء على مجموعة مختارة من العناصر التى تضمنها مسح الصندوق والتى توضح بعض جوانب الاهتمام بالأمن السيبرانى فى القطاعات المالية العربية، والتى تشمل البنوك، شركات التأمين والقطاعات المالية غير المصرفية.

[1] صندوق النقد العربي (2020). تقرير الاستقرار المالي في الدول العربية 2020، أبو ظبي: صندوق النقد العربي.ص ص،206، 237.

جدول (1-4)

أهم نتائج استبيان صندوق النقد العربي حول الأمن السيبرانى فى المؤسسات المالية العربية – مع الإشارة إلى موقف مصر

المحاور	نتائج إجمالية للمسح بخصوص كل محور	موقف مصر
التشريعات المتعلقة بالأمن السيبراني		
وجود تشريعات أو لوائح للأمن السيبراني بالمصرف المركزى لمراقبة المؤسسات المالية	• غالبية البنوك المركزية (13 دولة من 15) لديها نوع من التشريعات التنظيمية والإشرافية المتعلقة بالأمن السيبراني وإدارة المخاطر السيبرانية كجزء من مراقبة المؤسسات المصرفية المالية المرخصة.	قانون رقم 33 لسنة 88، ومجموعة ضوابط خاصة بالعمليات المصرفية، وأخرى بخصوص الأمن السيبراني، والأنترنت والهاتف النقال.
إدراج تشريعات الأمن السيبراني بمخاطر التشغيل والرقابة الداخلية.	• أشارت أغلبية الدول 17.4% إلى ادراج هذه التشريعات أو اللوائح ضمن إطار المخاطر التشغيلية والرقابة الداخلية • أدرجت السعودية وقطر وتونس تشريعات مستقلة للأمن السيبراني خارج المخاطر التشغيلية والرقابة الداخلية	✓
الجهة/الجهات المسؤولة في المصرف المركزي عن متابعة الأمن السيبراني في القطاع المالي	• غالبية البنوك المركزية تضع مسؤولية وضع سياسة الأمن السيبراني تحت مسئولية الجهات الرقابية (12 دولة) • بدائل أخرى: وحدات متخصصة كوحدة السياسة التنظيمية في البحرين –إدارة أمن المعلومات في قطر وعمان – وحدة الإستجابة للحوادث السيبرانية في الأردن والمسؤولة عن لأمن السيبراني في القطاع المصرفي.	تم إنشاء FinCIRT-EG لمراقبة الأمن السيبراني في القطاع المالي.
عناصر تشملها تشريعات المصرف المركزي المتعلقة بالأمن السيبراني	• التدريب ودور الإدارة العليا وعمليات خرق الأمن وإستمرارية العمل واختبار الخرق لمواكبة التطورات الخاصة بالتكنولوجيا المالية.	• التدريب • دور مجلس الإدارة والإدارة العليا السيبرانى • عمليات خرق الأمن

المحاور	نتائج إجمالية للمسح بخصوص كل محور	موقف مصر
	• المخاطر التشغيلية (مخاطر بنظم المعلومات والتهديدات الإلكترونية ومعايير ضمان أمن المعلومات المصرفية، وتعليمات خاصة للمخاطر السيبرانية.	وإستمرارية العمل • اختبار الإختراق
تحديد والإبلاغ عن التهديدات الإلكترونية		
جهة الإستجابة للحوادث الحاسوبية المالية	• لدى جميع الدول المشاركة ما عدا ليبيا والعراق جهة للاستجابة للحوادث الحاسوبية في القطاع المالي، وذلك لكافة حالات الإختراق.	مركز الإستجابة لطوارئ الحاسب الإلى للقطاع المصرفي
هجمات الأمن السيبراني وتعزيز القطاع المالي		
أكثر هجمات سيبرانية تشكل تهديد على القطاع المالي	• اختار 13 مصرف مركزي هجمات التصيد Phishingوالهندسة الإجتماعية فى الصدارة، تليها البرمجيات الخبيثة (9 مصارف مركزية) وهجمات حجب الخدمة (7 مصارف مركزية)	هجمات التصيد والهندسة الاجتماعية – وهجمات حجب الخدمة DDos
عوامل نجاح الأمن السيبراني بالمؤسسات المالية	• جاء توافر إستراتيجية فى المرتبة الأهم، • ثم الأفراد المتخصصين.	• الإستراتيجية • الإجراء • الأشخاص – التقنية
أهم ضوابط نظام الأمن السيبراني	• حوكمة الأمن السيبراني Cybersecurity Governance • تعزيز الأمن السيبراني (حماية الأنظمة والمعلومات) • صمود الأمن السيبرانى Cybersecurity Resilience • الخصوصة وأمن السحابة – Cloud Computing	• حوكمة الأمن السيبراني • تعزيز الأمن السيبراني • صمود الأمن السيبراني (الإستمرارية)
أهم تحديات يواجهها القطاع المالي في تعزيز الأمن السيبراني	• التطور السريع فى تقنية المعلومات وضعف القدرة على مواكبتها لتفعيل التصدى للهجمات والقرصنة الإلكترونية • ارتفاع تكلفة تطبيق تقنيات وضوابط أمن	

المحاور	نتائج إجمالية للمسح بخصوص كل محور	موقف مصر
	نظم المعلومات لضعف ثقافة الأمن السيبراني.	
الأمن السيبراني والإستقرار المالي		
مخاطر سيبرانية للإستقرار المالي	• مخاطر متعلقة بالأطراف الخارجية والحوسبة السحابية • مخاطر متعلقة بحماية البيانات والمعلومات.	لم تذكر

المصدر: مركب بمعرفة الفريق البحثى من:

- صندوق النقد العربي (2020). تقرير الإستقرار المالي فى الدول العربية 2020، أبو ظبى: صندوق النقد العربي، ص ص، 206، 237.

المبحث الثالث

مؤشرات الأمن السيبرانى والعلاقة مع الاقتصادات الرقمية والمشفرة

يعرض المبحث للمكونات الرئيسية لمؤشرات الأمن السيبرانى العالمية، ونتائج هذه المؤشرات على المستويين العالمي والإقليمي، كما يعرض لطبيعة العلاقة بين الأمن السيبرانى والاقتصادات الرقمية والمشفرة بإعتبارهما نواتج للثورة الصناعية الرابعة

أولاً: المؤشرات العالمية للأمن السيبرانى:

نعرض فيما يلى لدليل الأمن السيبرانى للإتحاد الدولي للإتصالات، والمؤشر الوطني للأمن السيبرانى

1. مؤشر الأمن السيبرانى للإتحاد الدولي للإتصالات – GCI:

طور الإتحاد مؤشر الأمن السيبرانى العالمي Global Cybersecurity Index: GCI ليقيس خمسة محاور رئيسة معنية بالأمن السيبرانى لدى دول العالم: [1]([2])

- **محور الأطر القانونية – Legal**، ويقيس مدى توافر مؤسسات قانونية تتعامل مع الأمن السيبرانى والجرائم السيبرانية.
- **محور القدرة الفنية – Technical**، ويقيس مدى توافر مؤسسات وأطر فنية للتعامل مع الأمن السيبرانى.
- **محور تنظيمى –Organizational**، ويقيس مدى توافر سياسات وإستراتيجيات على المستوى الوطنى لتنمية وتطوير الأمن السيبرانى.
- **محور بناء القدرات – Capacity Building**، ويقيس مدى توافر برامج للبحث والتطوير والتعليم والتدريب المرتبط بالأمن السيبرانى وتأهيل معتمد لمتخصصين من مؤسسات عامة.
- **محور التعاون – Cooperation**، ويقيس مدى توافر شراكات فعالة وأطر للتعاون وشبكات لتبادل المعلومات والخبرات ذات الصلة بالأمن السيبرانى.

ويقوم الإتحاد بترتيب الدول على المؤشرات الخمسة الرئيسية ومؤشراتها الفرعية المرتبطة بها إلى ثلاثة مجموعات أو مستويات من الدول:

- **مستوى مرتفع:** دول ذات أداء والتزام أكبر على المحاور الخمس الرئيسية للمؤشر
- **مستوى متوسط:** بلدان تبنت التزامات جيدة وبرامج وأنشطة للأمن السيبرانى

---

(1) للتفاصيل عن الإطار المفاهيمى للمؤشر والمنهجية الخاصة به، يراجع:
ITU (2018). Global Cybersecurity Index 2018.Geneva: ITU. Studies &Research.pp7-10.

- **مستوى منخفض:** بلدان بدأت فى الشروع فى اتخاذ إجراءات للأمن السيبرانى

ويوضح الجدول التالى رقم 1-5 موقف ترتيب الدول العشرة الأولى على المستويين العالمي والعربي وفق مؤشر الأمن السيبرانى العالمي لعامى 2018 – 2020 للإتحاد الدولى للإتصالات ITU.

جدول (1-5)

الدول المتصدرة عالمياً وعربياً على مؤشرى الأمن السيبرانى في عام 2018 وعام 2020

مؤشر الأمن السيبرانى عن عام 2018 (193 دولة)		مؤشر الأمن السيبرانى عن عام 2020 (193 دولة)	
الدول الأوائل عالميًا	الدول الأوائل عربيًا	الدول الأوائل عالميًا	الدول الأوائل عربيًا
بريطانيا	المملكة السعودية	الولايات المتحدة	السعودية
الولايات المتحدة	سلطنة عمان	السعودية + بريطانيا	الإمارات
فرنسا	قطر	استونيا	سلطنة عمان
ليتوانيا	مصر	كوريا+ سنغافورا+ أسبانيا	مصر
استونيا	الإمارات	الإمارات + روسيا+ ماليزيا	قطر
سنغافورا	الكويت	ليتوانيا	تونس
أسبانيا	البحرين	اليابان	المغرب
ماليزيا	الأردن	كندا	البحرين
كندا	تونس	فرنسا	الكويت
النرويج	المغرب	الهند	الأردن

المصدر: مركب بمعرفة الفريق البحثى من:

ITU (2021). Global Cybersecurity Index 2020.Geneva: TU. Development Sector. ITU Publications.pp.25-30.

ITU (2018) .Global Cybersecurity Index 2018. Geneva. ITU. Studies &Research.p.14.

وبالنسبة لجوانب تميز الدول الكبرى والعربية يشير التقريرين إلى بعض الجوانب الهامة: [1]

- جوانب تميز الدول الكبرى:

- **جوانب تميز أمريكية،** مرتبة متقدمة عالميًا على المحور القانونى لتوافر تدابير متعددة قانونية وموضوعية واجرائية للتعامل مع الجرائم السيبرانية.

[1] للتفاصل حول جوانب التميز القطرية عالمياً وعربياً – يراجع:

Ibid. pp.25-28.

ITU (2021). Global Cybersecurity Index 2020.Geneva: TU. Development Sector. ITU Publications. pp.22-129.

- **جوانب تميز كندا**، تفوق عالمى فى المحور التنظيمى المرتبط بسياسات وطنية فعالة للأمن السيبرانى على المستوى الكلى.

- **جوانب تميز لدى الدول الناهضة: سنغافورا وماليزيا**، تتصدر سنغافورا المحور القانونى بين دول آسيا والباسفيك، حيث أصدرت تشريع خاص للأمن السيبرانى، فى حين تتفوق ماليزيا فى إطار نفس المجموعة فى محورى: القدرات التنظيمية وبناء القدرات.
- **طفرات سيبرانية عربية نوعية**، وعلى رأسها دخول المملكة العربية السعودية إلى مربع الكبار فى العالم بإحتلالها المرتبة الثانية عالميًا مع بريطانيا لعام 2020، كما دخلت دولة الإمارات ذات المربع بإحتلالها المرتبة الخامسة عالميًا. وتشير التقارير إلى تميز المملكة السعودية فيما يتعلق بمحور (بناء القدرات) وتعدد المبادرات الوطنية فى هذا الخصوص كبرنامج الحاضنات التكنولوجية، والشبكة السعودية للبحوث والإبتكار وغيرهما.

2. مؤشر القوة السيبرانية الوطنية – NCPI

يعبر المؤشر National Cyber Power Index لمركز بلفر للعلوم والشئون الدولية عن مفهوم خاص بالمركز لقياس القوة السيبرانية تسعى دول العالم المختلفة لتحقيقها من خلال 7 أهداف:[1]

- مسح ومراقبة المجموعات المحلية.
- تقوية وتعزيز الدفاعات السيبرانية الوطنية
- التحكم في وإدارة بيئة المعلومات
- القيام بأنشطة جمع معلومات استخبارية اجنبية لدعم الأمن القومى
- تحقيق مكاسب تجارية أو تعزيز نمو الصناعة المحلية
- تدمير أو تعطيل البنية التحتية للخصم السيبرانى وقدراته
- المشاركة فى بلورة القواعد والمعايير السيبرانية الفنية الدولية.

ومن وجهة نظر المنهجية، فإن المؤشر يوجه الأنظار إلى أهمية التمييز (النية –Intent) وبين (القدرة – Capabilities) في التعامل مع الأمن السيبرانى الوطنى من خلال الأهداف السبعة السابق الإشارة اليها، فالحكومات قد تكون لديها القدرات لتحقيق هدف باستخدام الوسائل السيبرانية، ولكن ليس لديها النية للقيام بذلك. وقد ترغب في السعي لتحقيق هدف من خلال الوسائل الإلكترونية

---

(1) للمزيد من التفاصيل، يراجع:

Julia Voo. et.al. **Op. cit**. Pp.20-40.

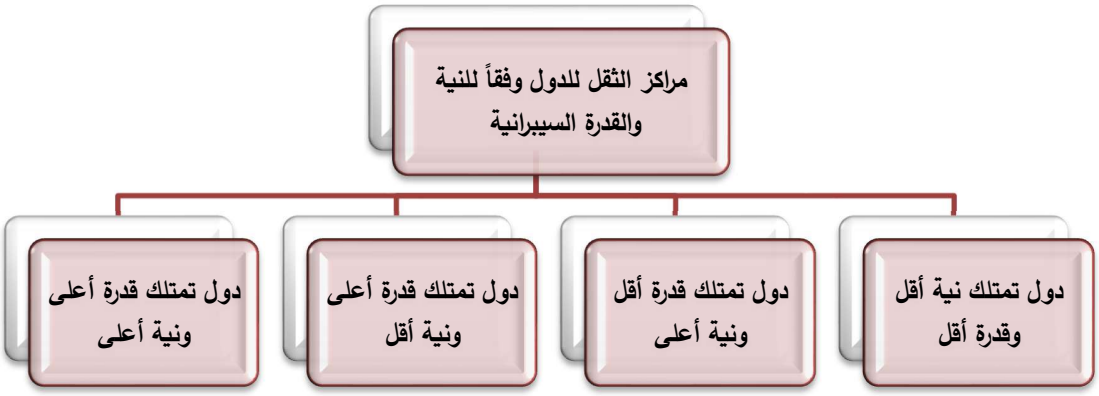
لكنها تفتقر إلى القدرة أو الموارد المطلوبة للقيام بذلك بالفعل. وعلى ذلك فقد توصل المركز إلى إلى تصنيف رباعى للدول، أو القوى السيبرانية الكبرى، وفقًا لمعيار القدرة والنية (شكل رقم 1-9).

فى إطار المنهجية السابقة خلص التقرير إلى مجموعة حقائق لتصنيف العالم سيبرانيًا

- **المجموعة الأولى: دول تمتلك قدرات أعلى ونية أعلى فى مجال الأمن السيبرانى،** ويأتى على رأسها: الولايات المتحدة الولايات المتحدة والمملكة المتحدة والصين وفرنسا وألمانيا.

شكل (1-9)

التقسيم السيبرانى الرباعى لدول العالم وفقاً لمؤشر القوة السيبرانية الوطنية:NCPI



المصدر: مركب بتصرف بمعرفة الفريق البحثى من:

-Julia Voo, et.al. (2020)), National Cyber Power Index Methodology and Analytical Considerations. USA. Belfer Center for science and International Affairs, Harvard Kennedy School, pp.3-6.

- **المجموعة الثانية: دول تمتلك قدرة أقل ونية أعلى فى مجال الأمن السيبرانى:** حيث تحاول اتباع سياسة الردع ولكنها لا تمتلك القدرات التي تمكنها من أن تصبح قوة إلكترونية شاملة، وتعلن عن نيتها لخوض هجمات سيبرانية واسعة النطاق ضد الهجمات السيبرانية التى تستهدفها، وأبرز تلك الدول: روسيا، إيران، إسرائيل، هولندا، وتقع أيران في هذه المجموعة ويُنسب إليها، وفقاً لتقرير بلفر، شن هجمات إلكترونية متعددة مما يشير إلى أنها كانت تسعى بقوة لتحقيق بعض الأهداف من خلال الفضاء الإلكتروني، ويتسم نهج الدول بهذه المجموعة بمحاولات الردع اللفظي لكن قدراتها المعلنة أقل مما تنوى القيام به.

- **المجموعة الثالثة: دول تمتلك قدرة أعلى، ونية أقل،** وتأتي في هذه المجموعة دول مثل كوريا الجنوبية وسنغافورة، وتتسم هذه الدول بتوافر القدرات العالية لتصبح قوة الكترونية ولكنها ليس لديها نية معلنة لشن هجمات أو تحقيق لأهداف محددة، للرغبة فى تجنب النزاعات والتمسك بالردع السيبرانى السلمى.
- **المجموعة الرابعة: دول ذات نية أقل وقدرة أقل،**وتندرج في هذه المجموعة كل من مصر وليتوانيا، وتتسم هذه المجموعة، وفق التقرير، بأنها اما لا تعمل بنشاط على تطوير قدرتها الالكترونية، كما أنها لا تعلن عن نيتها لبلوغ أهداف خارجية محددة لإبراز القوة في الفضاء السيبرانى، أو أنها لم تنشر قدرًا كافيًا من المعلومات عن استراتيجيتها السيبرانية.

ويوضح الجدول رقم (1-6) تطور تصنيف دول العالم على بعض المؤشرات العالمية للأمن السيبرانى بخلاف مؤشر القوة السيبرانية الوطنية لعام 2020.

جدول (1-6)

ترتيب الدول في مؤشر القوة السيبرانية الوطنية ومؤشر الأمن السيبرانى

م	ترتيب القوى السيبرانية العالمية وفقاً لمؤشر القوة السيبرانية الوطنية لعام 2020- NCPI	ترتيب القوى السيبرانية العالمية وفقاً لمؤشر الأمن السيبرانى العالمي لعام 2020- GCI
1	**الولايات المتحدة**	**الولايات المتحدة**
2	**الصين**	**السعودية + بريطانيا**
3	**المملكة المتحدة**	**استونيا**
4	**روسيا**	**كوريا+ سنغافورا+ اسبانيا**
5	**هولندا**	**الإمارات + روسيا+ ماليزيا**
6	**فرنسا**	**ليتوانيا**
7	**المانيا**	**اليابان**
8	**كندا**	**كندا**
9	**اليابان**	**فرنسا**
10	**استراليا**	**الهند**

المصدر: مركب بعرفة الفريق البحثى من :

Julia Voo, et.al. (2020). National Cyber Power Index Methodology and Analytical Considerations.USA: Belfer Center for science and International Affairs, Harvard Kennedy School, pp.11-13.

- ITU (2021). Global Cybersecurity Index 2020.Geneva: TU. Development Sector. ITU Publications.pp.25-29.

ويوضح تقرير عام 2020 لمركز بلفر أن الولايات المتحدة الأمريكية والصين، وفق التقرير، يعتبران القوى السيبرانية الأكثر شمولا على مستوى العالم فى عام 2020. ويركز التقرير فى خلاصاته على الحاجة إلى مزيد من الشفافية العالمية بخصوص أوضاع وبيانات الإنترنت والأنشطة الخاصة ببناء القدرات السيبرانية لدى دول العالم المختلفة، وهى الخطوات التى سوف تساهم فى مزيد من تعزيز قدرة العالم على مواجهة المهددات والمخاطر السيبرانية. [1]

ثانياً: الأمن السيبرانى والاقتصادات الرقمية والتنمية المستدامة والمشفرة فى إطار الثورة الصناعية:

تشير التقارير العالمية إلى أن الأمن السيبرانى يمثل أحد المقومات الرئيسية للتحول الرقمى فى العالم من واقع مسئوليته عن حماية حماية المواطنين والمنتجات والخدمات والأصول الرقمية الوطنية فى كافة القطاعات الإنتاجية والخدمية، وبناء مجتمع رقمي آمن.

فى ضوء ذلك يمكن الإشارة إلى الحقائق التالية:

- تعمق الإتصالية Connectivity، والتشبيك Networking فى البيئات التكنولوجية العالمية والمحلية فى إطار الثورة الصناعية يعزز المخاطر السيبرانية المصاحبة ، حيث يتزايد الإعتماد على التكنولوجيات البازغة والرقمية: الذكاء الإصطناعى، والبيانات الضخمة، وانترنت الأشياء، وسلسلة الكتل، والحوسبة السحابية، وغيرها من التكنولوجيات التى قادت إلى توسع فى استخدام شبكة الإنترنت حيث يتوقع أن يصل عدد الأجهزة المتصلة Connected devices إلى 27 مليار جهاز بنهاية عام 2021. بالإضافة إلى ذلك يستخدم أكثر من 66% من سكان العالم الهواتف المحمولة حيث يتجاوز عدد الخطوط، 8 مليار خط، يزيد عن عدد سكان العام ذاته فى مطلع 2021 وهو 7.8 مليار نسمة [2]، كما يصل عدد الخطوط إلى 8 مليار، ويضاعف من هذا التوسع خفض تكلفة الوصول للشبكة

---

[1] Julia Voo. et.al.**Op. cit**., p49.
Julia Voo, et.al. (2020). National Cyber Power Index Methodology and Analytical Considerations.USA: Belfer Center for science and International Affairs, Harvard Kennedy School, p.8.
ITU (2021). **Op. cit**. pp.25-27.

[2] يصل مستخدمي الشبكة الدولية الى أكثر من 4.7 مليار نسمة فى يناير 2021، ومستخدمى وسائط التواصل الإجتماعى الى 4. مليار نسمة يمثلون أكثر من 53% من سكان العالم. يراجع:
ITU (2021). Digital world 2021-Global Overview Report. Geneva: ITU. https://datareportal.com/

والتوسع فى النطاق العريض والجيل الخامس والسحابات، ومن ثم أصبحت التكنولوجيا الرقمية هى أساس جميع النظم الاقتصادية والاجتماعية الحديثة المبتكرة والتى يعتمد عليها النمو الاقتصادي العالمي ورفاهية الإنسان بشكل متزايد.

ويشير أحد التقارير الحديثة للإتحاد الدولي للإتصالات، وبناء على نموذج اقتصاد قياسى، إلى وجود آثار ايجابية مؤكدة على الاقتصادات الوطنية، بما فيها مصر، تنعكس على الناتج المحلى الإجمإلى والإنتاجية نتيجة التوسع فى استخدام الهواتف الثابتة والمحمولة العاملة بنظام النطاق العريض للإنترنت. بالإضافة إلى ذلك فإن الرقمنة ومبادرات التحول الرقمى لها تأثيرات أكثر ايجابية على الاقتصاد والناتج المحلى والإنتاجية أيضاً خاصة فى الاقتصادات المتقدمة أكثر من النامية، كما أن الإجراءات المؤسسية والتنظيمية تنعكس بصورة ايجابية وتوسعية على بيئة عمل الاقتصادات الرقمية فى دول العالم المختلفة. [1]

وقد أدى هذا الإنتشار الواسع للتكنولوجيا الرقمية والترابط الوثيق بين الأشياء والبشر والذكاء الاصطناعي والبيانات إلى زيادة مخاطر الهجمات السيبرانية التى أصبحت من وجهة نظر المنتدى الاقتصادى العالمي أحد المخاطر الراهنة الواضحة التى يواجهها العالم. وعلى الأجل المتوسط، فإن المنتدى يعود ويلقى الأضواء على مخاطر الأمن السيبرانى مجدداً فى سياق أوسع يرتبط بالتطورات التكنولوجية فى اطار الثورة الصناعية الرابعة حيث يضيف مخاطر انهيار البنية التحتية التكنولوجية، وفشل حوكمة التكنولوجيات البازغة والذى يضاعف بدوره من مخاطر المهددات السيبرانية خاصة مع توقعات للمنتدى بأتمتتة 85 مليون وظيفة خلال الخمس سنوات القادمة.

[1] عن العلاقة بين الرقمنة والإقتصاد والمؤشرات العالمية التى تراعى المزج بين البعدين، يراجع
Raul Katz and Fernando Callorda (2018). The economic contribution of broadband, digitization and ICT regulation. Geneva: ITU Expert Reports.

شكل (1-10)

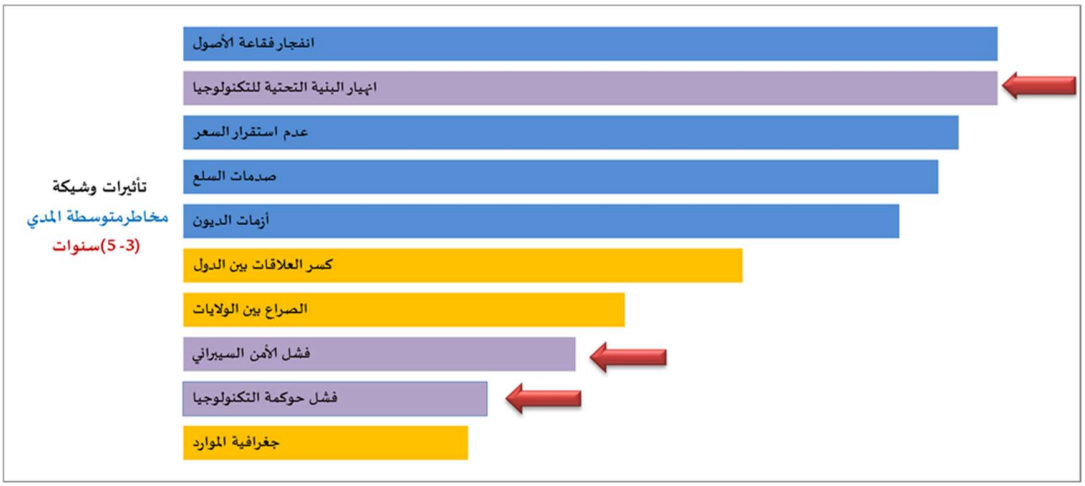
موقع المخاطر السيبرانية فى المخاطر العالمية الواضحة التى يواجهها العالم

Source: WEF (2020). The global risks report 2021- Insight Report.Geneva:WEF.p.11.

وتؤكد شركة – IBM على الترابط بين البيئات التكنولوجية المترابطة والتقدم الاقتصادى فى العالم الرقمى بالإشارة إلى أن قطاع الصناعات التحويلية قد تقدم إلى المرتبة الثانية كأكثر القطاعات الاقتصادية تعرضاً للهجمات السيبرانية بعد قطاع الخدمات المالية فى عام 2020، فى حين كان يحتل المركز الثامن فى التعرض لهذا النوع من الهجمات عام 2019. [1]

شكل (1-11)

مخاطر الأمن السيبرانى وانهيار البنية التكنولوجية وفشل حوكمة التكنولوجيا



Source: WEF. (2020). The global risks report 2021- Insight Report.Geneva: WEF.p.11.

[1] وجاء ترتيب القطاعات التى تعرضت للهجمات على النحو التالى: المال والتأمين، الصناعة، الطاقة، التجزئة، الخدمات المهنية، والخدمات الحكومية ، يراجع:
IBM. (2021). IBM.x-Force Threat Intelligence Index 2021.USA: IBM.pp.37-38.

وفى ظل هذا النوع من الترابط والتشبيك ترتفع المخاطر التشغيلية والتجارية الرئيسية لكافة المؤسسات الخاصة والعامة، والتى تحتاج فى هذه البيئات التكنولوجية التشابكية المترابطة إلى تبنى إستراتيجيات وعمليات لإدارة أمن المعلومات على نحو يخفف من التهديدات السيبرانية، مع الحفاظ على توافقها مع متطلبات الأمان والسرية وإمكانية التتبع والامتثال للوائح الحديثة.[1]

ويتوقع البعض أن تؤدي المخاطر الاقتصادية الضخمة وعدم وضوح الصورة إلى قيام المؤسسات الخاصة بزيادة وعيها بأهمية معالجة المعلومات وحمايتها لتحقيق أهداف العمل، ومع ارتفاع تكلفة خرق البيانات يتعين على المؤسسات إعادة النظر في إستراتيجياتها الأمنية. بالإضافة إلى دمج الأمان مع الأجهزة والتقنيات التي تحافظ على سلامة الشركات والأفراد، يجب أيضاً دمج الأمان عبر الإدارات لتعزيز الإنتاجية، وإنتاج منتجات موثوقة، وتعزيز علاقات العملاء القوية، ودفع الابتكار، حيث أنه على الرغم من أن الالتزام باللوائح أمر ضروري إلا أنه يمكن اختراق أي شركة بسبب عدم فعالية أو إهمال أى شخص والحلول التقنية فقط هى القادرة على تعويض الإهمال البشري، فثقافة الشركات التي تحترم الأمن الرقمي هي أعظم دفاع يمكن أن تنشئه الشركة لحماية بيئتها الرقمية. [2]

المجتمعات والاقتصادات الرقمية العالمية تدفع تكلفة فادحة للمخاطر والهجمات السيبرانية

فعلى سبيل المثال فإن هناك أكثر من 5 مليار مستخدم للهواتف النقالة التى يعد أكثر من 60% منهما هواتف ذكية، ويرتبط استخدامات هذه الهواتف اليومية بالعديد من المخاطر التى تتزايد يوماً بعد يوم. كما تتضمن الهندسة الإجتماعية ووسائل التواصل الإجتماعى خدعاً على المستخدمين لإفشاء المعلومات أو اتخاذ الإجراءات التي يمكن أن تعرض الأمن للخطر. ويساعد فى ذلك إنتشار المعلومات الشخصية بسهولة المتوفر عبر الإنترنت والتى يسهل توافرها وإنتشارها تمكين المهاجم السيبرانى من القرصنة واستخدام ملفات صغيرة كميات من المعلومات لكسب ثقة المستخدم وتأمين معلومات أعمق وأكثر شخصية. [3]

بالإضافة إلى ذلك، فإن الشكل رقم (1-12) يوضح أن تكلفة الهجمات السيبرانية قد تجاوز 5 تريليون دولار عام 2020 يتوقع أن ترتفع إلى 6 تريليون عام 2021. كما يوضح الشكل رقم

---

[1] KatiaValtorta, et.al. (2020). ICT security in the digital transformation Era-Do organization need digital security strategies. ArthurD. Little.pp.104. https://www.adlittle.com.

[2] KatiaValtorta, et.al. (2020). **Op. cit**.

[3] Look at:

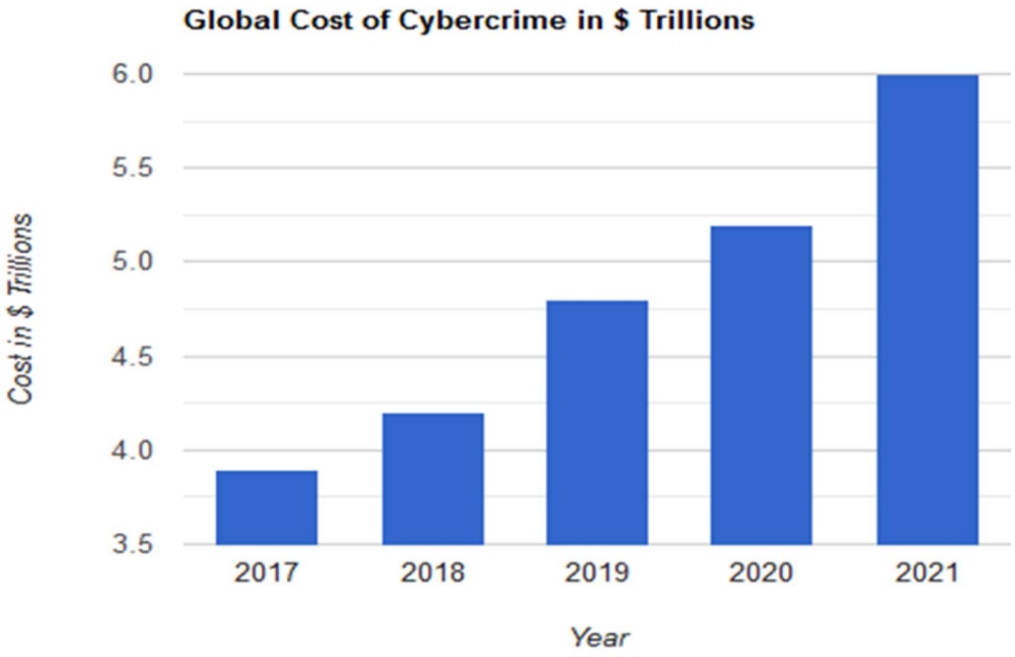
-WEF (2020). Connecting digital economies: Policy recommendations for cross-border Payments-Insight Report. Geneva: WEF.pp5-22.

(1-13) أن تصاعد تكلفة الهجمات يقابله تصاعد موازى فى تكلفة الإنفاق على خدمات الأمن السيبرانى بما فيها تأمين الهواتف المحمولة، والتى يتوقع أن ترتفع خدمات الأمن السيبرانى عليها فى المنشآت الصغيرة والمتوسطة والكبيرة من 5.5 مليار دولار عام 2020 إلى أكثر من الضعف فى عام 2025 ليصل الرقم المتوقع إلى 12.6 مليار دولار. [1]

شكل (1-12)

" تقديرات خسائر الأمن السيبرانى بين عامى 2017-2020 "

(تريليون دولار)



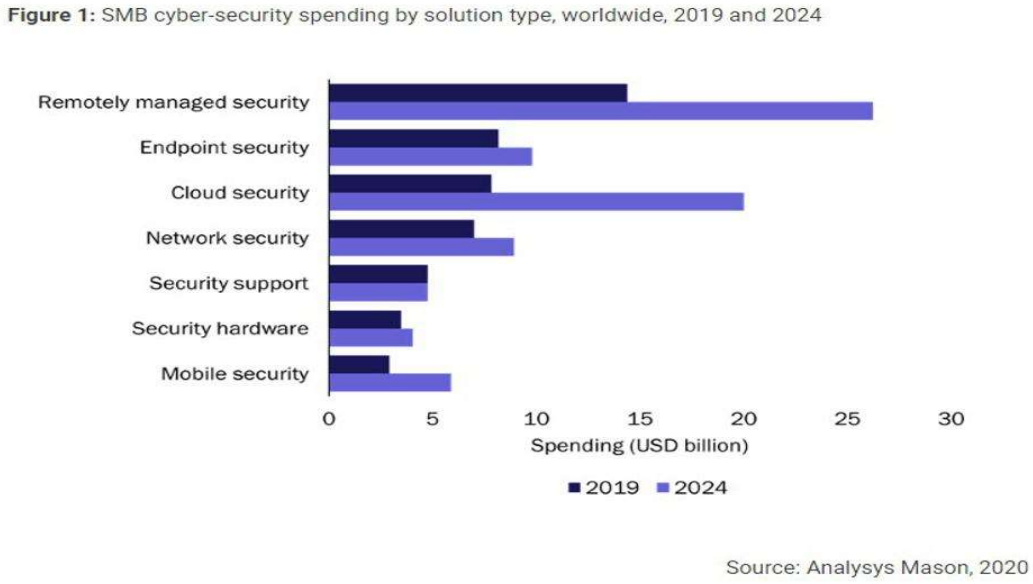
Source: Hailbytes (2020).33 Cybersecurity Stats for 2020. https://hailbytes.com/

ويوضح الشكل رقم (1-12) أن بعض أوجه هذا الإنفاق بين عامى 2019-2024 قد تزيد عن الضعف وعلى الأخص خدمات الأمن السيبرانى فى الحوسبة السحابية، وخدمات الأمن السيبرانى عن بعد.

[1]Elieen zimber (2021) SMB spend on securing mobile devices will increase at a CAGR of 18% to almost USD9 9 in 2025. https://www.analysysmason.com/.

شكل (1-13)

تكلفة الإنفاق على أنواع خدمات الأمن السيبرانى بين 2019-2024 (مليار دولار)



Source: Analysis mason 2020. https://www.analysysmason.com/.

- علاقات وثيقة بين الأمن السيبرانى والأمن الإجتماعى: دروس الجائحة:COVID-19

لم تقتصر الهجمات السيبرانية على القطاعات المالية والاقتصادية والتجارية فقط، لكنها امتدت إلى قطاعات اجتماعية هامة ومنها الخدمات الصحية التى اكتسبت أهمية خاصة فى كافة انحاء العالم فى ظلال جائحة كورونا: COVID 19. ففي أكتوبر 2020 تم رصد موجة من رسائل البريد الإلكتروني المخادعة التى تستهدف الأفراد والمنظمات والكيانات فوق الوطنية ذات الصلة بالتقنيات المرتبطة بالتوزيع الآمن للقاح COVID-19 بما فيها نشاط منظمة الأمم المتحدة للطفولة (اليونيسف) وتحالف اللقاح العالمي Gavi ومنصات تحسين معدات سلسلة التبريد (CCEOP) التي تُستخدم لتوزيع اللقاحات على مستوى العالم.[1]

كانت هذه هجمة /حملة تصيد سيبرانية Phishing تهدف للحصول على معلومات خاصة بعمليات النقل والتوزيع اللقاحات. وشملت الأهداف المستهدفة العديد من الوكلات والأجهزة المعنية فى الإتحاد الأوروبي، ومنظمات عالمية أخرى فى مقارها فى: في ألمانيا وإيطاليا وكوريا الجنوبية، جمهورية التشيك وأوروبا الكبرى وتايوان.[2]

---

[1]IBM. **Op. cit**. pp. 15-17.
[2]Ibid, pp.16-17.

نتائج الفصل الأول

- **أهمية مفاهيم الأمن السيبرانى على كافة الأصعدة،** فهى مقدمات وأدوات لازمة لفهم العالم الجديد الذى يزداد ترابطاً من خلال الشبكات والنظم وسلاسل القيمة الرقمية والتقنيات البازغة العابرة بتشابكاتها للحدود، والتى تحمل (القيمة الرقمية العالمية الجديدة) و(الأصول العالمية الرقمية الجديدة)، كما تحمل معها (المخاطر والمهددات السيبرانية الجديدة) فى نفس الوقت.
- **جوهر الأمن السيبرانى،** ويعبر عن قدرة الدول والمنظمات على حماية أنظمة المعلومات والإتصالات والمعلومات والدفاع عنها ضد المخاطر السيبرانية بكفاءة وأقل الأضرار والتكلفة.
- **دوائر تماس واسعة للأمن السيبرانى،** حيث ترتبط بإرتباط 27 مليون جهاز فى العالم بالإنترنت نهاية عام 2021، واستخدام 66% من سكان العالم للهاتف المحمول، وتمدد الاقتصادات الرقمية، وإنتشار التقنيات البازغة وتقنيات الجيل الخامس G5، وغيرها.
- **ترابط الأمن السيبرانى مع أشكال أخرى من الأمن،** حيث يتجاوز أمن الأنظمة والتطبيقات والشبكات إلى: الأمن الفضائي، والأمن الجنائي، والأمن العسكري، والأمن الجيوسياسي، والأمن الاقتصادي، والأمن الاجتماعي، والأمن البيئي، والأمن الشخصي للمواطن العادي.
- **تنوع المهددات السيبرانية وفداحة تداعياتها،** ومنها الهندسة الاجتماعية، وهجمات الفدية، وهجمات حجب الخدمات، وهجمات الحوسبة السحابية، والتصيد والبرامج الضارة وغيرها، والتي كلفت العالم أكثر من 5 تريليون دولار عام 2020، ويتوقع صعودها إلى 6 تريليون عام 2021.
- **تنوع وتطور أدوات الحماية ضد الهجمات السيبرانية،** مع تقدم وتطور الهجمات ذاتها، وتنقسم إلى أدوات الدفاع عن الشبكة، وأدوات فحص ثغرات الويب أو غيرهما من الأدوات.
- **تعولم مخاطر الأمن السيبرانى يهدد النظام العالمي،** وهناك إدراك عالمي متصاعد بخطورة المهددات السيبرانية للاقتصاد العالمي وبنية النظام العالمي، وهناك محاولات من الأمم المتحدة والإتحاد الأوروبى وغيرهما لترتيب نوع من الإصطفاف العالمي ضد هذه المخاطر المتصاعدة.
- **الحوكمة السيبرانية العالمية مطلب ملح،** وقد ظهرت مبادرات متعددة فى هذا الخصوص للأمم المتحدة ووكالاتها، والمنتدى الاقتصادى العالمي، وقمم مجموعة العشرين G20.

- **علاقة الأمن السيبرانى بحقوق الإنسان**، وهو ملف عالمى مطروح لضمان عدم الجور والإجتراء على حقوق المقررة الإنسان وفق المواثيق الدولية بحجة تعزيز الأمن السيبرانى ودرء مخاطره.
- **الدبلوماسية السيبرانية والرقمية**، مداخل مطروحة لتجنب انزلاق العالم لفوضى سيبرانية لضعف التواصل، ونقص تبادل المعلومات والخبرات ورص الصفوف لمواجهة المخاطر السيبرانية.
- **فداحة الخسائر السيبرانية فى القطاعات المالية**، حيث تتكبد المؤسسات المالية أكثر من 9% من صافى دخولها نتيجة الهجمات السيبرانية بما يفرض تحديات متصاعدة وغير مسبوقة على القطاعات المالية فى العالم، وتفرض أولويات جديدة على هذه القطاعات.
- **مبادرات متعددة لحوكمة الأمن السيبرانى فى القطاعات المالية**، سواء لصندوق النقد الدولي، البنك الدولي، بنك التسويات الدولية، مجلس الإستقرار المالي ولجنة بازل للرقابة المصرفية، المنظمة الدولية لهيئات الأوراق المالية، وغيرهم.
- **مخاطر سيبرانية جدية فى القطاعات المالية العربية**، وتتطلب مداخل غير تقليدية للتعامل معها وتضمين إدارة المخاطر السيبرانية ضمن إستراتيجيات وسياسات المصارف العربية، بناء وتنمية القدرات السيبرانية، تبادل الخبرات والمعلومات بين المؤسسات المالية الوطنية والعربية.
- **أهمية المؤشرات العالمية للأمن السيبرانى**، حيث تلقى بعض الأضواء على جوانب القوة والضعف وفرص التحسين، ومن أبرزها: مؤشر الأمن السيبرانى العالمي:GCI للإتحاد الدولي للإتصالات، ومؤشر القوة السيبرانية الوطنية: NCPI لمركز بلفر.
- **الإرتباط الإيجابى بين الأمن السيبرانى والاقتصادات الرقمية والتنمية المستدامة**، حيث تمثل البنة التحتية للمعلومات والإتصالات والتقنيات البازغة المكون الرئيس لهذه الاقتصادات الصاعدة، كما تمثل فى ذات الوقت أحد أدوات الأمم المتحدة لتسريع انجاز التنمية المستدامة وفق مؤتمرات الذكاء الإصطناعى للصالح العالم التى نظمتها المنظمة فى السنوات الأخيرة.
- خبرات متعددة مستفادة لمصر:

- نشر ثقافة الوعى السيبرانى على التوازى مع توسع استخدام تكنولوجيا المعلومات والإتصالات والتكنولوجيات البازغة فى الاقتصاد والمجتمع فى مصر.

- تبنى رؤية متكاملة لإدارة البيانات على المستوى القومى وكافة الجهات والأجهزة المعنية فى الدولة العامة والخاصة
- تبنى نظم متكاملة لإدارة المخاطر بوجه عام والمخاطر السيبرانية على وجه الخصوص فى المؤسسات العامة، ومؤسسات قطاعات الأعمال والمنظمات غير الحكومية.
- أهمية الإنخراط بقوة أكبر فى الحوارات والمبادرات العالمية ذات الصلة بالأمن السيبرانى
- تفعيل الدبلوماسية السيبرانية والرقمية، وأدوار مأمولة فاعلة للخارجية المصرية
- متابعة موقف مصر على المؤشرات العالمية ذات الصلة والعمل على سد الفجوات
- توفير تمويل كاف للإنفاق على أمن المعلومات كنسبة من الإنفاق على الأنظمة والشبكات والنظم والبنية التحتية المعلوماتية.

الفصل الثانى

أدوار عالمية وإقليمية وتجارب وطنية حول الأمن السيبرانى

نتج عن تعولم الأمن السيبرانى وتأثيراته الكبيرة على الأمن القومى والسلام الإجتماعى والقطاعات المؤثرة على الاقتصادات العالمية خاصة القطاعات المالية وعلى التنمية المستدامة بزوغ العديد من الأدوار العالمية الحاكمة فى التعامل مع أبعاد وتداعيات ومتطلبات الأمن السيبرانى.

وقد تصدرت الأمم المتحدة العديد من مشاهد التعامل مع الأمن السيبرانى وتأثيراته وعلى الأخص من خلال أدوار متعددة للإتحاد الدولي للإتصالات ITU، وهى الأدوار التى تتشابك مع أدوار إستكمال متطلبات القمم العالمية لمجتمع المعلومات وغيرها من المبادرات العالمية الأممية ذات الصلة. وقد صاحب هذه الاهتمامات الأممية إهتمامات إقليمية متعددة خاصة على المستوى الأوروبى سواء برعاية الإتحاد الأوروبى أو بمبادرات أهلية وبحثية لمراكز الفكر، كما وصل الاهتمام إلى المستوى الإقليمي الأفريقى وكذلك العديد من الجهود والمبادرات على المستوى الإقليمي العربي التى تستحق القاء الضوء على بعض جوانبها.

وفى ضوء هذه الاهتمامات العالمية والإقليمية وتفاعلات دول العالم المختلفة معها، فقد راكمت دول العالم على اختلاف مستويات التنمية بها العديد من الخبرات الوطنية التى مزجت بين تطورات الأمن السيبرانى الداخلية وتطوراته وبين مخاطره ومهدداته الخارجية العابرة للحدود والتى تتطلب أنواع مختلفة ومتعددة من الحوكمة والمبادرات الإستباقية لإدارة المخاطر السيبرانية على المستوى الوطنى، خاصة مع تعاظم تلك المخاطر مع التطورات فى الرقمنة وتعمق الاقتصادات الرقمية، والتوسع فى استخدام التكنولوجيات البازغة فى مناحى الحياة المختلفة.

يُلقى الفصل الحالى بعض الأضواء على الجهود العالمية والإقليمية البارزة التى تسعة لخلق اصطفاف عالمى للتعامل مع مهددات الأمن السيبرانى خاصة العابرة للحدود، كما يلقى الفصل الأضواء ببعض التفاصيل على تجارب دولية متميزة وفق المؤشرات العالمية للأمن السيبرانى لدى دول العالم المختلفة المتقدمة والناهضة والنامية ومنها: التجربة الأمريكية، تجربة كوريا الجنوبية، تجربة الهند،وتجربة اسرائيل، وبعض التجارب العربية وتشمل: المملكة العربية السعودية، وسلطنة عمان ودولة الإمارات العربية المتحدة.

وتقدم المراجعات السابق الإشارة اليها العديد من الخبرات التى يمكن الإستفادة منها فى تطوير التجربة المصرية فى التعامل مع الأمن السيبرانى لاحقاً.

المبحث الأول: أدوار ومبادرات عالمية وإقليمية فى التعامل مع الأمن السيبرانى

المبحث الثانى: خبرات الأمن السيبرانى فى تجارب دول متقدمة وناهضة ونامية

المبحث الثالث: خبرات التعامل مع الأمن السيبرانى فى تجارب دول عربية

المبحث الأول

أدوار ومبادرات عالمية وإقليمية في التعامل مع الأمن السيبرانى

تشير الجهود العالمية والإقليمية في مجال الأمن السيبرانى إلى الرابطة الوثيقة بين قضايا الأمن السيبرانى وومبادرات وخطط التحول إلى الاقتصادات والأنشطة الرقمية فى العالم، كما تشير إلى أدوار مأمولة للأمن السيبرانى والحوكمة الرقمية فى دعم التنمية المستدامة.

أولاً: لأمم المتحدة والإتحاد الدولي للإتصالات: مبادرات متعددة فى إطار القمم العالمية لمجتمع المعلومات، والربط بين التحولات الرقمية والأمن السيبرانى

1. أدوار متعددة للأمم المتحدة ووكالاتها المتخصصة

أكدت مؤتمرات مجتمع المعلومات للأمم المتحدة على الربط المباشر بين التوسع فى استخدام الإنترنت فى العالم لأكثر من 50% من سكان العالم وبين تمدد الاقتصادات الرقمية وأشكالها خاصة التجارة الإليكترونية حيث يتسوق ربع سكان العالم عبر الشبكة الدولية.

ويركز المؤتمر الأخير لمجتمع المعلومات على قضايا سيبرانية هامة تتبناها الأمم المتحدة بهدف تعزيز الثقة والأمن فى استخدام تكنولوجيا المعلومات والإتصالات، وأبرزها: [1].

- **توجهات متعددة للتنبيه إلى مخاطر أمن المعلومات**، سوا ء بقرارات منفردة أو فى سياقات القمم العالمية لمجتمع المعلومات منذ عام 2000 وبينها تأسيس فريق خبراء حكوميين: GGE" منذ عام 2004–2005 لمناقشة مخاطر أمن المعلومات على المستوى العالمي، كما نبهت الأمم المتحدة منذ عام 2006 إلى مخاطر أمن الشبكات وأهمية حماية البنى المعلوماتية التحتية من الهجمات.
- **تحفيز تأسيس فرق وطنية للإستجابة للحوادث والأمن السيبرانى**، بهدف التعامل مع الحوادث الأمنية الحاسوبية، والتى يتم متابعة نشاطها من خلال الإنكتاد: UNCTAD.
- **حوكمة وإدارة مخاطر الإنترنت والتحولات الرقمية** والتكنولوجيات البازغة ودوره فى دعم التنمية المستدامة، من خلال أنشطة متعددة من أهمها:
  - مؤتمرات الذكاء الإصطناعى للصالح العام – AI 4Good

---

(1) يراجع فى هذا الخصوص:
الجمعية العامة (2020). التقدم المحرز في تنفيذ نتائج القمة العالمية لمجتمع المعلومات ومتابعتها على الصعيدين الإقليمي والدولي. نيويورك: المجلس الإقتصادى والإجتماعى، ص ص، 15، 29.

- **منتدى حوكمة الإنترنت فى برلين 2019** تحت شعار: عالم واحد، شبكة واحدة، رؤية واحدة، والتركيز على قضايا إدارة البيانات، الأمن السيبرانى، والشمول الرقمى، ودور التكنولوجيات الرقمية فى دعم التنمية المستدامة.
- **الشراكة العالمية لتفعيل دور تكنولوجيا المعلومات والإتصالات فى التنمية المستدامة 2020**، بتعاون حوالى 14 وكالة أممية لربط مؤشرات تكنولوجيا المعلومات والإتصالات بأهداف التنمية المستدامة: SDGs.
- **تشكيل فريق رفيع المستوى للتعاون الرقمى**، فى عام 2018 لدراسة الآثار الإجتماعية والأخلاقية والاقتصادية للتعاون الرقمى ومحاولة بلورة التزامات عالمية فى هذا الخصوص بما يعزز دور التعاون الرقمى فى تحقيق التنمية المستدامة.

2. أدوار رائدة للإتحاد الدولي للإتصالات – ITU

تأسس الإتحاد فى عام 1965 ليعمل فى ثلاثة اتجاهات: الإتصالات الراديوية، تقييس الإتصالات، وتنمية الإتصالات.

ويمكن الإشارة بخصوص إهتمامات الإتحاد فى مجال الأمن السيبرانى، إلى أن أدوار الإتحاد فى هذا الجانب لم تقتصر فقط على المتابعات وترتيب إصدار الإحصاءات والمؤشرات ذات الصلة بما فيها الرقمية فقط، وانما تعدى ذلك إلى تقديم الدعم الفنى المباشر لدول العالم المختلفة فى اعداد الإستراتيجيات السيبرانية الوطنية من خلال الأدلة الفنية الداعمة من جهة، وتقديم العون الفنى المباشر، والمشاركة فى تظيم المؤتمرات والفاعليات ذات الصلة عالمياً وإقليمياً ذات صلة من جهة أخرى [1]. ويربط الإتحاد الدولي بصورة صريحة فى توجهاته وأنشطته بين أهمية بناء الثقة فى البنة التحتية للمعلومات والإتصالات وبين تحقيق التنمية الاقتصادية والإجتماعية المستدامة خاصة مع تطور استخدام شبكات الإتصالات المتنقلة للجيل الخامس من جهة، وتوقعات الإتحاد بوصول عدد الأجهزة الموصولة بالإنترنت إلى 50 مليار جهاز عام 2025.

يُلقى الجدول التالى رقم (2–1) بعض الأضواء على الدور الرائد الذى يقوم به الإتحاد الدولي للإتصالات:ITU فى مجال الأمن السيبرانى، والتى تشمل العديد من المجلات بما فيها مواجهة جائحة كورونا، والإهتمات الخاصة بالحماية والتمكين للمرأة والأطفال والشباب.

---

[1] وقد أصدر الإتحاد دليل خاص لإعداد الإستراتيجيات السيبرانية للأمن السيبرانى بالمشاركة مع أطراف متعددة من بينها البنك الدولة وحلف شمال الأطلنطى، وبعض مراكز الفكر والمنظمات غير الحكومية:
الإتحاد الدولي للإتصالات وآخرون (2018). دليل لوضع استراتيجية وطنية للأمن السيبرانى – التزام استراتيجى بالأمن السيبرانى. جنيف: الإتحد الدولي للإتصالات: ص ص،10-50.

جدول (2-1)

برامج ومبادرات الاتحاد الدولي للإتصالات فى مجال الأمن السيبرانى

مجال العمل	الأدوار – المبادرات – الأطر
التخطيط والسياسات	- برنامج العمل العالمي للأمن السيبرانى GCA، وأطلق عام 2007 ويهدف لتحسين الثقة والأمن فى مجتمع المعلومات. - الإتحاد مسئول عن تنفيذ مبادرات القمم العالمية لمجتمع المعلومات WSIS، ومنها مبادرة ربط العالم Connect the World - تكوين الفريق الإستشارى لتنمية الإتصالاتTDAG، ويضم بدوره فرق فرعية فنية متخصصة لدعم قطاعات الإتصالات عبر العالم. - إصدار دليل عملى عام 2018 لدعم عملية اعداد الإستراتيجيات الوطنية للأمن السيبرانى بمشاركة العديد من الأطراف المعنية فى العالم.
المؤشرات والتقارير والأدلة	- المؤشر العالمي للأمن السيبرانى GCI - قاعدة بيانات مؤشرات واحصاءات تكنولوجيا المعلومات والإتصالات - تقارير الإتجاهات الرقمية العالمية والإقليمية Digital Trends Reports - اطلاق دليل وضع إستراتيجية وطنية للأمن السيبرانى بالتعاون مع البنك الدولي وشركاء آخرين عام 2018.
جائحة كورونا COVID19	-اطلاق خطة عمل بالتعاون مع المنتدى الاقتصادى العالمي WEF عام 2020 لدعم الحكومات والمواطنين والقطاع الخاص فى توظيف التكنولوجيا الرقمية للتعامل مع تداعيات الجائحة من خلال مبادرات مشتركة لتسهيل وتوسيع النفاذ الموثوق والآمن للأنظمة الصحية المعنية بأزمة الجائحة.
المرأة	- يقوم الإتحاد بالشراكة مع آخرين بأكثر من مبادرة لتمكين النساء فى الفضاء السيبرانى منها مبادرة: Women in Cyber Mentorship، والتركيز على المساواة الرقمية وتسويق النماذج النسوية السيبرانية، وبناء القدرات من خلال تدريب متخصص متاح على الشبكة (مارس- أغسطس2021).
الشباب	- اطلاق أكثر من مبادرة منها: Generation Connect، ومبادرة Youth4Cyber، لتطوير شبكة عالمية من الجمعيات التي يقودها الطلاب والتي توفر للشباب الوعي والمعرفة ومهارات الأمن السيبراني. - تأسيس منصة عالمية لدعم مبادرات الشباب السيبرانية 18-26 سنة لتعزيز استفادة الشباب من الفرص السيبرانية، ومواجهة التحديات السيبرانية.
الطفولة	- الإصدار الرسمي للمبادئ التوجيهية الجديدة للإتحاد الدولي للاتصالات لعام 2020 بشأن حماية الأطفال على الإنترنت (COP). - نظم الإتحاد حوارًا متخصصاً بمشاركة فتيان عبر الإنترنت حول المبادىء

مجال العمل	الأدوار – المبادرات – الأطر
	التوجيهية – يونيو 2020 بمشاركات واسعة من القطاع الخاص سعياً لتطوير أطر وطنية وإقليمية تدعم حماية الأطفال عبر الشبكة.

المصدر: مركب بمعرفة الفريق البحثى من موقع الإتحاد :https://www.itu.int/ar/about/

3. اهتمامات حلف شمال الأطلسي NATO بالأمن السيبرانى

حيث قام بتأسيس مركز قيادة متخصص للتعامل مع مهددات الأمن السيبرانى لحلف شمال الأطلنطي عام 2018، ويعمل الحلف بصورة مستمرة على تطوير أنشطة للدفاع السيبرانى: Cyber Defence، وقام منذ عام 2016 بتطوير معاهد للدفاع السيبرانى:Cyber Defence Pledge للتعامل مع النمو المتزايد للأخطار السيبرانية التى تهدد دول الحلف.[1]وتهدف هذه الجهود بالدرجة الأولى إلى حماية شبكات وعمليات الحلف وشبكات الدول الأعضاء فى الجو والأرض والبحر، بما يتطلبه ذلك من جهود بناء القدرات والتدريب بحيث تتحول واجبات الدفاع السيبرانى جزء لا يتجزء من منظومات الدفاع بالدول الأعضاء. وقد شارك الحلف، كما سبقت الإشارة، فى دعم بعض أنشطة الإتحاد الدولي للإتصالات بما فى ذلك اصدار دليل وضع الإستراتيجيات الوطنية للأمن السيبرانى.

ثانياً: مبادرات سيبرانية إقليمية متنوعة ذات صلة:

يشير الجدول (2–2) إلى مجموعة من الملامح في الاهتمام بالأمن السيبرانى على المستوى الإقليمي من أبرزها:

- **الربط بين الأمن السيبرانى والتحولات الرقمية لتعزيز الثقة فى الاقتصاد والبنية التحتية**، وهو ملمح رئيسي فى التجارب الأوروبية والأفريقية والعربية على السواء، وهو ما يتوافق مع التوجهات العالمية السابق الإشارة اليها فى هذا الخصوص.

(1)NATO (2021). Cyber Defence. https://www.nato.int/cps/en/.

جدول (2-2)

أهم المبادرات الإقليمية في مجال الأمن السيبرانى والتحول الرقمي

الأقاليم العالمية	أهم المبادرات والخطوات
أوروبا	- تأسيس وكالة الإتحاد الأوروبي للأمن السيبرانى 2004 – ENISA، وإصدار قانون الإتحاد الأوروبى للأمن السيبرانى لعام 2013. - توسيع أدوار الوكالة منذ عام 2019 لدعم الإدارة الإلكترونية، مواجهة الجريمة السيبرانية، آليات أوروبية لحوكمة انترنت الأشياءIoT والذكاء الإصطناعي. - طرح الإستراتيجية الأوروبية للبيانات عام 2020 من جانب المفوضية الأوروبية. - طرح الإستراتيجية الأوروبية للأمن السيبرانى فى ديسمبر 2020، وتقرير خاص عن بلورة معايير سيبرانية للتعامل مع الجيل الخامس G5 فى فبراير 2021.
أفريقيا	- إهتمام أجندة التنمية المستدامة لأفريقيا: 2063 بالأمن السيبرانى لصالح الأفراد والمؤسسات والدول. - اتفاقية الإتحاد الأفريقي للأمن السيبرانى وحماية البيانات الشخصية (اتفاقية مالابو)، الصياغة 2011، والتبنى 2014، والتصديق عام 2020 من جانب 8 دول فقط، كما وقعت 14 دولة ولم تصدق عليها بعد. - تشكيل فريق خبراء للأمن السيبرانى يتبع الإتحاد الأفريقي عام 2018، - إعتماد مجلس وزراء تكنولوجيا المعلومات والإتصالات الأفارقة إستراتيجية أفريقية للتحول الرقمى عام 2020،
الوطن العربي	- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 - المركز العربي الإقليمي للأمن السيبرانى ARCC، وبدء نشاطه عام 2013 لتعزيز الأمن السيبرانى العربي بالتعاون مع الإتحاد الدولي للاتصالات – ITU. - جهود الجامعة العربية فى تحديث الإستراتيجة العربية للإتصالات وتكنولوجيا المعلومات 2022-2026، ومشروع قانون عربى للأمن السيبرانى. - المنتدى العربي رفيع المستوى لمجتمع المعلومات ودوره فى دعم التنمية المستدامة عام 2020، أولويات الاقتصاد الرقمي وإدارة الإنترنت والتمكين والشمول الرقمى. - الدورة الرابعة للمؤتمر العربي لأمن المعلومات (6 – 12 سبتمبر 2020) في مصر تحت شعار "الأمن السيبرانى فى عصر التحول الرقمى." - إطلاق (المجلة العربية للمعلوماتية وأمن المعلومات)، وقد صدر العدد الأول من المجلة فى أكتوبر 2020، عن المؤسسة العربية للتربية والعلوم والآداب.
غربى آسيا	- تبنى اللجنة الاقتصادية والإجتماعية لغربى آسيا (الإسكوا) خططاً للأمن السيبرانى، وتعظيم دور تكنولوجيا المعلومات والإتصالات فى تحقيق التنمية المستدامة فى دول الإقليم.

المصدر: مركب بمعرفة الفريق من مصادر متعددة (قائمة المراجع)، ومنها:

-European Union Agency for Cybersecurity-ENISA (2021). Security in G5 specifications. Greece. ENISA. Pp.9-39.

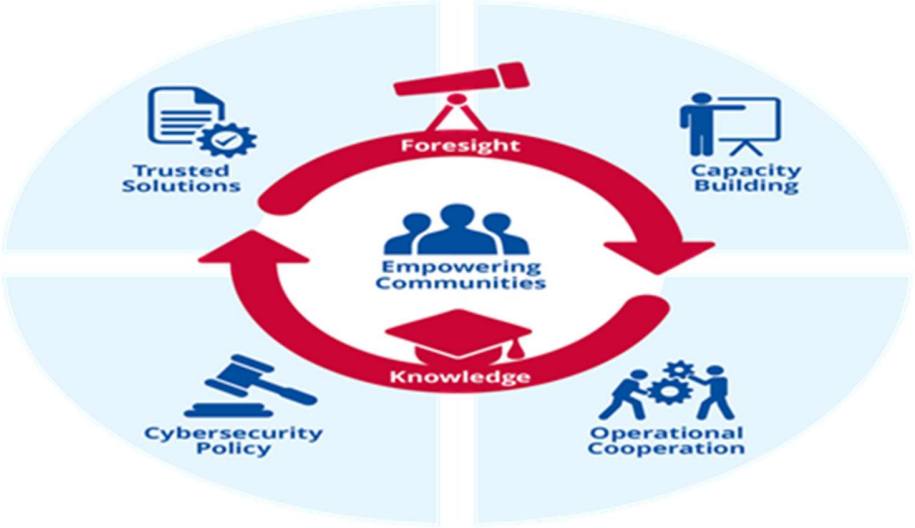
- **دور الأطر المؤسسية السيبرانية الفاعلة إقليميًا**، ويبرز فى هذا الخصوص دور وكالة الإتحاد الأوروبى للأمن السيبرانى – ENISA [1]، والتى تلعب دوراً محورياً فى تنسيق وتوجيه الجهود الأوروبية فى مجال الأمن السيبرانى وتقديم الدعم الفنى وبناء القدرات ذات الصلة، ودعم الثقة فى الاقتصاد الأوروبى الشبكى المترابط من خلال رؤية مستقبلية وإستباقية كما يوضح الشكل رقم 2–1، كما تبرز أدوار أوروبية أخرى مثل (المركز الأوروبى لدراسات مكافحة الإرهاب والمخابرات –ECCi) والذى يعطى قضايا (الأمن الإليكترونى) وانعكاساتها السياسية والاقتصادية أهمية بالغة فى السنوات الأخيرة.
- **جهود مطلوبة لتعزيز الأمن السيبرانى الأفريقى**، كما يوضح الجدول السابق، تفتقر القارة الأفريقية، على خلاف التجربة الأوروبية، إلى الإطار المؤسسى الفاعل الموثوق به للأمن السيبراني الأفريقى لتنظيم المعاملات الإلكترونية وحماية البيانات الشخصية وتعزيز الأمن السيبراني والحوكمة الإلكترونية ومكافحة الجرائم الإلكترونية. ولهذا السبب يصنف الإتحاد الدولي للإتصالات دول القارة بإعتبارها الأقل التزاماً بمعايير الأمن السيبرانى وفقاً لتقرير المؤشر العالمي للأمن السيبرانى: GCI لعام 2018.[2]

[1] وتعمل الوكالة على تنسيق الجهود الوطنية وتبادل الخبرات والمعارف لتعزيز الإدارة الفعالة للأمن السيبرانى مع أطراف أوروبية وغير أوروبية مثل كوريا الجنوبية على سبيل المثال:
-European Union Agency for Cybersecurity-ENISA (2020). Trusted and cyber secure Europe – ENISA strategy. Greece: ENISA. Pp.5-17.

[2] Landry Signé and Kevin Signé (2021). How African states can improve their cybersecurity. Washington: BROOKINGS Institution. Pp.1-3.

شكل (2-1)

محاور عمل وكالة الإتحاد الأوروبى للأمن السيبرانى



Source: European Union Agency for Cybersecurity-ENISA (2020). Trusted and cyber secure Europe – ENISA strategy. Greece: ENISA. P.5.

- **فجوات متعددة فى جهود تعزيز الأمن السيبرانى العربي**، فعلى الرغم من تعدد الجهود والمبادرات الا أن الأمن السيبرانى العربي يفتقر بدوره، كما الأفريقى، إلى آلية فعالة تشريعية ومؤسسية لتكامل وتنسيق الجهود العربية القطرية فى سياق عربى مشترك. وقد جرت محاولات أولية من جانب مجلس وزراء العدل العرب لطرح مسودة مشروع القانون العربي الإسترشادى لحماية الأمن السيبرانى عام 2019 لكن النتائج الأخيرة لم تظهر بعد. [1]

من جهة أخرى، بذلت جهود لوضع مبادىء توجيهية لحماية الإنترنت فى الوطن العربي، وذلك فى ضوء زيادة أنشطة الاقتصاد والمجتمع العربي على الشبكة الدولية والتوسع فى التجارة الإليكترونية وغيرها من الأنشطة الشبكية. وفى هذا السياق قامت جمعية دولية (جمعية الإنترنت- Internet Society) بوضع مجموعة من مبادىء أمن البنية التحتية للشبكة فى العالم العربي بما يعزز دورها الآمن فى التنمية الاقتصادية الإجتماعية العربية، وسعياً لتعزيز الإرتباط الآمن للاقتصادات العربية فى الاقتصاد العالمي، خاصة مع ارتفاع تكلفة الهجمات فى بعض الدول العربية مثل المملكة العربية

(1) جامعة الدول العربية (2019). مذكرة الأسباب الموجبة لأمن وسلامة الفضاء السيبرانى – الإنترنت (غير منشورة) ومسودة مشروع القانون الإسترشادى العربي لحماية الأمن السيبرانى. بيروت: المركز العربي للبحوث القانونية والقضائية.

السعودية ودولة الإمارات العربية، وعلى الأخص هجمات الفدية –Ransomware .[1]

ثالثاً: اسهامات الجماعات العلمية ومراكز الفكر فى قضايا الأمن السيبرانى

صاحب التوسعات الرقمية فى مجالات النشاط الإنسانى المختلفة جهود موازية وحافزة من الجماعات العلمية للباحثين ومراكز ومعاهد البحوث، وكذلك من مراكز الفكر المختلفة حول العالم والتى سنعرض لجوانب منها فيما يلى.

1. دور الجماعة العلمية والأنشطة البحثية حول الأمن السيبرانى:

توضح نتائج استعلام الفريق البحثى فى قاعدة بيانات البحوث العلمية: Web of Science، أنه تم إصدار حوالى 57,685 بحث ذو علاقة بالأمن السيبرانى فى الفترة 2015 – 2020، وتناولت موضوعى(الأمن السيبرانى: Cyber–Security) و(أمن المعلومات: Information Security)

ويوضح شكل 2–2 النمو السنوي المطرد والأيجابى لعدد الأبحاث الذى تم نشرها، حيث يملك عام 2019 النصيب الأكبر منها بنسبة 20%، وفى عام 2020 انخفضت الأبحاث المنشورة وهو الأمر الذى قد يرجع للأثر السلبى لتداعيات أزمة كوفيد–19 وما صاحبها من معدلات إصابات وتطبيق إجراءات التباعد الاجتماعي التي أثرت بالسلب على البحث العلمى.[2]

كما يوضح جدول شكل 2–3 عدد الأبحاث التي شاركت فيها كل دولة، حيث يتصدر باحثي الصين والولايات المتحدة الأمريكية بنسبة تصل إلى حوالي 44% وبفارق كبير في عدد الأبحاث عن باقي دول العالم الأخرى، وهو تصدر يتوافق إلى حد كبير مع تصدر الولايات المتحدة الأمريكية المؤشرات العالمية المختلفة للأمن السيبرانى. ويوضح الجدول أيضاً مساهمات الباحثين المصريين فى هذا الزخم العلمى العالمي حيث شارك الباحثون المصريون في عدد 355 بحثًا. ومن الإسهامات الحديثة صدور كتاب عالمي حول الأمن السيبرانى من جانب مجموعة من الباحثين فى مراكز وجامعات

---

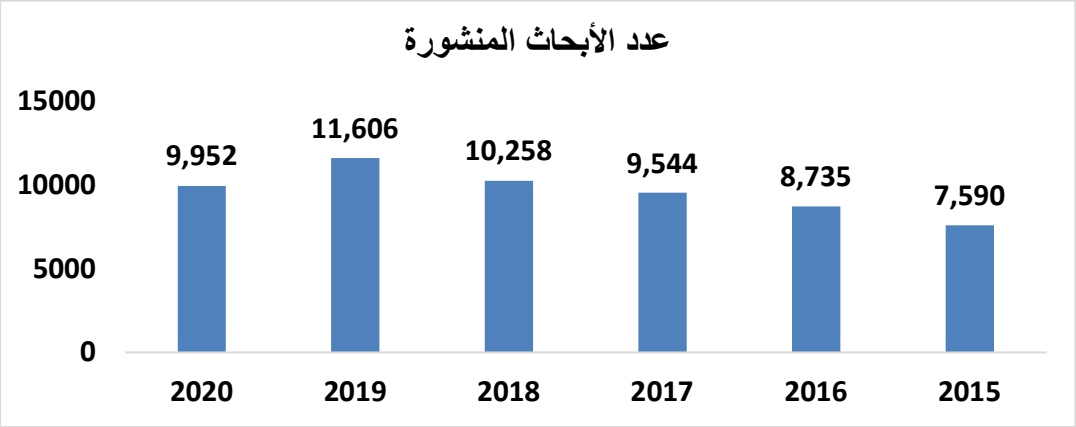
[1] وقد تعرض التقرير لدور الإستراتيجيات الوطنية للأمن السيبرانى، وأدوار مقترحة للفرق الوطنية العربية للتصدى لحوادث أمن المعلومات، مع اقتراح توصيات مناسبة، يراجع:
- جمعية الإنترنت (2020). المبادئ التوجيهية المتعلقة بأمن البنية التحتية للإنترنت فى المنطقة العربية. الولايات المتحدة الأمريكية: جمعية الإنترنت، ص ص، 7، 39.

[2] تمت مراجعة القاعدة فى يناير 2021 – يراجع: https://access.webofknowledge.com/

عالمية وتحرير أكاديميين مصريين من جامعتى القاهرة والمنصورة عام 2019.[1]

شكل (2-2)

تطور أعداد الأبحاث حول الأمن السيبرانى بين عامى (2015-2020)



المصدر: مركب بمعرفة الفريق البحثى فى يناير 2021 من:https://access.webofknowledge.com

جدول (2-3)

بيان مساهمات دول العالم ومصر فى أبحاث الأمن السيبرانى في الفترة (2015-2020)

اسم البلد	عدد الأبحاث	اسم البلد	عدد الأبحاث	اسم البلد	عدد الأبحاث
CHINA	13204	FRANCE	1419	SOUTH AFRICA	760
USA	12434	SPAIN	1416	SINGAPORE	751
INDIA	5728	JAPAN	1366	NETHERLANDS	736
ENGLAND	3311	KSA	1097	POLAND	665
AUSTRALIA	2328	MALAYSIA	961	SWEDEN	653
GERMANY	2123	TAIWAN	941	Egypt	355
S. KOREA	1936	BRAZIL	879		
CANADA	1933	PAKISTAN	830		

المصدر: مركب بمعرفة الفريق البحثى فى يناير 2021 من:https://access.webofknowledge.com

[1] وقد تناول الكتاب مجموعة متنوعة من قضايا الأمن السيبرانى الهامة فى علاقتها بتطبيقات المدن الذكية وانترنت الأشياء والحوسبة السحابية وغيرها.

Aboul Ella Hassanin and Mohamed Elhoseny-Editors (2019). Cybersecurity and Secure Information Systems-Challenges and solutions in a smart environment. Switzerland: Springer- Advanced Sciences and Technologies for Security Applications.

وبخصوص القضايا النوعية المرتبطة بالأمن السيبرانى التى تناولتها الإسهامات البحثية السابق الإشارة اليها، ومن واقع استخدام برامج التنقيب (برنامج R) فقد تصدرت قضايا: نظام الأمن السيبرانى Cybersecurity system، مهددات الأمن السيبرانى Cybersecurity threats قواعد وحوكمة الأمن السيبرانى Cybersecurity Regulation، وتطبيقات الأمن السيبرانى Cybersecurity Applications، بالإضافة إلى أبحاث تتناول أمن الخصوصية Security Privacy، وطرق اكتشاف الهجمات السيبرانية، وعلاقة انترنت الأشياء بالتطبيقات السيبرانية وطرق وأساليب إدارة مخاطر الأمن السيبرانى.

2. <u>دور مراكز الفكر والمنظمات الأهلية فى الاهتمام والتوعية بأهمية الأمن السيبرانى</u>

يعتبر (المنتدى الاقتصادى العالمي– WEF) أحد النماذج العالمية الجديرة بالتحليل فى هذا الخصوص، حيث بادر بتأسيس (مركز الأمن السيبرانى– Center of Cybersecurity) ليقود الحركة العالمية لتحديد تحديات الأمن السببرانى وسبل تحسين حالة الثقة الرقمية فى العالم، من خلال تبنى المركز لثلاثة أولويات فى مجال الأمن السيبرانى:[1]

أ. **بناء مرونة وتكيف سيبرانى فعال –Cyber Resilience:** من خلال تقديم حلول سيبرانية فعالة، ونشر أفضل الممارسات ذات الصلة فى البيئات الرقمية المختلفة فى دول العالم.

ب. **تعزيز التعاون العالمي:** خاصة بين الأطراف المعنية فى القطاعين العام والخاص، والعمل على تشكيل مبادرات عالمية جماعية لتحديد والتعامل مع مخاطر الأمن السيبرانى.

ت. **تشكيل فهم أفضل لشبكات وتكنولوجيات المستقبل:** بتحديد تحديات الأمن السيبرانى واستغلال الفرص المتاحة فى إطار تكنولوجيات الثورة الصناعية الرابعة.

ويشارك فى هذه الأنشطة للمنتدى الاقتصادى العالمي العديد من مراكز الفكر فى العالم (مثل كارنيجى للسلام)، والجامعات (جامعة اكسفورد)، وأجهزة الأمم المتحدة المعنية مثل الإتحاد الدولي للإتصالات، كما يشارك بعض المؤسسات العربية مثل شركة آرامكو السعودية، وهيئة تقنية المعلومات بسلطنة عمان، والهيئة الوطنية للأمن السيبرانى بالمملكة العربية السعودية.

---

(1) ويعتبر المركز منصة مستقلة لتعزيز الحوار العالمي والتعاون بين الأطراف المعنية بالأمن السيبرانى فى سياق اهتماته بالثورة الصناعية الرابع وحوكمة التكنولوجيات البازغة، والقضايا ذات الصلة:
- https://www.weforum.org/

ويتبنى المركز العديد من الشراكات البحثية مع جامعات عالمية لتناول قضايا الأمن السيبرانى ومن بين تلك الشراكات برنامج عمل مشترك مع جامعة اكسفورد البريطانية: مدرسة أكسفورد مارتين (Oxford Martin School) لإصدار سلسلة تقارير ذات طابع مستقبلى حول الأمن السيبرانى (Cybercrime 2025).[1]

وعلى المستوى العربي يمكن رصد بعض الجهود والمبادرات الأهلية الهامة:

أ. **الإتحاد العربي للإنترنت والإتصالات**ARISPA: وهو منظمة عربية دولية غير ربحية تعمل فى اطار مجلس الوحدة الاقتصادية العربية وتأسست عام 2006 بمبادرة من شركات الإتصالات العربية. ويهدف الإتحاد لخلق تجمع مهنى عربى يدعم صناعة وتطوير الأعمال فى مجل تكنولوجيا المعلومات والإتصالات. وقد نظم الإتحاد مؤتمره الإقليمي الأول حول تطبيقات التحول الرقمى فى المنطقة العربية فى عام 2020 بمشاركة العديد من الخبراء فى مجال تكنولوجيا المعلومات والأمن السيبرانى.

ب. **الإتحاد العربي لتقنية المعلومات والإتصالات – البحرين:** وتأسس عام 2018 ويضم فى عضويته 9 دول عربية ويعمل على تعزيز العلاقات بين الشركات والمنظمات غير الربحية العربية الناشطة فى مجال تكنولوجيا المعلومات والإتصالات.

ت. **الإتحاد العربي لتكنولوجيا المعلومات:** وهو منظمة غير ربحية عربية تضم فى عضويتها 6 دول عربية، وتعمل على نشر الوعى المعلوماتى ودعم التعاون بين الشركات العربية المعنية بصناعة تكنولوجيا الإتصات والمعلومات.

[1] المصدر السابق - https://www.weforum.org/

المبحث الثانى

خبرات الأمن السيبرانى فى تجارب دول متقدمة وناهضة ونامية

تقدم خبرات التعامال مع الأمن السيبرانى فى تجارب دول العالم المختلفة خبرات هامة حول أفضل الممارسات فى إدارة وحوكمة الأمن السيبران التى يمكن تطويع بعضها والإنتفاع بها فى تطوير التجربة المصرية فى الأمن السيبرانى.

أولاً: تجربة الولايات المتحدة الأمريكية:

تعرضت الولايات المتحدة لهجمات سيبرانية منهجية منظمة للتجسس على، وسرقة أبحاث لقاحات COVID-19، وعلى مجموعة من الوزارات والشركات الأمريكية وصل عددها إلى 40 جهة فى ديسمبر 2020، وأشارت بعض التقارير إلى أن الهجمات المذكورة لم تكن من قراصنة أفراد ولكن من جانب أطراف وجهات تحركها دول: Nation-State actors. وفى هذا السياق، فقد تعرضت أكبر شبكة أنابيب لنقل الوقود فى الساحل الشرقى للبلاد لهجوم سيبرانى واسع فى مايو 2021 (كولونيال بايبلاين).

كما تمخضت أول قمة رئاسية بين الرئيس الأمريكى (جو بايدن) والرئيس الروسى (فلاديمير بوتين) فى يونيو 2021عن التوافق على بدء (مفاوضات سيبرانية) بين الطرفين فى أقرب فرصة.

وقد أولت الولايات المتحدة أهمية كبرى للأمن السيبرانى في سياق الأمن القومي الأمريكي من خلال (إستراتيجية الأمن القومي:National Security Strategy) التى أطلقت عام 2017 [1]. كما تمثل (الإستراتيجية الأمريكية للأمن السيبرانى: National Cyber Strategy) الصادرة عام 2018، وفق دونالد ترامب الرئيس الأمريكى حينها فى مقدمة الوثيقة، أول إستراتيجية متكاملة للأمن السيبرانى فى الولايات المتحدة عبر 15 عاماً.[2] وتعبر مكونات الوثيقتين بصورة أو أخرى عن التوجهات الرئيسية للدولة الأمريكية بخصوص التعامل مع قضايا الأمن السيبرانى، والتى نلقى الأضواء على بعضها على النحو التالى:

---

[1] يراجع للتفاصيل:

-The White House. (2017). National Security Strategy of the United States of America. Washington: The White House.pp.8-14.

[2] والتى تتناول قضايا الأمن السيبرانى الأمريكى بكافة جوانبها:

-The White House. (2018). National Cyber Strategy of the United States of America. Washington: The White House.pp.1-26.

1. الأمن السيبرانى جزء من منظومة الأمن الوطنى الأمريكى الشامل

حيث أصدرت الولايات المتحدة وثيقة للأمن الوطنى عام 2017، والتى سبقت الإشارة اليها، تضمنت جوانب متعددة للإهتمام بالأمن السيبرانى:

1.1. الأمن السيبرانى يمثل تحدياً استراتيجياً للولايات المتحدة الأمريكية

حيث تنطوى الهجمات السيبرانية الأرضية والجوية والفضائية على تحديات كبيرة للدولة الأمريكية خاصة فى تهديدها للمصالح السياسية والاقتصادية والأمنية بما فيها الديموقراطية، وتهديدها للبنى التحتية والشبكات والأنظمة التى تعتمد عليها الأجهزة الفيدرالية وقطاعات الأعمال والمواطن.

وقد تجلى ذلك بوضوح فى الأمر التنفيذى الذى أصدره الرئيس الأمريكى فى مايو من العام الحالى (2021/5/21) بعد تزايد الهجمات السيبرانية داخل البلاد، وقد أشار فيه بوضوح إلى مواجهة البلاد حملات إلكترونية خبيثة مستمرة ومتطورة بشكل متزايد تهدد القطاع العام والقطاع الخاص، وتهدد أمن وخصوصية الشعب الأمريكي، بما يستوجب قيام الحكومة الإتحاد ية بتحسين جهودها لتحديد وردع وحماية واكتشاف والإستجابة لهذه الإجراءات والجهات الفاعلة.[1]

1.2. تكلفة منخفضة لشن الهجمات السيبرانية وتكلفة فادحة لتداعياتها وأضرارها

وهو الأمر الذى يفرض على الأجهزة الأمريكية المعنية متابعة الأطراف المعنية بهذه الهجمات وردعها على نحو استباقى سواء داخل أو خارج الولايات المتحدة.

2. أبعاد متعددة للأمن السيبرانى فى الولايات المتحدة الأمريكية[2]

2.1. تعزيز الأمن السيبرانى يمثل دعم للشعب والوطن ونمط الحياة الأمريكى

حيث تستهدف الإستراتيجية حماية شبكات المعلومات العامة والخاصة والبنية التحتية المعلوماتية المرتبطة بحياة المواطنين وإستمرارية الأعمال ضد كافة أنواع الهجمات والجرائم السيبرانية. وفى هذا الخصوص فقد تم تأسيس (وكالة للأمن السيبرانى وأمن البنية التحتية–CISA) عام 2018، كوكالة فيدرالية مستقلة تحت اشراف وزارة الأمن الداخلى، وهناك أدوات متعددة للحوكمة وإدارة المخاطر السيبرانية على المستوى الوطنى من خلال:

---

[1] ويتناول الأمر التنفيذى تعزيز تبادل المعلومات بين الأجهزة المعنية، وتعزيز معايير أمن الأجهزة الحكومية، ومعايير توريد البرمجيات، وتعزيز مشاركات القطاع الخاص فى المواجهة السيبرانية، يراجع:

-Joseph R. Biden (2021). Executive order on improving the Nation's Cybersecurity. Washington. The White House.pp.1-6.

[2] يراجع لتفاصيل الأبعاد المذكورة، وثيقة استراتيجية الأمن السيبرانى

-The White House (2018). Op.cit. pp.6-17.

- **مسئوليات محورية للحكومة الفيدرالية**، خاصة ما يتعلق بحماية نظم المعلومات الفيدرالية والبنية التحتية التكنولوجية الوطنية الأكثر حيوية والأكثر انكشافاً. مع بلورة المعايير الخاصة بالأمن السيبرانى وإدارة المخاطر السيبرانية، وحماية ونشر الإنترنت الآمن الموثوق، بالإضافة إلى توزيع للمهام السيبرانية بين: وزارة الأمن الداخلى: DHS، ووزارة الدفاع:DoD، وأجهزة وأنظمة الإستخبارات المختلفة. كما تتضمن تلك المسئوليات تبنى ونشر أفضل الممارسات.
- **رفع قدرات إدارة المخاطر السيبرانية عبر الدولة**، من خلال تطوير التشريعات ذات الصلة، وإجراءات لتمكين أدوار مدراء نظم المعلومات فى الأجهزة المختلفة والقطاع الخاص بخصوص الأمن السيبرانى الإستباقى، ووضع أولويات لتنظيم مشتريات تكنولوجيا المعلومات، وأولويات أخرى لتأمين البيانات والمعلومات، وضمان التنسيق والتواصل وتبادل الخبرات حول إدارة المخاطر السيبرانية، ومخاطر سلاسل التوريد خاصة لتكنولوجيا المعلومات والإتصالات، ومخاطر خدمات المتعاقدين فى القطاعات المختلفة.
- **تحسين الإستثمار والبحوث والتطوير فى مجال الأمن السيبرانى**، من خلال التعاون الإيجابى مع شركات القطاع الخاص لتمويل بحوث استباق ودرء المخاطر السيبرانية من جهة، وتمويل فرص استثمارية فعالة فى هذا المجال من جهة أخرى. وتركيز البحوث والتطوير على استخدام التكنولوجيات البازغة لدعم الأمن السيبرانى وإدارة المخاطر السيبرانية.

2.2. <u>علاقة وثيقة بين الأمن السيبرانى والاقتصاد الرقمى الأمريكى،</u>

حيث تتوسع الرقمنة فى الاقتصاد الأمريكى فإن هناك حرص على تبنى الإجراءات والمعايير المناسبة التى تضمن التكيف الفعال للاقتصاد الرقمى مع الهجمات السيبرانية، والتعاون مع الشركات الكبرى والقطاع الخاص والأهلى لتطوير الإبتكارات الفعالة والتقنيات الآمنة لإمتصاص ومواجهة التهديدات السيبرانية. كما تتضمن الأولويات الحفاظ على التفوق الأمريكى فى الأجيال الجديدة من البنية التحتية والتقنيات البازغة، التدفق الآمن للبيانات عبر الحدود، دورة حياة الأمن السيبرانى، نظم حماية الملكية الفكرية، ومراجعة دورية لأنماط وأشكال الإستثمار فى الولايات المتحدة.

- **تنمية رأس مال بشرى متميز فى مجالات الأمن السيبرانى**، وتشمل التوجهات رعاية المواهب فى مجالات تعزز التنافسية الوطنية، التعليم الداعم وإعادة تطوير المهارات RE-SKILLING، التحفيز وتشجيع التميز فى مجال الأمن السيبرانى للكوادر البشرية المحترفة.

2.3. الدبلوماسية السيبرانية، وتعزيز التعاون والشراكات الإقليمية والعالمية للتعامل مع المخاطر السيبرانية

بما فيها هجمات الجريمة السيبرانية المنظمة العابرة للحدود، والأنشطة السيبرانية الإرهابية والتى يقف خلفها دول أو أطراف من غير الدول. والعمل على بناء وتعزيز تحالفات عالمية فعالة للتعامل مع المخاطر السيبرانية. وفى هذا الإطار تنوى الولايات المتحدة اصدار (قانون الدبلوماسية السيبرانية:Cyber Diplomacy Act)عام 2021، وتأسيس (مكتب للسياسات السيبرانية الدولية:Bureau of International Cyberspace Policy) بوزارة الخارجية الأمريكية ضمن نفس القانون.

ثانياً: تجربة كوريا الجنوبية:

تعرضت الدولة لهجمات سيبرانية شديدة عام 2013، واختراق مشغل الطاقة المائية والنووية عام 2014 وقد ترتب عليها العديد من الترتيبات المبكرة لدرء المخاطر السيبرانية على مستوى الدولة.ويتم استهداف الدولة بإعتبارها من أهم (الاقتصادات الرقمية) فى العالم، ومن المنتجين الكبار فى العالم لمنتجات وخدمات المعرفة والمعلومات (الحواسب، الإليكترونيات، ومنتجات الألياف الضوئية) بدعم من شركات كورية دولية مثل: Samsung+LG. كما توسعت تطبيقات واستخدامات تكنوجيا المعلومات والإتصالات بأشكالها فى كافة مناحى الحياة فى المجتمع الكورى خاصة بين الشباب.

1. أطر حوكمة الأمن السيبرانى فى الدولة[1]:

1.1. مرجعيات تشريعية وتخطيطية:

1.1.1. مرجعيات تشريعية

تشريع لحماية أمن الحاسب (1986)، وأسرار أمن الشبكات (1993)، أمن الإتصالات والمعلومات (2001)، والأعمال فى مجال الإتصالات (2008)، وحماية وسائط الإنترنت والوسائط الإعلامية المتعددة (2008)، تشريع التوقيع الرقمى (2009)، وحماية الأطفال من الإستغلال الجنسى (2009)، وعقوبات الجرائم الجنسية (2011)، وحماية خصوصية المعلومات الشخصية (2011). بالإضافة إلى تشريعات لحماية البطاقات الإئتمانية .

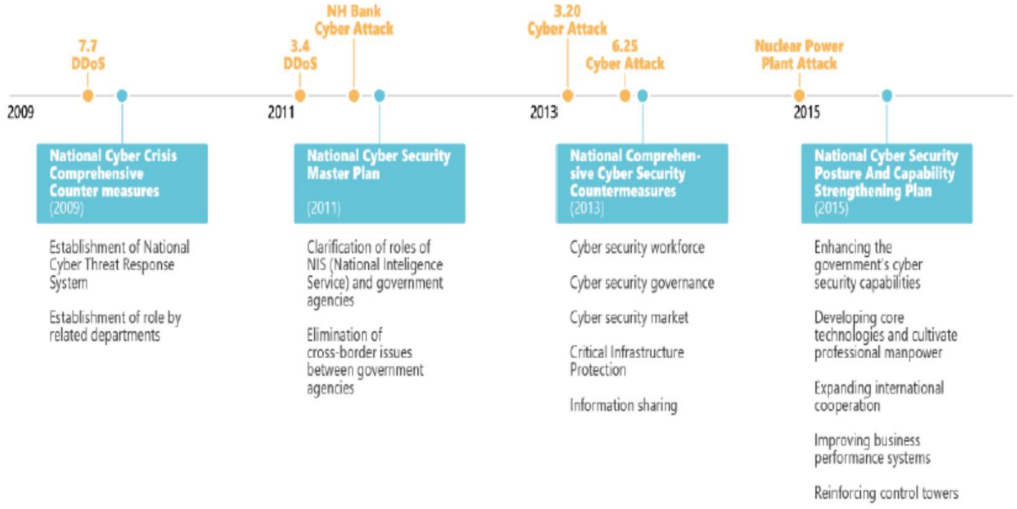
[1] للتفاصيل حول الأطر المؤسسية الفاعلة سيبرانياً ومهامها وتفاعلاتها، يراجع:
-Hannes Ebert and Laura Groenendaal (2020). Cyber resilience and diplomacy in the Republic of Korea: Prospects for EU cooperation. Brussels: EU Cyber Direct.pp:10-17.

1.1.2. أطر تخطيطية

- **مخطط رئيس للأمن السيبرانى الوطني**، وتم اطلاقه عام 2011 كرد فعل مباشر على هجمات واسعة لحجب الخدمات: DDos وهجمات بنكية أخرى، وقد حدد المخطط أدوار محددة لأجهزة المخابرات والوكالات المعنية الأخرى. كما تبنت نظم لإستباق واكتشاف الهجمات، مزيد من تدابير حماية البنية التحتية الحرجة، وتعزيز التعاون الدولي. وقد سبق هذا المخطط تبنى إجراءات وطنية للتعامل مع الأزمات السيبرانية عام 2009 تضمنت بناء نظام وطنى للإستجابة للتهديدات السيبرانية [1].
- **الإجراءات الوطنية الشاملة للأمن السيبرانى**، وتم اطلاقها عام 2013 لتركز على تعزيز تدابير حماية البنى الحرجة، وتنمية عمالة ماهرة فى مجال الأمن السيبرانى، وتفعيل تبادل المعلومات بين الأجهزة المعنية.

شكل (2-3)

أبرز السياسات الوطنية السيبرانية فى كوريا الجنوبية في الفترة (2009-2015)



Source: Hannes Ebert and Laura Groenendaal (2020). Cyber resilience and diplomacy in the Republic of Korea: Prospects for EU cooperation. Brussels: EU Cyber Direct.p.9.

1.1.3. أطر للحوكمة المؤسسية السيبرانية

- **آلية وطنية عليا للأمن الوطنى – مكتب الأمن الوطنى –NSO**، في رئاسة الدولة (البيت الأزرق) كمنصة عليا لمراقبة للأمن السيبراني في الدولة فى مواجهة أية هجمات، وتم تعزيز سلطات

[1]. لمزيد من التفاصيل، يراجع:

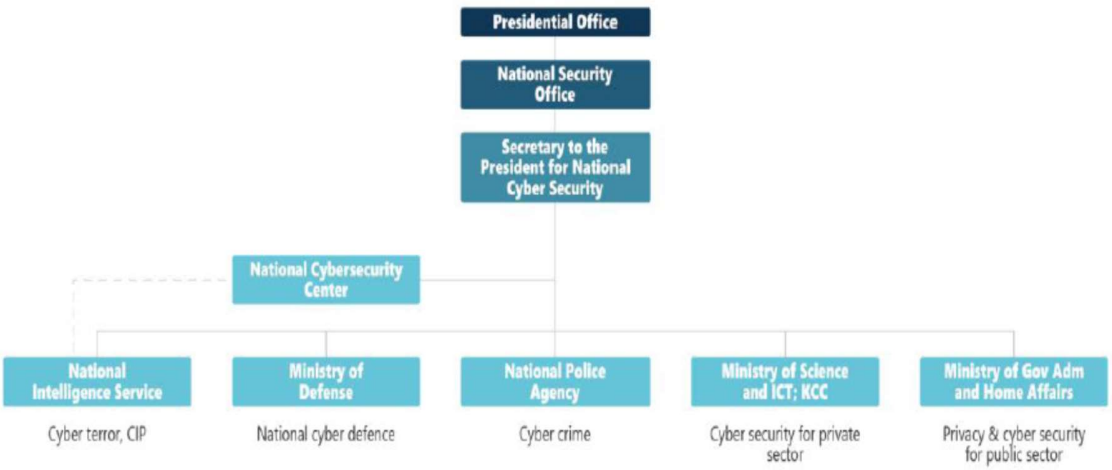
-National Cyber Security Master Plan -2011.pp1-4.

مراقبة الأمن السيبراني الخاصة لدى المكتب بعد تعرض محطة الطاقة المائية النووية لهجوم سيبرانى عام 2014، كما تم تعيين مفوض رئاسى للأمن السيبرانى داخل المكتب يشغله مسئول عسكرى أو استخباراتى.

- مركز وطنى للأمن السيبرانى – NCC، ويتولى العديد من المهام الرئيسية:
  - ضمان سلامة أمن الشبكات والنظم والبنى المعلوماتية الحرجة
  - تقديم الداعم الفنى للقطاع الخاص وتحفيزه على المشاركات السيبرانية مع القطاع العام
  - متابعة وتنفيذ (إستراتيجية الأمن السيبرانى الوطنية) والسياسات الأخرى ذات الصلة.
  - التعاون الخارجى فى مجال الأمن السيبرانى
- **المركز الكورى للإستجابة لطوارىء الحاسبات والشبكات** – KN:CERT، ويعتبر أحد الجهات التابعة للمركز الوطنى للأمن السيبرانى.
- **تواصل مكتب الأمن السيبرانى مع أجهزة الدولة**، ويتم دعم أنشطة المكتب من خلال: (جهاز المخابرات الوطنى –NIS) والمسئول عن الأنشطة الإرهابية، و(وزارة الدفاع –MND) المسئولة عن الدفاع السيبرانى الوطنى،و(هيئة الشرطة – NPA) المسئولة عن الجرائم السيبرانية، و(وزارة العلوم وتنولوجيا المعلومات والإتصالات – KCC) المسئولة عن الأمن السيبرانى فى قطاع الأعمال الخاص، و(وزارة الإدارة الحكومية والشئون الداخلية) المسئولة عن الخصوصية والأمن السيبرانى فى القطاع العام.

شكل (2-4)

الأطر المؤسسية لإدارة الأمن السيبرانى فى كوريا الجنوبية



Source: Hannes Ebert and Laura Groenendaal (2020). Cyber resilience and diplomacy in the Republic of Korea: Prospects for EU cooperation. Brussels: EU Cyber Direct.p:15.

3. **شراكات عالمية هامة فى إطار الدبوماسية السيبرانية– Cyber Diplomacy**

حيث يولى خبراء الدبلوماسية الكورية الجنوبية والخبراء الحكوميين المعنيين الآخرين أهمية خاصة للمشاركة في المناقشات العالمية المتعددة الأطراف بشأن انطباق القانون الدولي في الفضاء السيبراني، وتدابير بناء الثقة ، وبناء القدرات فى هذا الخصوص. وقد شاركت الدولة مؤخراً فى سبتمبر 2019، مع مجموعة من 27 دولة لمناقشة وإصدار بيان مشترك حول تعزيز سلوك الدول المسؤول في الفضاء الإلكتروني لتطوير إطار عالمى حاكم فى هذا الخصوص.

ثالثاً: تجربة الهند:

يعتبر قطاع تكنولوجيا المعلومات والإتصالات أحد القطاعات الرائدة والقائدة فى الهند خلال السنوات الماضية لآثاره الإيجابية العميقة الاقتصادية والإجتماعية فى الدولة حتى أصبحت الهند أحد القوى العالمية فى هذا المجال. وقد ذكرت دراسة مشتركة أجرتها شركة PwC India ومجلس أمن البيانات في الهند (DSCI) أن سوق الأمن السيبراني في الهند سيصل إلى 3.05 مليار دولار أمريكي بحلول عام 2022، بمعدل نمو سنوي مركب يبلغ 15.6٪، وهو ما يقرب من 1.5 ضعف معدل سوق الأمن السيبرانى العالمي[1].

فى المقابل، فقد ذكر بنك الاحتياطي الهندي (RBI) في تقريره السنوي للفترة 2019–2020 أن عمليات الاحتيال المصرفية قد قفزت بنسبة 28% مقابل عام 2018–2019. كما أشارت تحليلات لشركات متخصصة هندية في مارس 2020، أن الهند كانت مع الولايات المتحدة ضمن أكبر 5 دول فى العالم استهدافاً بالهجمات السيبرانية عام 2019 [2].

1. الأطر التشريعية والتخطيطية الرئيسية

1.1. أطر تشريعية

- **إطار تشريعى جامع – قانون تكنولوجيا المعلومات لعام 2000**، وينظم معظم قضايا المعلومات والإتصالات فى الدولة ومنها: الأمن السيبرانى، التوقيع الرقمي، الحكومة والحوكمة الإليكترونية،التجارة الإليكترونية، وحماية أصول البيانات الوطنية Assets Data.
- تشريع جديد تحت التطوير لحماية البيانات الشخصية.

---

(1) https://blog.eccu.edu/

(2) وأكدت وثائق وطنية تزايد كبير فى الهجمات السيبرانية التى تعرضت لها الدولة فى السنوات الأخيرة، يراجع :

- https://www.newdelhitimes.com/

-FTI Consulting and AMCHAM India. (2020). A white paper on India, s National Cybersecurity Strategy 2020.India.FTI. pp.5-13.

- **قواعد نوعية أخرى موازية وداعمة ذات صلة**، ومنها قواعد لبنك الإحتياط الهندى RBI، وقواعد تنظيم الإتصالات من السلطة المعنية بالإتصالات TRAI، وقواعد لأعمال البورصة وسوق المال، بالإضافة إلى قطاع التأمين.

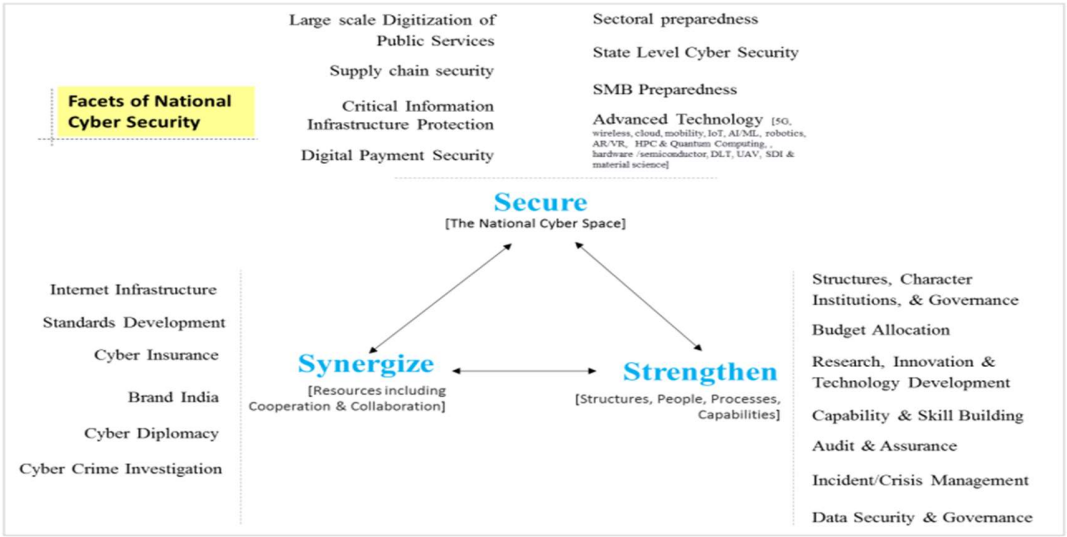
1.2. أطر تخطيطية

- **سياسة الأمن السيبرانى الوطنية عام 2013- NCSP**، وتنطلق من رؤية وطنية تسعى لبناء فضاء سيبرانى قوى وآمن للمواطنين، والأعمال، والحكومة.
- **توجهات لبناء إستراتيجية جديدة للأمن السيبرانى 2020**، حيث قام فريق استشارى متخصص: FTI، برصد الفجوات الهامة فى المحاور الرئيسية لسياسة الأمن السيبرانى 2013 والتى تشمل: الحوكمة، وبناء القدرات، والقابلية للتطبيق على القطاع الخاص، العلاقة مع البنية الحرجة للمعلومات، العمل مع مركز طوارىء الحاسبات، والعمل مع القطاع العام.

وبناء على تحليل الفجوات السابق، قدم الفريق الإستشارى العديد من التوصيات للأخذ بها فى الإستراتيجية الوطنية للأمن السيبرانى 2020-2025. وقد تم إعداد مسودة للإستراتيجية الوطنية للأمن السيبرانى فى الهند 2020 تركز على محاور ثلاثة: الفضاء السيبرانى الوطنى، تنسيق الجهود فيما يخص بنية الإنترنت والمعايير السيبرانية والدبلوماسية السيبرانية وتسويق الهند السيبرانية والجرائم السيبرانية. أما المحور الثالث فيتناول تعزيز القدرات والحوكمة والبحوث والإبتكار وإدارة الأزمات وتأمين البيانات، كما يوضحها شكل رقم (2-5).

شكل (2-5)

محاور الإستراتيجية المقترحة للأمن السيبرانى للهند 2020



Source: https://www.drishtiias.com/

2. أطر وأدوار مؤسسية رئيسة

رغم أحادية وعدم تعدد الأطر التشريعية ذات الصلة بالأمن السيبرانى فى الهند الا أن هناك العديد من الأطر المؤسسية ذات الصلة والتى تلعب أدواراً تخطيطية أو تنسيقية، أو للتدخل والدعم الفنى بخلاف مؤسسات الجريمة وانفاذ القانون والقوات المسلحة، كما يوضح الجدول التالى.

جدول (2-4)

الأطر المؤسسية الرئيسية المعنية بالأمن السيبرانى فى الهند

الأجهزة – المؤسسات	المهام الرئيسية
مكتب منسق الأمن السيبراني الوطني (NCSC)	• تأسس تحت إشراف سكرتارية أمانة مجلس الأمن القومي • ينسق مع كافة الأجهزة الحكومية والولايات والأقاليم الإتحاد ية، ووكالات إنفاذ القانون ذات الصلة عبر العالم فيما يخص الأمن السيبرانى.
المركز الوطنى لحماية البنية المعلوماتية الحرجة:NCIIPC	• الوكالة المخولة بحماية الأصول المعلوماتية الحرجة • ماعدا مايخص القوات المسلحة، وقليل من قطاعات إستراتيجية معينة
وزارة الإليكترونيات وتكنولوجيا المعلومات MeitY– قسم الأمن السيبرانى [1]،	• وضع قواعد حماية التطبيقات والبنة التحتية، بناء القدرات، • بلورة معايير وإجراءات منها قواعد شراء منتجات الأمن السيبرانى-2019
فريق الإستجابة لطوارئ الحاسبات CERT-IN	• تأسس في وزارة الإلكترونيات وتكنولوجيا المعلومات، • إصدار التنبيهات والإرشادات فيما يتعلق بالأحدث والتهديدات الإلكترونية والتدابير المضادة على نحو منتظم، • وضع المبادئ التوجيهية لتأمين البنية التحتية لتكنولوجيا المعلومات.
المركز الهندى للتنسيق بشأن الجرائم السيبرانية-14C	• يتبع وزارة الشئون الداخلية MHA، ويهتم بالجرائم السيبرانية • ينسق جهات العدالة والقانون ومختبر الطب الشرعى
وكالة الدفاع السيبرانى- DCA	• يتعاون مع مكتب منسق الأمن اليبرانى فيما يخص قضايا الأمن اليبرانى فى المجال العسكرى
هيئة الفضاء السيبرانى Cyberspace Agency	• جارى العمل على تأسيسها

Source: FTI Consulting and AMCHAM India. (2020). A white paper on India's National Cybersecurity Strategy 2020.India.FTI. p.12.

(1) يراجع موقع الوزارة والقسم:
https://www.meity.gov.in/cyber-security-division

رابعاً: تجربة دولة اسرائيل:

على غرار العديد من التجارب العالمية التى راعت الأبعاد الاقتصادية /الاجتماعية/الأمنية للأمن السيبرانى، وضعت حكومة إسرائيل رؤية على المستوى الكلى أن تكون الدولة رائدة في تسخير الفضاء الإلكتروني كمحرك للنمو الاقتصادي والرفاهية الاجتماعية والأمن القومي. من جهة أخرى فإن الدولة منخرطة فى (صراع سيبرانى) محتدم مع احدى القوى الإقليمية الفاعلة وهى ايران. وتوجد بالفعل نوع من الحرب السيبرانية غير المعلنة بين اسرائيل وايران كانت أحدث حلقاتها فى اتهام وزير الخارجية الإيرانى اسرائي بالهجوم السيبرانى على أنشطة تخصيب اليورانيوم وامدادات الطاقة الكهربائية فى منشأة (ناتنز –Natanz) النووية الإيرانية فى أبريل عام 2021.

1. الأطر التشريعية والقواعد الناظمة [1]:

- قانون الكمبيوتر الإسرائيلي 1995
- قانون حماية خصوصية البيانات 1981، وينطبق القانون على أي كيان يدير أو يمتلك قاعدة بيانات، بما في ذلك الكيانات الخاصة والعامة.
- قواعد لحماية البيانات عام 2018، وقانون حقوق النشر، وقانون العقوبات، وقانون مراقبة الصادرات الدفاعية لعام 2007،
- قانون تنظيم الأمن في الهيئات العامة (مقترح، ولكن لم يتم سنه بعد)
- مشروع قانون مقترح ومعدل لتعزيز القوة السيبرانية / الدفاع السيبرانى– مارس 2021.

1. الإطار الإستراتيجية والمؤسسية – إستراتيجية الأمن السيبراني القومي لإسرائيل:

وضعت اسرائيل إستراتيجية الأمن السيبراني القومي لإسرائيل، كوسيلة لتحقيق الرؤية السيبرانية الإسرائيلية لتكريس الحفاظ على أمن الفضاء الإلكتروني ومواجهة التهديدات السيبرانية المختلفة، بما يتوافق مع المصالح الوطنية للدولة، كما تسعى من خلال الإستراتيجية لتكون شريكاً فاعلاً في تشكيل الفضاء السيبراني. [2]

وتستند الإستراتيجية الاسرائيلية للامن السيبراني على مفهوم عام حول العمليات في مجال الامن السيبرانى، وتحدد الاطار المفاهيمي لكل جهود الدولة ووظائفها في اطار الأمن القومي السيبراني،

---

[1] لمزيد من التفاصيل، يراجع:

-Haim Ravia et.al. (2021). Cybersecurity 2021- Israel- Law and practice. /https://practiceguides.chambers.com Israel.

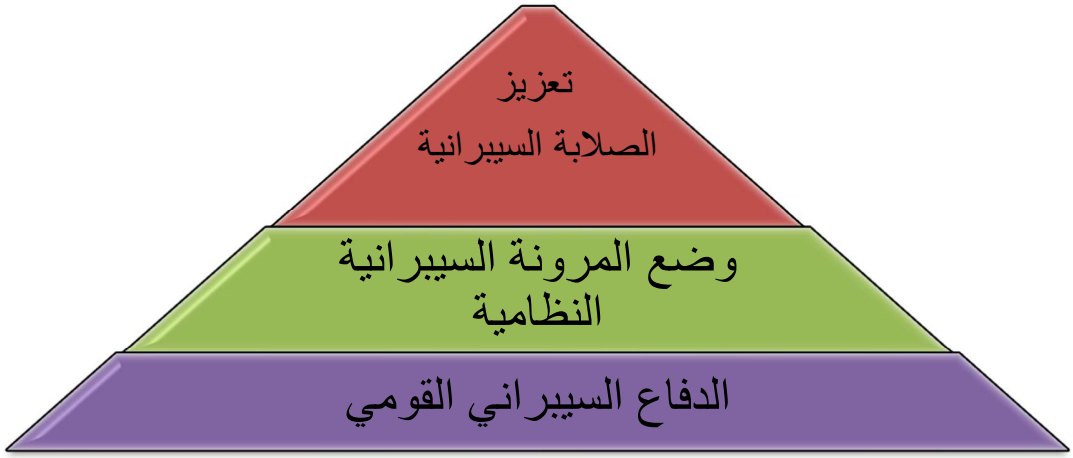
[2] Keith Breene, who are the cyberwar superpowers? The World Economic Forum , 04 May 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers, accessed on 09/01/2021.

ويشمل الاطار كل من الافعال المباشرة للدولة لمواجهة التهديدات السيبرانية، والجهود غير المباشرة الهادفة الي تشجيع ودعم التدابير الأمنية السيبرانية للقطاع الخاص والتي تتعاون معها. ويدور حول مفهوم العمليات ثلاثة طبقات تشغيلية:

- **تعزيز الصلابة السيبرانية – Cyber Resilience**، وتعتمد على قدرة المنظمات على مواجهة التهديدات اليبرانية وتقليل ودرء المخاطر السيبرانية.
- **وضع المرونة السيبرانية النظامية**، وتعنى القدرة السيبرانية الجماعية (بما فيها القطاعين العام والخاص وقدرات الإبتكار والتواصل مع العالم الخارجى) للتعامل الفعال قبل وأثناء وبعد حدوث المخاطر/ الهجمات السيبرانية، والتركيز على التواصل بين الأطراف وتبادل المعلومات فى إدارة هذه المخاطر.
- **الدفاع السيبراني القومي – National Cyber Defence**، ويتعامل مع التهديدات ضد الموارد أو المؤسسات والأصول الوطنية الإستراتيجية والتى تشكل تهديد للأمن القومى للدولة، بالتنسيق مع الجهود الدفاعية فى هذا الخصوص.

شكل (2-6)

مستويات العمليات فى مجال الأمن السيبرانى فى اسرائيل



Source: State of Israel Prime Minister Office((2017). National Cyber Directorate, Israel National Cyber Security in Brief.
https://www.gov.il/en/departments/units/israel_national_cyber_directorate_unit, accessed on 2/02/2021

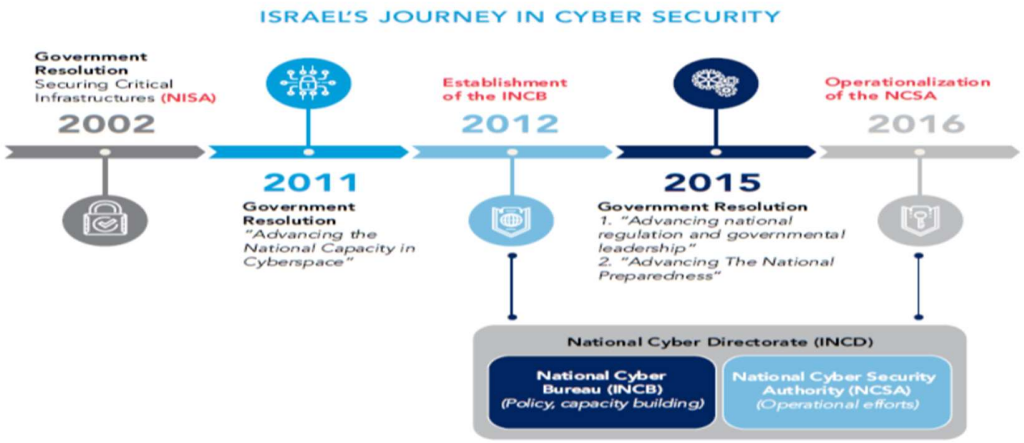
وقد مرت إستراتيجية الأمن السيبراني بإسرائيل بعدة مراحل رئيسة، كما يظهر في الشكل التالى حيث بدأ الاهتمام بالبنية التحتية للإتصالات والمعلومات مبكراً منذ عام 2002 بالتركيز على البنية

المعلوماتية الحرجة وشهدت هذه البداية تأسيس الهيئة القومية لأمن المعلومات NISA وقد تم تكليف الهيئة القومية لأمن المعلومات NISA لترشيد وحماية الأنظمة المحوسبة الحيوية لدى الأجهزة والمنظمات العامة والخاصة والمدنية. وقد ثم تطور الاهتمام فى عام 2011 بالتركيز على بناء قدرات بنية تحتية سيبرانية قوية، وأعقبها تأسيس الهيئة الوطنية للأمن السيبرانى INCP التى تتبع رئيس وزراء الدولة مباشرة.

كما حدث تحول نوعى فى الجهود الإسرائيلية عام 2015 بزيادة دور الحكومة فى ترتيب القواعد الناظمة لأمن المعلومات والأمن السيبرانى وتحسين الجاهزية الوطنية فى هذا الخصوص وإستكمال الأطر المؤسسية المسئولة عن إدارة الأمن السيبرانى فى الدولة [1]. وفى هذا الخصوص أصدرت الحكومة الاسرائيلية قرارين نتج عنهما الإستراتيجية القومية السيبرانية تم العمل عليها من جانب الهيئة، وأسفر عنها تأسيس السلطة القومية للأمن السيبراني NCSA. وتعتبر الهيئة الوطنية للأمن السيبراني: INCD مسئولة عن أنشطة الأمن السيبرانى فى الدولة، وأنشطة الطوارىء السيبرانية – CERT، ودعم الاقتصاد الرقمى، ودعم الأنشطة السيبرانية الدفاعية.

شكل (2-7)

مراحل تطور ومأسسة أنشطة وجهود الأمن السيبرانى فى إسرائيل



Source: Lior Tabansky, Israel Defence Forces and National Cyber Defense, https://connections-qj.org/article/israel-defense-forces-and-national-cyber-defense, accessed on 06/02/2021

(1) Lior Tabansky, Israel Defense Forces and National Cyber Defense, https://connections-qj.org/article/israel-defense-forces-and-national-cyber-defense, accessed on 06/02/2021

بالإضافة إلى ذلك، يتواجد قسم اشرافى سيبرانى فى بنك اسرائيل Bank of Israel مسئول عن انفاذ القواعد السيبرانية فى البنوك وشركات بطاقات الإئتمان، فى حين تخضع أسواق الأواق المالية وقطاع التأمين والمؤسسات المالية لقواعد سيبرانية ناظمة تضعها وزارة المالية.

2. <u>إهتمامات خاصة: بناء القدرات البحثية والبشرية، تنمية الأعمال والصادرات السيبرانية:</u>

2.1. <u>بناء قدرات البحث والتطوير والقدرات البشرية:</u>

كان هناك إدراك عبر مراحل مأسسة جهود الأمن السيبرانى بضرورة تدشين جهود موازية لدعم القدرات العلمية والتكنولوجية للدولة بوجه عام والقدرات السيبرانية الإبتكارية على وجه الخصوص بجانب تأهيل الكوادر البشرية الإحترافية، وتولت الهيئة الوطنية للأمن السيبران جنباً هاماً من المسئولية فى هذا الخصوص من خلال:

- **دعم البحث والتطوير لرفع قدرات وتكنولوجيات الأمن القومي،** بما فيها تأمين وتفعيل مشاركة المعلومات والحلول الداعمة لإستباق واحتواء الهجمات السيرانية وتقوية العمليات السيبرانية.
- **دعم الأنشطة البحثية التكنولوجية ذات الطابع السيبرانى وكوادرها البشرية،** بما فيها الصناعات الابتكارية، ودعم الأبحاث الأكاديمية ذات الصلة، وإنشاء مراكز بحثية فى الجامعات الكبرى لتنمية رأس المال البشرى والكوادر الإحترافية. وقد زاد عدد المتخصصين في مجالات الأمن السيبرانى الحربية وزادت المعاهد التى تركز على البحث والتنمية المعنى بالأمن السيبرانى Cyber Focused R&D Centers ويتم تشغيلها عبر شركات متعددة الجنسيات منها IBM اوركل وسيسكو وميكروسوفت وانتل وسيتي بنك وMcAfee وامازون[1].

2.2. <u>تطوير الأنشطة الاقتصادية الداعمة والمرتبطة</u>

بهدف تنمية اقتصاد للامن السيبراني وتعزيز فرص الدولة الاقتصادية فى هذا السياق، وتحفيز الشركات الاسرائيلية والشركات العملاقة والمراكز البحثية والأكاديمية والاكاديمين والمراكز المدنية والعسكرية ذات الصلة وأجهزة الأمن السيبرانى على تشبيك الجهود والتواصل مع العالم الخارجى بما يعزز فرص الدولة التنافسية الاقتصادية والعسكرية فى هذا الخصوص. وقد أثمرت هذه الجهود عن بعض النتائج، حيث بلغت نسبة مشاركة اسرائيل في سوق الأمن السيبراني العالمي حوالي 5% على

[1] Ministry of Economic and Industry, How Israel Became a Cybersecurity Superpower, https://itrade.gov.il/Netherlands/how-israel-became-cybersecurity-superpower/, accessed on 24/01/2021.

الرغم أن سكانها لا يتجاوز 0.1% من سكان العالم، كما تبلغ نسبة الاستثمارات للشركات الاسرائيلية العاملة في اسرائيل فى مجال الامن السيبراني حوالي 815 مليون دولار وفقاً لتقديرات عام 2017.
ومن ضمن الأنشطة التى ازدهرت فى هذا السياق، صناعة السيارات المرتبطة بالانترنت Connected cars فهي سيارات تتضمن اكثر من 100 مليون خط من الاكواد لحماية العجلات والركاب وتعمل عليها شركة Argus للأمن السيبراني كما قدمت الشركة أيضا حلول في مجال الأمن السيبراني في صناعة الطيران.
كما تضاعفت جهود ومشروعات حماية البنية التحتية النقدية وحماية المنتجات الأمنية السيبرانية ومحطات المياه، ونظم السكة الحديد. ومن أبرز الشركات الاسرائيلية العاملة Radiflow التي تطور نظم التحكم الصناعي والتحكم الإشرافي والتحقق من البيانات SCADA لاستخدامات الطاقة والبترول والغاز والمياه. وفي اغسطس 2018 أطلقت وزارة الاقتصاد والصناعة وإدارة الامن السيبراني 90 مليون برنامج لمدة ثلاثة سنوات لإبتكارات الامن السيبراني في مجال البحث والتطوير للمشروعات الصغيرة -JUMP START، وتمويل مشروعات تجريبية. [1]
ويوضح الشكل التالي الذي نشره صندوق Glilot Capital Investment وIVC، لتحليل المعلومات التجارية في صناعة التكنولوجيا الفائقة، خريطة لشركات الإنترنت الإسرائيلية الخاصة في عام 2021. وتضم الخريطة أكثر من 120 شركة سيبرانية خاصة في الدولة، مقسمة إلى 14 مجال خبرة، بما في ذلك الحماية السحابية، وأمن الإنترنت والبريد الإلكتروني، وإنترنت الأشياء، والتجزئة الداخلية في خوادم حوسبية، وblockchain، وحماية الخصوصية، والذكاء، وأمن التطبيقات، تحديد وإدارة الوصول، تحليل ضعف النظام وغيرها من التطبيقات.[2]

2.3. <u>التعاون الدولي</u>

حيث تعتبر اسرائيل مشتركة في جهود للمساعدة في الفضاء السيبرانى بشكل آمن وتحرير النطاق السيبراني لتقوية الأمن السيراني القومي كمكون تكميلي لجهودها القومي في مجال الأمن السيبرانى.

---

(1) Ministry of Economic and Industry, How Israel Became a Cybersecurity Superpower, https://itrade.gov.il/Netherlands/how-israel-became-cybersecurity-superpower/, accessed on 24/01/2021

(2) Jewish Business News, Israeli Superpower: See Map of More Than 120 Largest Cyber Companies In 2021, 07/02/2021, https://jewishbusinessnews.com/2021/02/07/israeli-superpower-see-map-of-more-than-120-largest-cyber-companies-in-2021/, accessed on 07/02/2021

وقامت اسرائيل بدعوة شركاء دخول العالم للعمل معا للمشاركة في المعرفة وتطوير الحلول الجديدة للمستوي الطوني لتنفيذ الرؤية المنظورة لتأمين فضاء سيبرانى افتراضي مزدهر[1].

وتبقى عدة ملاحظات على التجربة السيبرانية الإسرائيلية:

- **غلبة الطابع السري على المقدرات السيبرانية لإسرائيل،** يعتبر مؤشر بلفر للقوة السيبرانية الوطنية لعام 2020 أن أسرائيل قد تكون تمتلك قدرات سيبرانية أعلى من المنشورة ولكنها تفضل اخفاء معالم ومقدرات هذه القوة، ويعتبر التقرير أيضاً أن أسرائيل قد تكون من ضمن الدول التي لها نوايا خفية خلاف المنشورة خارجياً سواء كان الأمر يتعلق بالإرادة السياسية أو تسخير الموارد الوطنية للدولة لتحقيق هدف معين.[(2)]
- **مساهمات كبيرة فى السوق العالمي السيبرانى الاقتصادى،** حيث تساهم إسرائيل كقوى سيبرانية بنحو 10٪ من المبيعات العالمية لتكنولوجيا أمن الكمبيوتر والشبكات، وهو الأمر الذي يعكس المكانة المميزة لإسرائيل كقوة كبيرة في المجال السيبراني[(3)].

خامساً: خبرات أخرى من الدول المتقدمة والناهضة والنامية:

يقدم الجدول التالى خبرات لدول أخرى متقدمة وناهضة ونامية قام فريق العمل بتجميعها من واقع العديد من الدراسات التى تم تحليلها وفحصها وإختيار أفضل الممارسات من خلالها.

جدول (2-5)

خبرات وتوجهات الأمن السيبرانى فى بعض دول العالم

الدولة	الخبرات والتوجهات
المملكة المتحدة	• يقدم المركز الوطني للأمن السيبراني(NCSC) ، وهو منظمة تابعة لحكومة المملكة المتحدة، المشورة والدعم للقطاعين العام والخاص لتجنب تهديدات الأمن السيبراني. • للتخفيف من انتهاكات البيانات والأمن، يوصي NCSC بثلاث مجموعات إرشادات:

(1) State of Israel Prime Minister Office: **Op.cit**

(2) Julia Voo et.al. (2020), National Cyber Power Index 2020 Methodology and Analytical Considerations, China Cyber Policy Initiative, Belfer Center for science and International Affairs, Harvard Kennedy School, Sept., https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf, accessed on 09/01/2020

(3) Keith Breene, who are the cyberwar superpowers? The World Economic Forum, 04 May 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers, accessed on 09/01/2021

الدولة	الخبرات والتوجهات
	حماية نقاط النهاية، حماية الشبكات، حماية المعلومات. • تأسيس القوة السيبرانية الوطنية National Cyber Force– أبريل 2020، كجهاز تابع للمخابرات البريطانية بهدف تعزيز الدفاع السيبرانى للدولة.
ألمانيا	• يقترح المكتب الفيدرالي لأمن المعلومات في ألمانيا تعزيز الفرص القانونية والتقنية والشخصية لتشكيل الرقمنة بنظام أمان آمن. والمبادئ التوجيهية الأساسية تشمل: 1. يجب تشفير الإتصالات الإلكترونية باستخدام نظام مصادقة مزدوج، 2. تجنب إدخال كلمة المرور في صفحات الويب المرتبطة بالبريد الإلكتروني، 3. إظهار رسائل البريد الإلكتروني المشبوهة إلى مسؤول تكنولوجيا المعلومات، 4. تغيير كلمة المرور سريعًا على الصفحة الأصلية إذا دخلت إلى صفحة ويب غير موثوقة 5. تدريب الموظفين على تحديد الإتصالات الإلكترونية الاحتيالية والمتلاعبة، 6. جعل التشفير بروتوكولات خالية من الثغرات الأمنية، 7. تكوين أجهزة التوجيه المنزلية والمكتبية لمنع أي دخول غير مصرح به إلى أجهزة الشبكة **8.** تكوين الجهاز المتصل لطلب الموافقة على الاتصال عبر الإنترنت
الصين	• ينص قانون الأمن السيبراني في الصين على: 1. الأفراد والمنظمات – المسؤولون عن شبكاتهم – لا يجوز لهم إنشاء مواقع ويب أو مجموعات اتصالات لأغراض احتيالية أو أنشطة غير قانونية أخرى، 2. حماية البنية التحتية للمعلومات الحيوية في الإتصالات العامة، خدمات المعلومات، والبنية التحتية الإلكترونية الحيوية، 3. يجب أن تحصل على موافقة من المستخدمين أثناء جمع معلوماتهم الشخصية
اليابان	• يضع مجلس الأمن القومي (NSC) في اليابان – وهو هيئة مشتركة بين الوكالات تنسق سياسات الأمن السيبراني الوطنية – سياسات إلكترونية أوسع لليابان. وتشمل هذه: 1. التدفق الحر للمعلومات في الفضاء السيبراني، 2. تطبيق القوانين السيبرانية لتطوير مجتمع معلومات مترابط ومتقارب، **3.** رؤية مشتركة للأمن السيبراني ومشاركة المسؤولية من قبل جميع أصحاب المصلحة
ماليزيا	• تقدم الوكالة الوطنية للأمن السيبراني في إرشادات وخدمات للسلطات والمؤسسات الأخرى لتطوير بنية تحتية إلكترونية مرنة وإطار عمل لإدارة المخاطر للكيانات المكونة.

الدولة	الخبرات والتوجهات
	• على سبيل المثال، باتباع الإرشادات الوطنية، تقوم لجان الأوراق المالية في ماليزيا (SCM)وبنك نيجارا ماليزيا (BNM) بتطوير إرشاداتها للشركات والبنوك المدرجة مثل: 1. يوفر مجلس الإدارة الإشراف والموارد الكافية لإدارة مخاطر الأمن السيبراني. 2. يجب على مجلس الإدارة مناقشة سياسات وإجراءات إدارة المخاطر الإلكترونية. 3. يشرف مجلس الإدارة على تنفيذ السياسات والإجراءات المعتمدة بشكل مناسب، 4. مراجعة وتنقيح سياسات وإجراءات المخاطر الإلكترونية فى ضوء مستويات المخاطر
بنغلاديش	• توفر الإستراتيجية الوطنية للأمن السيبراني في بنغلاديش (NCSB) إرشادات لإدارة المخاطر السيبرانية وفق مقترحات الإتحاد الدولي للاتصالات (ITU)، وتشمل: 1. وضع تشريعات وطنية شاملة للجرائم الإلكترونية، 2. اتخاذ التدابير المناسبة للحد من نقاط ضعف النظام السيبرانى الوطنى، 3. زيادة الوعي الأمني باستخدام الخدمات القائمة على تكنولوجيا المعلومات، 4. تطوير التعاون الدولي بشأن التهديدات والحلول الإلكترونية، **5.** تعزيز البنية التحتية الإلكترونية الآمنة والمرنة للاقتصاد والمجتمع

المصدر: مركب بمعرفة فريق العمل من مصادر الدراسة المختلفة.

المبحث الثالث

خبرات التعامل مع الأمن السيبرانى فى تجارب دول عربية

تقدم العديد من الدول العربية خبرات جديرة بالتحليل من وقع تعاملها مع قضايا الأمن السيبرانى المختلفة، وسوف يلقى المبحث الحالى الأضواء على ثلاثة تجارب عربية بارز للدول العربية التى تحقق مواقع متقدمة على المؤشرات العالمية الرئيسية للأمن السيبرانى وتكنولوجيا المعلومات والإتصالات، وهى: المملكة العربية السعودية، سلطنة عمان، ودولة الإمارات العربية.

أولاً: تجربة المملكة العربية السعودية [1]

حققت المملكة العربية السعودية قفزة نوعية هامة بإحتلالها المركز الثانى عالمياً على مؤشر الأمن السيبرانى العالمي:GCI لعام 2020 مقابل المركز 46 عالمياً على نفس المؤشر لعام 2017، كما تصدرت المملكة المركز الأول على قارة آسيا والأول عربياً على المؤشر المذكور.

وتتميز التجربة السعودية بالعديد من الخصوصيات ذات الأبعاد الوطنية والإقليمية ، وكذلك العالمية المرتبطة بعضوية السعودية فى مجموعة العشرين: G20.

كما تأتى خصوصية تجربة المملكة من تعرضها للعديد من الهجمات السيبرانية خاصة الهجمات السيبرانية على شركة ارامكو عام 2012 وعامى 2016 -2017، كما تعرضت الشركات السعودية لهجمات سيبرانية.

1. الخصوصيات الوطنية للتجربة السعودية فى مجال الأمن السيبرانى:

يلقى الجدول رقم (2-6) بعض الأضواء على ملامح التجربة السعودية فى التعاطى مع قضايا الأمن السيبرانى من خلال أطر للحوكمة التشريعية والمؤسسية والإجرائية.

---

[1] يعتمد العرض على مجموعة وثائق ومصادر هامة، من أبرزها:

- الهيئة الوطنية للأمن السيبرانى (2020). الإستراتيجية الوطنية للأمن السيبرانى:نظرة عامة. الرياض: الهيئة
- الهيئة الوطنية للأمن السيبرانى (2020). ضوابط الأمن السيبرانى للعمل عنبعد. الرياض: الهيئة.

جدول (2-6)

عناصر حوكمة وإدارة الأمن السيبرانى فى المملكة العربية السعودية

عناصر الحوكمة والإدارة السيبرانية	إضاءات حول عناصر حوكمة وإدارة الأمن السيبرانى
تشريعات	- قانون الجرائم الإليكترونية عام 2017. - قانون التجارة الإليكترونية عام 2018.
إستراتيجية وطنية للأمن السيبرانى	- اطلاق الإستراتيجية الوطنية للأمن السيبرانى عام 2020. - تهدف لتحقيق رؤية الأمن السيبرانى فى المملكة: (فضاء سيبرانى سعودى آمن وموثوق ويمكن النمو والإزدهار).
مؤسسات رئيسة	- تأسيس هيئة الإتصالات السعودية عام 2001، وتحولت إلى هيئة الإتصالات وتقنية المعلومات عام 2003. - تأسيس الهيئة الوطنية للأمن السيبرانى عام 2017 – ويتبع لها المركز الوطنى الإرشادى للأمن السيبرانى: SAUDI CERT.
ضوابط ومعايير	- وضعت الهيئة 114 من الضوابط والمعايير موزعة على خمسة مجموعات:حوكمة الأمن السيبرانى، تعزيز الأمن السيبرانى،صمود الأمن السيبرانى،الأمن السيبرنى والحوسبة السحابية، الأمن السيبرانى لأنظمة التحكم الصناعى. - وضعت الهيئة ضوابط للعمل عن بعد (مرتبطة بجائحة كورونا: COVID19)
مبادرات	- الإتحاد السعودى للأمن السيبرانى والبرمجة والدرونز، الأكاديمية الوطنية للأمن السيبرانى،مبادرة حصين للأمن السيبرانى، حماية الأطفال فى الفضاء السيبرانى، وحماية المرأة فى الفضاء السيبرانى.

المصدر: مركب بمعرفة الفريق البحثى من مصادر ومواقع سعودية متفرقة – قائمة المصادر.

وتتميز الإستراتيجية الوطنية للأمن السيبرانى فى المملكة بإرتباطها بصورة مباشرة برؤية المملكة 230 لدعم الوطن، والاقتصاد الرقمى، والتمكين الرقمى للمواطنين،كما يوضح شكل رقم (2-8).

شكل (2-8)

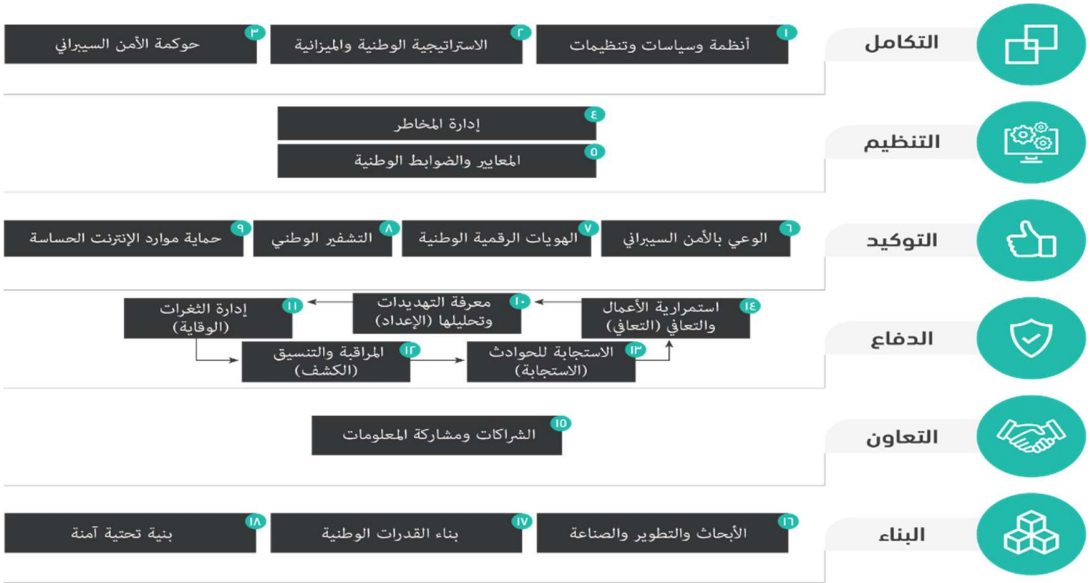
ربط استراتيجية الأمن السيبرانى بالرؤية الإستراتيجية للمملكة 2030

المصدر: الهيئة الوطنية للأمن السيبرانى(2020).الإستراتيجية الوطنية للأمن السيبرانى:نظرة عامة.الرياض: الهيئة.ص18

كما يوضح الشكل رقم 2-9 العناصر الستة الرئيسية والعناصر الفرعية التابعة (18 عنصراً) التى تشكل الإطار المرجعى للإستراتيجية الوطنية للأمن السيبرانى فى المملكة.

شكل (2-9)

الإطار المرجعى للإستراتيجية الوطنية للأمن السيبرانى بالمملكة العربية السعودية



المصدر:الهيئة الوطنية للأمن السيبرانى(2020).الإستراتيجية الوطنية للأمن السيبرانى:نظرة عامة.الرياض: الهيئة.ص22

2. <u>خصوصيات ومبادرات عالمية للتجربة السعودية فى مجال الأمن السيبرانى:</u>

- **المنتدى الدولي للأمن السيبرانى – الرياض فبراير 2020:** بمشاركة حوالى 1000 شخصية من صناع القرار والخبراء وقيادات الشركات. وناقش المنتدى قضايا هامة متعددة منها:

أ. هل هناك فرص اقتصادية استثمارية في الأمن السيبرانى

ب. صناعة وتعزيز الأمن السيبرانى

ت. مواجهة مخاطر الأمن السيبرانى

ث. التوعية بمخاطر الأمن السيبرانى

ج. إهتمام خاص بالمرأة والطفل في قضايا الأمن السيبرانى

ح. مجالات التعاون الدولي لتعزيز الأمن السيبرانى

خ. بناء وتطوير القدرات ذات الصلة

د. خارطة طريق للقرن 21

كما ناقش المنتدى فى جلسات خاصة أهم التحديات السيبرانية وسبل مواجهتها فى بعض القطاعات الرئيسية وعمن أبرزها: الطاقة والخدمات، الخدمات المالية،المدن الذكية، الإتصالات، الصحة والرعاية الصحية، بالإضافة إلى المرأة فى الأمن السيبرانى.

- الإجتماع الإستثنائى لوزراء الاقتصاد الرقمى بمجموعة العشرين – الرياض: مايو 2020 وقد أكد البيان الختامى للإجتماع على مجموعة من القضايا الهامة التى تربط بصورة مباشرة بين قضايا التحول لرقمى والأمن السيبرانى خاصة فى مواجهة تداعيات جائحة كورونا وغيرها من التحديات فى دول المجموعة والعالم:

أ. البنية التحتية للإتصالات والربط الشبكى

ب. تبادل البيانات بطريقة آمنة

ت. إجراء البحوث وتطوير التقنيات الرقمية فى مجال الصحة

ث. استخدام الحلول والتقنيات الرقمية لدى الشركات والأفراد والمؤسسات

ج. بيئة موثوقة وآمنة عبر شبكة الإنترنت، ومواجهة التهديدات والمخاطر السيبرانية

ح. مرونة الأعمال – بما فيها الصغيرة والمتوسطة وريادة الأعمال وتمكين المرأة

خ. **خطوات مقبلة:** تنسيق سياسات الاقتصاد الرقمى، تبادل الخبرات وأفضل الممارسات،تطوير الإبتكارات الرقمية ودعم الدول النامية فى مواجهة كورونا وغيرها.

ثانياً: تجربة سلطنة عمان:

جاءت سلطنة عمان فى المركز الثانى عربياً بعد المملكة العربية السعودية على مؤشر الأمن السيبرانى العالمي لعام 2018 للإتحاد الدولي للإتصالات، وتتميز تجربتها بخصوصيات عديدة.

1. خصوصيات وطنية للتجربة العمانية فى مجال الأمن السيبرانى:

1.1. أطر تشريعية هامة ذات صلة:

- قانون المعاملات الإليكترونية عام 2008
- قانون الجرائم الإليكترونية عام 2011
- قانون تنظيم الخدمات البريدية عام 2012.

1.2. أطر مؤسسية هامة ذات صلة:

- **وزارة التقنية والإتصالات**، وتاسست عام 2019، وآلت إليها اختصاصات هيئة تقنية المعلومات السابقة، واختصاصات الأجهزة الأخرى المتعلقة بالسياسات والتشريعات لقطاع الإتصالات، وبرامج التقنية الخاصة بتوطين تقنيات الثورة الصناعية الرابعة.
- **المركز الوطني للسلامة المعلوماتية**، وتأسس عام 2010، والذى يعد أحد مبادرات عمان الرقمية، ويسعى المركز إلى تحقيق الأهداف التالية:
  - أ. توفير بيئة معلوماتية آمنة عند استخدام الخدمات الالكترونية الحكومية.
  - ب. بناء القدرات وتشجيع الكوادر البشرية للعمل في قطاع أمن المعلومات بالسلطنة.
  - ت. الإستجابة لأية حوادث أمنية ومحاولة الحد من أثارها.
  - ث. نشر الوعي حول أهمية أمن المعلومات بين أفراد المجتمع العماني
- **المختبر الوطني للأدلة الرقمي**، ويتعامل مع الأدلة الرقمية التي يتم اكتشافها من الجرائم الالكترونية وتقديمها للعدالة لتطبيق القانون، كذلك خدمات العثور على الأدلة الرقمية في أجهزة الكمبيوتر والهواتف واستعادة بياناتها، ويسعى لإعتماد دولي للمختبر وخدماته.

وقد أشار التقرير السنوى لعام 2019 لوزارة التقنية والإتصالات [1]، إلى أن المركز الوطني للسلامة المعلوماتية قد تعامل مع 11.435.596محاولة اختراق مشبوه، و64 برنامج تجسس، بخلاف 25.256 فيروس تم اكتشافها والتعامل معها وتحليلها، بالإضافة إلى 332 حادثة أمنية سيبرانية تم اكتشافها ومعالجتها، كما يوضح شكل رقم (2-10).

---

(1) لمزيد من التفاصيل حول القضايا السيبرانية فى التقرير، يراجع
وزارة التقنية والإتصالات (2019). التقرير السنوى 2019م.مسقط: وزارة التقنية والإتصالات.ص.25-33

شكل (2-10)

أعمال قطاع أمن المعلومات والمركز الوطنى للسلامة المعلوماتية بعمان 2019

المصدر: وزارة التقنية والإتصالات(2019). التقرير السنوى 2019م.مسقط: وزارة التقنية والإتصالات.صص.26-27.

1.3. خصوصيات إقليمية للتجربة العمانية فى مجال الأمن السيبرانى:

فقد تم تأسيس (المركز العربي الإقليمي للأمن السيبرانى- ITU-ARCC) من جانب الإتحاد الدولي للإتصالات ITU وسلطنة عمان تماشياً مع أهداف الأجندة العالمية للأمن السيبراني للإتحاد الدولي للإتصالات، وبدأ المركز نشاطه عام 2013. ويهدف المركز لدعم بناء الثقة والأمن في إستخدام تكنولوجيا المعلومات والإتصالات وتنسيق مبادرات الأمن السيبراني في المنطقه العربيه، ويتم استضافة وإدارة وتشغيل المركز الإقليمي للأمن السيبرانى من جانب (المركز الوطني للسلامة المعلوماتيه بسلطنة عمان: OCERT)، وأهم أهداف المركز [1].

أ. الإشراف على تنفيذ برنامج الأمن السيبراني للإتحاد الدولي للاتصالات في المنطقة العربية.

ب. أن يكون مركزا للإدارة ومنصة لتنفيذ أهداف الأمن السيبرانى فى المنطقة العربية

---

[1] للتفاصيل، يراجع موقع المركز - https://arcc.om/

ت. وضع الأطر والخطط في مجال الامن السيبراني من خلال الدراسات الإقليمية وعقد ورش العمل، ورفع مستوى الوعي والخبرات في الأمن السيبراني والبنية التحتية للمعلومات.

ث. الإستجابة لمتطلبات الأمن السيبراني لأحدث التطورات.

ج. توفير مركز موحد للدول الأعضاء لإدارة برامج مبادرات الأمن السيبراني المشتركة.

ويوضح الشكل رقم 2-11 ، أن أنشطة المركز يغطى إلى حد كبير كافة الدول العربية ومن بينها مصر، وقد نظم المركز بالتعاون مع الإتحاد الدولي للإتصالات الأسبوع الإقليمي للأمن السيبرانى فى مسقط فى اكتوبر عام 2019.

شكل (2-11)

الدول العربية المشمولة بأنشطة المركز العربي الإقليمي للأمن السيبرانى

المصدر: موقع المركز العربي الإقليمي للأمن السيبرانى: https://arcc.om/

نتائج الفصل الثاني

- **دور محورى للأمم المتحدة ووكالاتها المتخصصة فى الأمن السيبرانى،** وعلى الأخص من خلال آليات متابعة تنفيذ مقررات القمم العالمية لمجتمع المعلومات والمعنية بالتعامل مع مخاطر أمن المعلومات، وتشكيل فرق عمل وطنية للإستجابة للحوادث السيبرانية.
- **أولويات أممية لحوكمة مخاطر الإنترنت والتكنولوجيات البازغة لدعم التنمية المستدامة،** ويبرز فى هذا الخصوص مؤتمرات الذكاء الإصطناعى للصالح العام AI 4 GOOD بين عامى 2017–2019 والشراكة العالمية لتفعيل دور تكنولوجيا المعلومات والإتصالات فى التنمية المستدامة.
- **أدوار رائدة للإتحاد الدولي للإتصالات: ITU،** فى مجالات خطط وإستراتيجيات الأمن السيبرانى، المؤشرات والإحصاءات، التعامل السيبرانى مع جائحة كورونا، والحماية السيبرانية للمرأة والشباب والطفل، بخلاف المبادرات السيبرانية الإقليمية .
- **مبادرات أمنية سيبرانية إستراتيجية – دور حلف شمال الأطلنطى NATO،**بتكريس منظومات الدفاع السيبرانى جزء لا يتجزء من المنظومات الدفاعية للحلف وللدول الأعضاء على السواء.
- **مبادرات سيبرانية إقليمية أوروبية،** ومنها تأسيس وكالة أوروبية للأمن السيبرانى: **ENISA،** وإستراتيجية أوروبية للبيانات 2020، ومعايير سيبرانية للجيل الخامس– 2021G5.
- **توجهات سيبرانية إقليمية أفريقية غير كافية،** ضمن أجندة أفريقيا للتنمية المستدامة: 2063، واتفاقية(مالاو) بين 2011–2020 للأمن السيبرانى وحماية البيانات الشخصية، وفريق خبراء سيبرانى للإتحاد الأفريقى 2018،وإستراتيجية أفريقية للتحول الرقمى 2020.
- **مبادرات عربية سيبرانية غير كافية،** منها جهود لصياغة إطار عربى استشرشادى للأمن السيبرانى، الإتفاقية العربية لمكافحة جرائم تقنية المعلومات،وتأسيس المركز العربي الإقليمي للأمن السيبرانى فى سلطنة عمان 2013 بالتعاون مع الإتحاد الدولي للإتصالات.
- **اسهامات موازية للجماعات العلمية فى العالم ومصر لدعم الأمن السيبرانى،** تم نشر 4830 بحثاً يتناول قضايا الأمن السيبرانى 2015–2020 مع تصدر للولايات المتحدة، وحوالى 16 مساهمة مصرية، كما صدر كتاب دولى حول القضايا بمحررن مصريين 2019.

- **دور مراكز الفكر ومنظمات الأعمال فى التوعية ودعم الأمن السيبرانى**، خاصة دور المنتدى الاقتصادى العالمي WEF بتاسيسه مركز متخصص للأمن السيبرانى ليقود أنشطة متنوعة، وأدوار لشركات عالمية متعددة من بينها: IBM. وعلى المستوى العربي هناك أدوار للإتحاد العربي للإنترنت والإتصالات:ARISPA، والإتحاد العربي لتقنية المعلومات والإتصالات.
- **ملامح هامة فى التجربة الأمريكية**، الربط بين الأمن الوطنى والسيبرانى استراتيجياً مع دور فيدرالى حاكم للدولة،الأمن السيبرانى يدعم منظومة الحياة والقيم الأمريكية، بناء قدرات البحوث والتطوير والكوادر البشرية المساندة،تنمية الاقتصاد الرقمى، والدبلوماسية السيبرانية.
- **خبرات سيبرانية كورية جنوبية**، تشريعات متعددة تشمل الإستغلال الجنسى وحماية الأطفال،مخطط رئيس وسياسات وطنية مصاحبة، أطر للحوكمة المؤسسية السيبرانية تبدأ من رئاسة الدولة، تنمية الاقتصاد الرقمى والبنية التحتية الرقمية والدبلوماسية السيبرانية.
- **ملامح هامة للتجربة الهندية**، الدور الحاكم لقطاع تكنولوجيا المعلومات والإتصالات فى التنمية،إطار تشريعى جامع مع أدوار مؤسسية بما فيها وزارة الإليكترونيات وتكنولوجيا المعلومات، سياسة وطنية عام 2013 جارى تطويرها لإستراتيجية وطنية منذ عام 2020.
- **تجربة اسرائيل ومزايا الاقتصاد السيبرانى**، ربط وثيق بين الأمن السيبرانى والوطنى للتعامل مع مهددات إقليمية حاضرة بقوة، أطر تشريعية ومؤسسية مع التركيز على الدفاع السيبرانى، ابحث والتطوير والكوادر، ميزات ومنافع اقتصادية (10% من المبيعات العالمية لأمن المعلومات).
- **خبرات متعددة من تجارب عالمية أخرى**، مركز سيبرانى وطنى لدعم الحكومة وقطاعات الأعمال العامة والخاصة(المملكة المتحدة)، مكتب فيدرالى لأمن المعلومات(ألمانيا)، قانون وتشديدات لحماية البنية المعلوماتية الوطنية(الصين)، ومجلس للأمن القومى مسئول عن السياسات السيبرانية(اليابان)، ووكالة وطنية مسئولة عن القواعد والإرشادات(ماليزيا)، وإستراتيجية وطنية مع ارشادات متوافقة مع ارشادات الإتحاد الدولي للإتصالات (بنغلاديش).
- **خبرات تجربة المملكة العربية السعودية**، ربط الأمن السيبرانى مع توجهات رؤية المملكة 2030، تشريعات ومؤسسات معنية، إستراتيجية وضوابط ومعايير ناظمة، استضافات

ومبادرات إقليمية سيبرانية هامة، ومشاركات معلوماتية وسيبرانية فاعلة فى إطار مجموعة العشرين G20.

- **خبرات تجربة سلطنة عمان**، أطر تشريعية ومؤسسية وطنية خاصة المركز الوطنى للسلامة المعلوماتية والمختبر الوطنى للأدلة الرقمية، ومساهمات إقليمية هامة لإإستضافة السلطنة المركز العربي الإقليمي للأمن السيبرانى منذ عام 2013.
- خبرات مستفادة للتجربة المصرية
  - الربط الوثيق بين الأمن السيبرانى والأمن الوطنى للدولة والأمن الإقليمي والعالمي
  - الربط الوثيق بين الأمن السيبرانى وإستراتيجيات وخطط الدولة التنموية
  - دور محورى للدولة فى تخطيط وتوجيه سياسات وقواعدا الأمن السيبرانى
  - دور هام للأمن السيبرانى فى دعم التنمية المستدامة وأهدافها الأممية والوطنية
  - أهمية الدبلوماسية السيبرانية والتواصل من خلالها على المستويين الإقليمي والعالمي.

الفصل الثالث

الأمن السيبرانى فى مصر

يجسد إهتمام الدولة بالأمن السيبرانى توجيه رئيس الجمهورية مؤخراً (29 مارس 2021) للحكومة والوزارات المعنية على وجه الخصوص بإيلاء أهمية لـ:"الأمن السيبراني"، بالإضافة إلى جودة البنية التحتية المعلوماتية خاصة فى العاصمة الإدارية [1]، كما أكد مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصري على إرتباط الأمن القومى والاقتصاد بالأمن السيبرانى.

ويتكامل هذا الاهتمام بصورة أو أخرى مع إهتمامات مصاحبة فى الدولة منها ما هو على المستوي الدستوري بالنص صراحة على العلاقة بين الأمن الفضائي المعلوماتي ومنظومتي الاقتصاد والأمن القومي فى دستور عام 2014، هذا بالإضافة للإهتمامات التشريعية المساندة ذات الصلة فى شأن جرائم تقنية المعلومات، أو فى شأن حماية البيانات الشخصية، أو بخصوص تنظيم التوقيع الإلكتروني، وغيرها من التشريعات التى سنعرض لها لاحقاً.

وقد صاحب هذه الاهتمامات الدستورية والتشريعية إجراءات عملية تخطيطية ومؤسسية وتنظيمية لتعزيز الاهتمام بالأمن السيبرانى فى مصر من خلال إنشاء المجلس الأعلى للأمن السيبرانى عام 2015، وإطلاق إستراتيجية الوطنية للأمن السيبرانى 2017-2021، وانعقاد المؤتمر الوطني الأول للأمن السيبرانى فى ديسمبر 2019، وغيرها.

يلقى الفصل الحالى الأضواء على بيئة عمل الأمن السيبرانى فى مصر ويركز، على غرار مؤشر الأمن السيبرانى العالمي:GCI، على تحليل المحاور التشريعية والمؤسسية والتقنية والتنظيمية، كذلك محورى بناء القدرات والتعاون عبر الفضاءات الإقليمية والدولية ذات الصلة. كما يضاف اليها محور الأمن القومى والعلاقة بين الأمن السيبرانى والتنمية المستدامة.

فى ضوء ذلك، يتناول الفصل الثالث القضايا التالية:

المبحث الأول: الوضع الراهن: المرجعيات الرئيسية ذات الصلة بالأمن السيبرانى

المبحث الثانى: المؤشرات والأدوار الرئيسية ذات الصلة بالأمن السيبرانى فى مصر

---

(1) وفق تصريحات المتحدث باسم رئاسة الجمهورية السفير / بسام راضى عن اجتماع لرئيس الدولة مع رئيس مجلس الوزراء، وزير الإتصالات وتكنولوجيا المعلومات، ووزير الإسكان والمرافق بمقر رئاسة الجمهورية فى مارس 2021.

المبحث الأول

الوضع الراهن: المرجعيات الرئيسية ذات الصلة بالأمن السيبرانى

يلقى المبحث الحالى الأضواء على المرجعيات الدستورية والتشريعية والتنموية للأمن السيبرانى فى علاقته بالاقتصاد الرقمى فى مصر.

أولاً: مرجعيات دستورية وتشريعية وتخطيطية للأمن السيبرانى والاقتصاد الرقمى فى مصر

1. نظرة دستورية شاملة للأمن السيبرانى: الاقتصاد والأمن ودور الدولة.

يقدم الدستور المصري لعام 2014 رؤية شاملة للأمن السيبرانى من خلال محاور ثلاثة [1]:

المحور الأول: الربط بين أمن المعلومات والاقتصاد الوطنى

المحور الثانى: الربط بين أمن المعلومات والأمن القومى

المحور الثالث: التزام الدولة بإتخاذ التدابير اللازمة للحفاظ على أمن المعلومات وفق الإطر التى ينظمها القانون.

وقد انعكست هذه النظرة الشاملة على إهتمام رئيس الدولة، الذى وجه للإهتمام بالأمن السيبرانى (29 مارس/ 2021) والتأكيد على أدوار محددة لكافة أجهزة الدولة المعنية للإهتمام بالأمن السيبرانى، وبناء وتطوير بنية تحتية وطنية متكاملة للمعلومات والإتصالات، بما يعكس أخذ الدولة لزمام المبادرة فى التعامل مع قضايا الأمن السيبرانى.

كما انعكس هذا الاهتمام لدى (مركز المعلومات ودعم اتخاذ القرار) بمجلس الوزراء المصري الذى أكد على أن الإختراقات السيبرانية تعتبر من أهم الأخطار المؤثرة سلباً على الأمن القومى والاقتصادات فى القرن الحالى ، مع التحذير من خطورة تلك الإختراقات على البنية التحتية الحرجة للمعلومات والإتصالات، واستهداف الشركات، وغيرها [2].

وتم ترجمة هذه الرؤية الدستورية الشاملة لاحقاً فى العديد من الخطوات التى تبنتها الدولة المصرية، ونعرض لها لاحقاً، بدءاً من إنشاء المجلس الأعلى للأمن السيبرانى عام 2015 وإطلاق إستراتيجية الوطنية للأمن السيبرانى 2017–2021، وانعقاد المؤتمر الوطني الأول للأمن السيبرانى فى ديسمبر 2019، وغيرها

---

(1) دستور جمعهورية مصر العربية – مادة رقم 31.

(2) مع توقعات أن تستمر هذه الإختراقات وما يصاحبها من مخاطر فى عام 2021. يراجع
مركز المعلومات ودعم اتخاذ القرار (2020). أهم اختراقات الأمن السيبرانى لعام 2020.القاهرة: رئاسة مجلس الوزراء. غير مرقم الصفحات.

2. أطر تشريعية داعمة للأمن السيبرانى والتحول الرقمى، وتنتظر المزيد:

2.1. الأطر الداعمة للأمن السيبراني في مصر

تتساوق الأطر التشريعية الوطنية -خاصة الحديث منها- مع التوجهات الدستورية حول محورية الأمن السيبرانى وأمن المعلومات وقضايا إدارة البيانات فى تعزيز الأمن القومى، ودعم التحول والاقتصاد الرقمى وما يرتبط بهما من أنشطة مثل التسويق الإليكترونى وغيره. ويوضح الجدول التالى أبرز الأطر التشريعية المرتبطة بصورة مباشرة أو غير مباشرة بدعم الأمن السيبرانى والتحول نحو الاقتصاد الرقمى فى مصر.

جدول (3-1)

الأطر التشريعية والقواعد التنظيمية ذات العلاقة بالأمن السيبرانى فى مصر

التشريعات	الملامح الرئيسية
قانون 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية	• حقوق الأشخاص المعنية بالبيانات وشروط جمع ومعالجة البيانات • التزامات المتحكم والمعالج للبيانات، ومسئول حماية البيانات • البيانات الشخصية عبر الحدود والتسويق الإليكترونى المباشر • تأسيس مركز متخصص لحماية البيانات الشخصية
قانون 175 لسنة 2018 فى شأن مكافحة جرائم تقنية المعلومات	• التزامات وواجبات مقدم الخدمات المعلوماتية والنطاق المكانى للقانون • التعاون الدولي لمكافحة جرائم تقنية المعلومات • الأحكام والقواعد الإجرائية، والأدلة الرقمية • الإعتداء على سلامة شبكات وأنظمة تقنيات المعلومات
قرار رئيس مجلس الوزراء رقم 2259 لسنة 2014 بإنشاء المجلس الأعلى للأمن السيبرانى	• وضع الإستراتيجية القومية للأمن السيبرانى • الإشراف على تنفيذ الإستراتيجية لمواجهة الأخطار والهجمات السيبرانية
قانون رقم 15 لسنة 2004 بتنظيم التوقيع الإليكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات - قرار وزير الإتصالات 361 لسنة 2020 بتعديل اللائحة التنفيذيه لقانون التوقيع الالكترونى	• إنشاء هيئة تنمية صناعة تكنولوجيا المعلومات لتنمية الإستثمار وفرص التصدير وبناء الكوادر • تشجيع المشروعات الصغيرة لإستخدام المعاملات الإليكترونية وتعزيز خدمات التوثيق الإليكترونى. • إنشاء الإطار التشريعى والتنظيمى لمنظومة التوقيع الإلكترونى • إنشاء الإطار الفنى التفصيلى لتنفيذ منظومة التوقيع الإلكترونى الخاص بشهادات الإعتماد ونظم التشفير

التشريعات	الملامح الرئيسية
قانون رقم 10 لسنة 2003 بإصدار قانون تنظيم الإتصالات	• دور الجهاز القومى لتنظيم الإتصالات • التراخيص والتصاريح لشبكات وخدمات الإتصالات والطيف الترددى • أدوار الشركة المصرية للإتصالات
قانون رقم 82 لسنة 2002بإصدار قانون حقوق الملكية الفكرية ولوائحه التنفيذية	• براءات الإختراع ومخططات التصميمات للدوائر المتكاملة • العلامات والبيانات التجارية والتصميمات والنماذج الصناعية • حقوق المؤلف والحقوق المجاورة
أطر وقواعد تنظيمية ذات صلة (الجهاز القومى لتنظيم الإتصالات)	• أطر تنظيمية للترابط، وسياسات المنافسة، وخدمات القيمة المضافة • قواعد المحافظ الإليكترونية،شرائح المحمول، إعتماد وتفعيل نقاط البيع، وبيع شرائح المحمول للشركات.

المصدر: مركب من التشريعات المبحوثة، وموقع جهاز تنظيم الإتصالات:https://www.tra.gov.eg/

ويمكن الإشارة إلى بعض الملاحظات حول الأطر التشريعية والقواعد التنظيمية:

- **الاهتمام بتوصيف الأمن القومى وتعريف مؤسساته،** خاصة القانون رقم 175 لسنة 2018 والذى عرف الأمن القومى بإعتباره كل مايتعلق باستقلال واستقرار وأمن الوطن ووحدة وسلامة أراضيه، كما عرف هذا القانون والقانون 151 لسنة 2020 كليهما جهات الأمن القومى: رئاسة الجمهورية، وزارة الدفاع، وزارة الداخلية، المخابرات العامة، وهيئة الرقابة الإدارية.
- **الاهتمام بحوكمة إدارة البيانات على المستوى الوطنى،** حيث صدر قانون خاص بالبيانات فى مصر، والذى يمثل نقلة نوعية كانت ملحة لتفعيل عمليات إدارة البيانات على المستوى الوطنى فى إطار يحمى الخصوصية الشخصية والمصالح الوطنية على السواء، ويضمن حماية بعض فئات المجتمع الهشة أو الأكثر انكشافاً خاصة الأطفال.
- **الاهتمام بحماية التحول الرقمى وأدواته وتشجيع ريادة الأعمال،** حيث أكد الفصل الثانى من القانون 175 لسنة 2018 على التعامل الصارم مع جرائم الإحتيال والإعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإليكترونى. كما أكد قانون تنظيم التوقيع الإليكترونى على دور هيئة تنمية صناعة تكنولوجيا المعلومات فى تشجيع المشروعات الصغيرة والمتوسطة على استخدام وتوظيف آليات المعاملات الإليكترونية، بالإضافة إلى

تشجيع انشاء الشركات التى تعمل فى مجال تنمية صناعة تكنولوجيا المعلومات والإتصالات.

- **تعديلات تشريعية لمواكبة وتسريع التحولات الرقمية**، حيث قامت وزارة الإتصالات وتكنولجيا المعلومات بتعديل اللائحة التنفيذية لقانون التوقيع الإلكترونى المصري لمواكبة التطورات التكنولوجية وتسريع عمليات التحول الرقمي والتى تضمنت إضافة خدمة الختم الإلكترونى وإضفاء الحجية القانونية للتوقيت الزمنى للمحررات الإلكترونية (أو ما يعرف بالبصمة الزمنية)[1].

2.2. فجوات تشريعية وتنظيمية متعددة

- **غياب تشريع خاص للأمن السيبرانى**، وقد أشارت وقائع ورشة العمل حول الأمن السيبرانى بالمعهد (فبراير 2021) إلى أن هناك جهود جارية لإعداد مثل هذا التشريع لدعم تنفيذ أهداف المجلس الأعلى للأمن السيبرانى والإستراتيجية الوطنية للأمن السيبرانى.
- **غياب قانون جديد متطور للتجارة الإليكترونية**، حيث يجرى إعداد هذا القانون بين لجنة الإتصالات وتكنولوجيا المعلومات بمجلس النواب بالتعاون مع وزارة التموين ووزارة الإتصالات وتكنولوجيا المعلومات بعد وصول حجم التجارة الإليكترونية فى مصر إلى 40 مليار دولار عام 2020.
- **أكثر من تشريع لضبط وإدارة البيانات**، قانون عام لتنظيم عمليات حماية وتأمين البيانات على المستوى القومى، وقانون لتنظيم إنشاء وإدارة مراكز البيانات فى الدولة، إطار قانونى بإلزام الجهات الحكومية والقطاع الخاص بتطبيق قانون التوقيع الإلكترونى كأحد محاور حماية وتأمين تدفق المعلومات. بالإضافة إلى قانون لتنظيم عملية بناء وإدارة المواقع اللألكترونية والتى تتعامل مع الجهات الحكومية من قطاع خاص ومجتمع مدنى، وضوابط حمايتها وتشغيلها فى إطار الأمن السيبرانى.
- **تعديلات مطلوبة على قانون حماية الملكية الفكرية المتقادم**، فمن جهة تتطلب التحولات الرقمية ادخال تعديلات على القانون تتعلق بقواعد حماية المحتوى الرقمى والحقوق فى

---

(1) للتفاصيل يراجع :

-Ministry of Communication and Information Technology. (2021). MCIT Yearbook 2020. Cairo. MCIT.

البيئات الرقمية، هذا بخلاف تحديات ضعف الإنفاذ فى الواقع العملى [1].

- **متطلبات تشريعية وإجرائية رقمية هامة** [2]، قواعد للهوية الرقمية، وضع قواعد واضحة لإجراءات جمع والتحفظ ونقل (الأدلة الرقمية) والتعامل معها، ووضع اطار ينظم التعاون الرقمى مع العالم الخارجى، وإعادة تنظيم إجراءات استيراد وتصنيع المعدات التكنولوجية.

3. الأطر التخطيطية وصناعة السياسات للأمن السيبرانى وعلاقتها بالاقتصاد الرقمى فى مصر

أشارت وثيقة إستراتيجية التنمية المستدامة: رؤية مصر 2030 بوضوح إلى ضعف الثقافة الرقمية ومنظومة التجارة الإليكترونية وثغرات فى البيئة القانونية والتنظيمية والتعامل مع الإنترنت بما يضعف فرص مصر فى الاقتصاد الرقمى[3].

فى ضوء ذلك تبنت الوثيقة وتحديثاتها، بالإضافة إلى وثائق التنمية الأخرى الرئيسية والنوعية المرتبطة بها بعض التوجهات للتعامل مع التحديات التى رصدتها الإستراتيجية والسابق الإشارة اليها كما يوضح الجدول التالى:

جدول (3-2)

توجهات وثائق التنمية حول التحول الرقمى والأمن السيبرانى فى مصر

الوثيقة التنموية	ملامح الاهتمام بالتحول الرقمى والأمن السيبرانى
إستراتيجية التنمية المستدامة: رؤية مصر 2030 –	• زيادة تنافسية الاقتصاد والتنوع والإعتماد على المعرفة • دمج تكنولوجيا المعلومات فى القطاعات الاقتصادية وتعظيم صادراتها
تحديثات إستراتيجية التنمية المستدامة:رؤية مصر 2030	• نمو اقتصادى قائم على المعرفة وتحقيق التحول الرقمى ودعم مرونة وتنافسية الاقتصاد، والشمول المالي. • فرص التشغيل، بيئة الأعمال، ريادة الأعمال البعد الإجتماعى والبيئى
خطة التنمية متوسطة المدى 2025/24-2019/18	• بناء مجتمع المعلومات وتطوير نظم الإتصالات وتكنولوجيا المعلومات لدعم الإصلاح الاقتصادى والإجتماعى • نشر استخدام تكنولوجيا المعلومات لتضييق الفجوة الرقمية • برامج للتحول إلى المجتمع الرقمى، وآخر لتطوير (أمن المعلومات)
برنامج عمل الحكومة 2025/24-2019/18	• برنامج لتطوير نظم الإتصالات وتوطين صناعة تكنولوجيا المعلومات يتضمن: تطوير تشريعى، البنة التحتية بما فيها الجيل الخامس G5،

---

[1] محمد حجازى(2021). الأمن السيبرانى بين التشريعات الوطنية والمتطلبات الدولية: القاهرة: ورشة عمل بمركز المعلومات ودعم اتخاذ القرار. صص.7-11.

[2] المرجع السابق، نفس الصفحات.

[3] استراتيجية التنمية المستدامة: رؤية مصر 2030، ص32.

الوثيقة التنموية	ملامح الاهتمام بالتحول الرقمى والأمن السيبرانى
	التحول للمجتمع الرقمى، وبناء الكوادر البشرية المعلوماتية.
خطة التنمية السنوية – خطة العام الثالث 2021/20 – 2021/2020	• تهيئة البنية المعلوماتية للإنتقال إلى العاصمة الإدارية (مركز البيانات + أرشفة الوثائق) • ميكنة الخدمات الحكومية • تطوير البنية المعلوماتية(القدرات الرقابية + ورفع مستوى تأمين البنية المعلوماتية الحرجة)
مبادرة مصر الرقمية (وزارة الإتصالات وتكنولوجيا المعلومات)	• الوصول إلى مجتمع رقمى مصرى يتعامل رقمياً فى كافة مناحى الحياة • تحويل الحكومة إلى مترابطة رقمياً • تمكين الحكومة الإليكترونية، وضمان مشاركات مجتمعية داعمة • 7 منصات للتحول الرقمى
الإستراتيجية الوطنية للأمن السيبرانى (2017–2022)	• رصد للمخاطر والمهددات السيبرانية للدولة والمجتمع • دعم التحول نحو(اقتصاد رقمى متكامل) • مواجهة المخاطر السيبرانية وتعزيز الثقة فى البنة التحتية • 6 برامج: التطوير التشريعى، منظومة حماية سيبرانية وطنية،حماية الهوية الرقمية،إعداد الكوادر والخبرات، دعم البحث العلمى ذى الصلة، التوعية السيبرانية المجتمعية.
الإستراتيجية القومية للعلوم والتكنولوجيا والإبتكار 2030	• محور خاص لتكنولوجيا المعلومات والفضاء • قضايا متنوعة ذات صلة: أمن الحاسوب وحماية الأجهزة والبرمجيات الأمن السيبرانى والأمن الذكى، معالجة البيانات الضخمة والبيانات مفتوحة المصدر، تقنيات الجيل الخامس، خدمات الحوسبة السحابية، شبكات وقواعد المعلومات، سلسلة الكتل ونقل القيمة عبر الإنترنت.
إستراتيجيات وخطط نوعية متعددة أخرى	• إستراتيجية مصر 2030 فى الإتصالات وتكنولوجيا المعلومات • المحتوى الرقمى العربي، الحوسبة السحابية،البرمجيات الحرة مفتوحة المصدر، المسئولية المجتمعية.

المصدر: مركب بمعرفة الفريق البحثى من وثائق التنمية – قائمة المراجع

وبخلاف وثائق التنمية المختلفة، فقد أكدت العديد من الدراسات العلاقة الأكيدة بين قوة وصلابة قطاع تكنولوجيا المعلومات والإتصالات وبين تحقيق التنمية المستدامة أو الشاملة فى مصر وتنظيم

هذا القطاع تخطيطياً وتشريعياً ومؤسسياً لأداء هذا الدور التنموى الهام[1].

ويمكن الإشارة إلى الملاحظات التالية من مراجعة الجدول السابق:

- **تفاوتات فى الاهتمام بقضية الأمن السيبرانى (أمن المعلومات) فى علاقته بالاقتصاد الرقمى فى مصر**، بين وثائق التنمية السابق العرض لها دون أن تتوافر سياسات وتوجهات واضحة تترجم برامج إستراتيجية الأمن السيبرانى إلى برامج عملية تدرج فى وثائق التنمية المختلفة وفق جداول زمنية وتكاليف استثمارية محددة ومؤشرات أداء للتقييم والمراجعة.
- **إهتمام بقضية التشريعات عبر الوثائق التخطيطية**، سواء فى الحاجة إلى تشريعات جديدة أو تطوير التشريعات القائمة كما سبق وعرضت الدراسة فى البند السابق.
- **إهتمام بالتحول نحو الاقتصاد الرقمى فى الإستراتيجية الوطنية للأمن السيبرانى**، فمع تركيز الإستراتيجية بصورة أكبر على بيئة وقواعد عمل الأمن السيبرانى، إلا أن مقدمة الإستراتيجية تشير بوضوح إلى توجه الإستراتيجية لدعم التحول نحو اقتصاد رقمى متكامل يحقق طموحات المواطنين فى التنمية.

ويبقى أن يتحول هذا الاهتمام بالاقتصاد الرقمى إلى برامج ومشروعات محددة يتم التوافق عليها مع جهاز التخطيط فى اطار برامج التنمية الاقتصادية للدولة، ويتم تضمينها فى وثائق التنمية المختلفة وبرامج العمل الحكومية.

- **الكثير من الإستراتيجيات النوعية والقليل من الحضور والترابط والأثر العملى**، حيث تتعدد الخطط النوعية دون الإنتظام فى رؤية إستراتيجية تنموية موحدة تنطلق من:
  - رؤية إستراتيجية لتعزيز حصانة الدولة وأمنها القومى رقميًا وسيبرانياً
  - أهداف إستراتيجية محددة للتحول الرقمى فى الاقتصاد والمجتمع
  - أهداف إستراتيجية لتعزيز حضور ومشاركة مصر فى سلاسل القيمة الرقمية الإقليمية والعالمية بما يعزز الميزات التنافسية للدولة.
  - أدوار ومسئوليات فى النظام الإيكولوجى للأمن السيبرانى والاقتصاد الرقمى
    - أطر تشريعية جديدة، وأطر تشريعية مطورة

---

(1) على اعتبار المعلومات أحد الموارد الرئيسة لتحقيق التنمية الإجتماعية والاقتصادية فى مصر، يراجع:

- تامر حنفي داود (2020). تصور مقترح لبناء سياسة وطنية للمعلومات كركيزة لتأسيس نظام وطنى للمعلومات فى جمهورية مصر العربية: ضرورة ملحة لتلبية احتياجات التنمية الوطنية الشاملة والمستدامة. (المجلة العربية للمعلوماتية وأمن المعلومات، المجلد الأول، العدد الأول، أكتوبر 2020)، ص.83-164.

- أدوار مؤسسية ومبادرات منفردة أو مشتركة أو جماعية للحكومة، قطاعات الأعمال العامة والخاصة، والمجتمع الأهلى المعنى، بالإضافة إلى الأدوار الإعلامية والتوعوية.
- برامج ومشروعات محددة تقوم بها الأجهزة والقطاعات المعنية فى الدولة، ويتم ادراجها فى خطط وبرامج التنمية الوطنية.
- قواعد عمل وأطر تنظيمية وإجرائية
- أدوار اعلامية للتوعية المجتمعية

المبحث الثانى

المؤشرات والأدوار الرئيسية ذات الصلة بالأمن السيبرانى فى مصر

يلقى المبحث الضوء على موقف مصر فى بعض المؤشرات الخاصة بالأمن السيبرانى وتكنولوجيا المعلومات والإتصالات والاقتصاد الرقمى، والأدوار المؤسسية الفاعلة فى مجال وقضايا الأمن السيبرانى فى مصر.

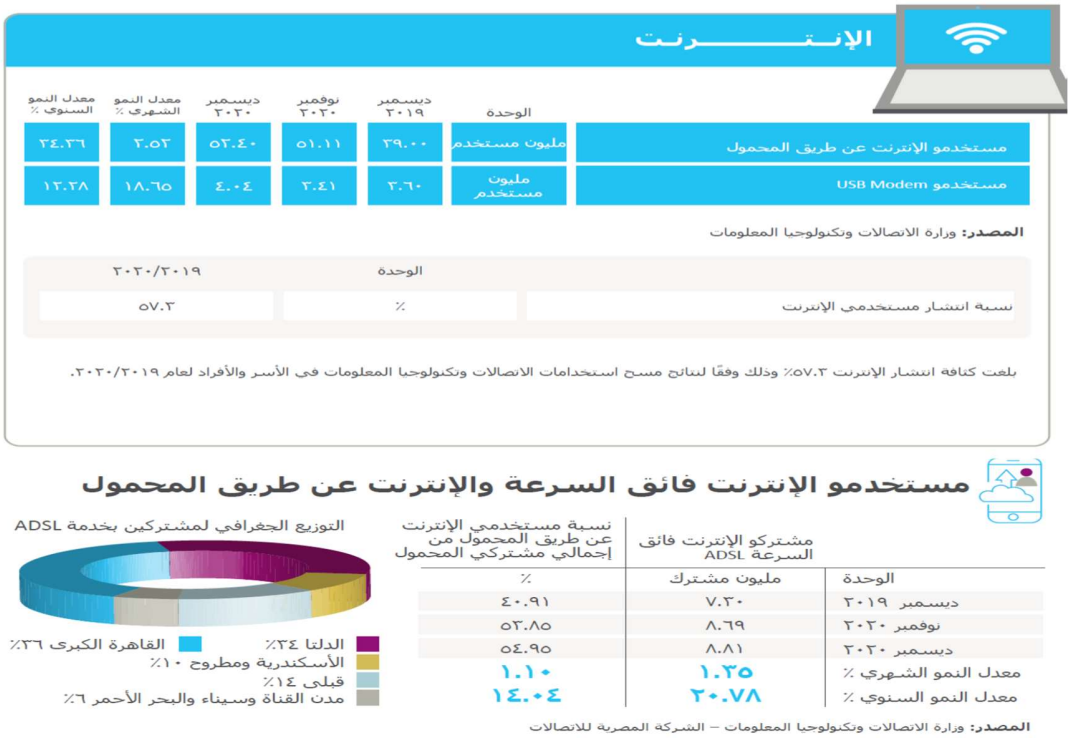
أولاً: مؤشرات تكنولوجيا المعلومات والإتصالات والأمن السيبرانى فى مصر

يشير أحدث التقارير الدورية (مارس 2021) الصادرة عن وزارة الإتصالات وتكنولوجيا المعلومات إلى بعض المؤشرات الوطنية، والتى يلاحظ منها:

- **نسبة إنتشار كبيرة للهواتف المحمولة**، زيادة أعداد خطوط الهاتف المحمول فى نهاية ديسمبر عام 2020 ليصل إلى 95.4 مليون خط بنسبة إنتشار تتجاوز 93.6 %.

شكل (3-1)

مستخدمى الإنترنت العادى وفائق السرعة ومن خلال الهواتف المحمولة (ديسمبر 2019 – نوفمبر 2020 – ديسمبر 2020)



الإنترنت

	الوحدة	ديسمبر ٢٠١٩	نوفمبر ٢٠٢٠	ديسمبر ٢٠٢٠	معدل النمو الشهرى ٪	معدل النمو السنوى ٪
مستخدمو الإنترنت عن طريق المحمول	مليون مستخدم	٣٩.٠٠	٥١.١١	٥٢.٤٠	٢.٥٢	٣٤.٣٦
مستخدمو USB Modem	مليون مستخدم	٣.٦٠	٣.٤١	٤.٠٤	١٨.٦٥	١٢.٢٨

المصدر: وزارة الاتصالات وتكنولوجيا المعلومات

	الوحدة	٢٠٢٠/٢٠١٩
نسبة انتشار مستخدمي الإنترنت	٪	٥٧.٣

بلغت كثافة انتشار الإنترنت ٥٧.٣٪ وذلك وفقًا لنتائج مسح استخدامات الاتصالات وتكنولوجيا المعلومات فى الأسر والأفراد لعام ٢٠٢٠/٢٠١٩.

مستخدمو الإنترنت فائق السرعة والإنترنت عن طريق المحمول

الوحدة	مشتركو الإنترنت فائق السرعة ADSL	نسبة مستخدمي الإنترنت عن طريق المحمول من إجمالي مشتركي المحمول
	مليون مشترك	٪
ديسمبر ٢٠١٩	٧.٣٠	٤٠.٩١
نوفمبر ٢٠٢٠	٨.٦٩	٥٣.٨٥
ديسمبر ٢٠٢٠	٨.٨١	٥٤.٩٥
معدل النمو الشهري ٪	١.٣٥	١.١٠
معدل النمو السنوي ٪	٢٠.٧٨	١٤.٠٤

التوزيع الجغرافي لمشتركين بخدمة ADSL

المصدر: وزارة الاتصالات وتكنولوجيا المعلومات – الشركة المصرية للاتصالات

المصدر: وزارة الإتصالات وتكنولوجيا المعلومات (2021).تقرير موجز عن مؤشرات الإتصالات وتكنولوجيا المعلومات –عدد شهرى: مارس.القاهرة: الوزارة: ص1-4.

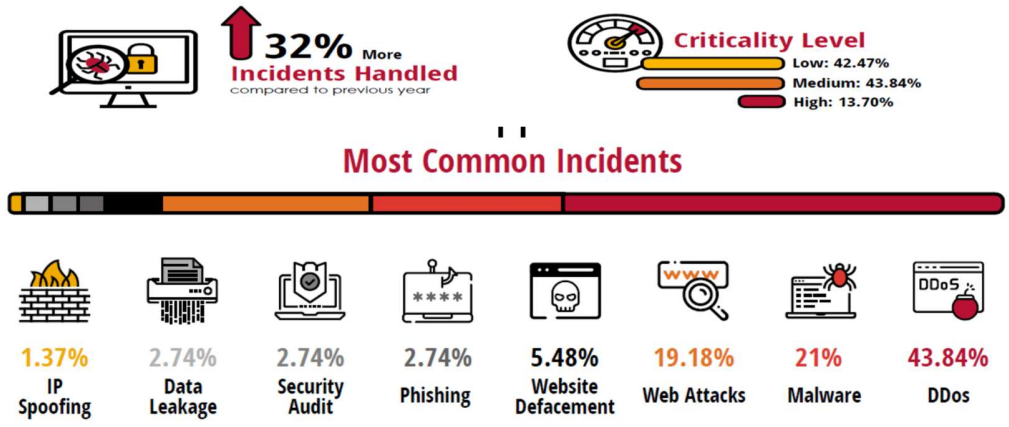
- **تطورات إنتشار الإنترنت بما فيه النطاق العريض**، حيث وصلت نسبة إنتشار مستخدمى الإنترنت إلى 57.3%، وتجاوز عدد مشتركى الإنترنت فائق السرعة 8.8 مليون مشترك فى ديسمبر 2020، كما وصلت نسبة مستخدمى الإنترنت من اجمإلى المشتركين فى الهاتف المحمول إلى 54.9 % فى نفس التاريخ.
- مؤشرات الأمن السيبرانى لعام 2020،

تشير احصاءات أخيرة متاحة لمركز الإستعداد لطوارىء الحاسبات والشبكات:EG-CERT إلى مجموعة من الحقائق:

- **تحسن تعامل المركز مع الهجمات**، حيث زاد عدد الهجمات التى تعامل معها المركز بنسبة 32% مقارنة بالعام السابق.
- **تباينات فى مستوى خطورة وشدة الهجمات**، حيث مثلت الهجمات الأقل خطورة نسبة 42.5% من إجمإلى الهجمات، فى حين شكلت الهجمات شديدة الخطورة حوالى 13.7% من اجمإلى الهجمات مقابل 43.8% للهجمات متوسطة الخطورة. الأمر الذى يعنى أن الهجمات متوسطة وشديدة الخطورة تمثل حوالى 57.5% من إجمإلى الهجمات.
- **هجمات حجب المواقع تتصدر DDos**، حيث شكل هذا النوع من الهجمات حوالى 43.8% من إجمإلى الهجمات فى مقابل 21% لهجمات البرامج الضارة، و19% لهجمات المواقع الإليكترونية. وتشكل الأنواع الثلاثة معاً حوالى 83.8% من اجمإلى الهجمات.
- البرامج الضارة .

شكل (3-2)

موقف الهجمات السيبرانية فى مصر: يوليو / ديسمبر 2020



المصدر: المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات – EG CERT

ثانياً: تقييم موقف مصر على بعض المؤشرات العالمية والإقليمية ذات الصلة:

يوضح الجدول التالى تطور ترتيب مصر على بعض المؤشرات العالمية ذات الصلة بالأمن السيبرانى والاقتصاد الرقمى.

جدول (3-3)

تطور ترتيب مصر بين عامى 2018-2020 على بعض المؤشرات العالمية ذات العلاقة بالأمن السيبرانى والاقتصاد الرقمى

المؤشر	ترتيب 2018	ترتيب 2020	ملاحظات
مؤشر الأمن السيبرانى العالمي – GCI	23	23	سبق العرض لتفاصيل المؤشر
مؤشر القوة السيبرانية الوطنية–NCPI	59	29	سبق العرض لتفاصيل المؤشر
مؤشر الجاهزية الشبكية –NRI		84	المؤشرات: التكنولوجيا،الأفراد والأعمال والحكومة، الحوكمة، والأثر (خاصة على التنمية المستدمة)
مؤشر جاهزية الحكومات للذكاء الإصطناعى –	111 (2019)	56	يتناول 3 محاور، 10 أبعاد، و33 مؤشر فرعى: الحكومات، قدرات القطاع التكنولوجى،والبيانات والبنية التحتية بما فيها الجيل الخامسG5
مؤشر المعرفة العالمي	99	72	7 مؤشرات: التعليم قبل الجامعى، التعليم التقنى والتدريب المهنى، التعليم العإلى، البحث والتطوير والإبتكار، تكنولوجيا المعلومات والإتصالات، الاقتصاد والتمكين
مؤشر الإبتكار العالمي –GII	95	96	وقد تحسن الترتيب إلى المركز 92 عام 2019 ليتراجع إلى 96.

المصدر: مركب من التقارير العالمية للمؤشرات المذكورة – قائمة المراجع

1. الجوانب الإيجابية والتحديات المستخلصة من التقارير السابقة:

- **تحسن ترتيب مصر العالمي على بعض المؤشرات الهامة**، ويأتى على رأسها مؤشر القوة السيبرانية الوطنية الذى شهد تطوراً بارزاً فى عام 2020 مقارنة بعام 2018. كما تحسن موقف مصر على مؤشر جاهزية الحكومات للذكاء الإصطناعى والذى يلحق به تحسن ترتيب الجامعات المصرية، وأدوار مشهود لها لكلية الحاسبات بجامعة القاهرة وفق تقرير الذكاء

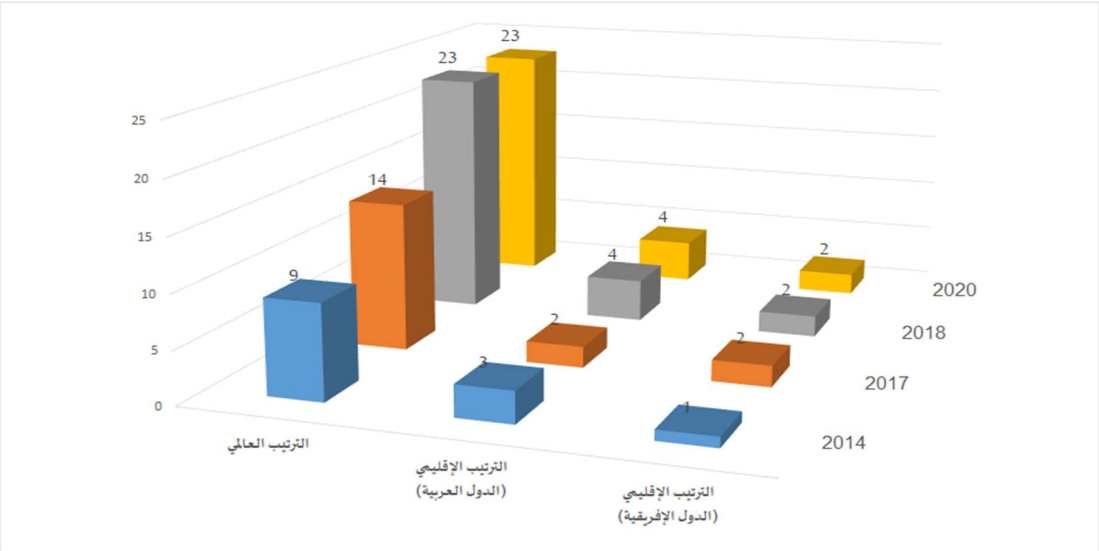
الإصطناعى. وكذلك التحسن الملموس فى ترتيب مصر على مؤشر المعرفة العالمي والذى حقق تقدماً جيداً بين عامى 2018-2020، ويبقى تحسن مصر فى ترتيب الدول العربية على المؤشر المذكور حيث تأتى مصر فى المرتبة السابعة عربياً.

- **تطورات إيجابية موازية على مؤشر الأمن السيبرانى العالمي**، فعلى الرغم من ثبات الترتيب العالمي لمصر للعام 2020 مقارنة بعام 2028 (المركز 23 عالمياً)، وثبات الترتيب عربياً وأفريقياً بين نفس العامين كما يوضح الشكل رقم 3-3 إلا أن التقرير الدولي لعام 2020 تضمن جوانب ايجابية هامة فى الموقف المصري. وفى هذا الخصوص يشير التقرير إلى تحقيق مصر مجموع درجات يصل إلى 95.48 درجة مقابل 88.3 درجة عام 2017، كما نوه التقرير إلى تحقيق مصر تطوراً ايجابياً على ثلاثة محاور رئيسة للمؤشر: المحور القانونى، والمحور التنظيمى، ومحور تطوير القدرات.[1]

ومع الطفرة الكبيرة فى ترتيب السعودية ودولة الإمارت العربية عالمياً على المؤشر المذكور لعام 2020(الثانى والخامس عالمياً) وكذلك سلطنة عمان (المركز 21 عالميًا)، فإن هناك فرصاً جيدة أمام مصر لتحسين ترتيبها العالمي فى السنوات القادمة أسوة بالدول العربية المذكورة.

شكل (3-3)

تطور موقف مصر على مؤشر الأمن السيبرانى عالميًا /أفريقيًا وعربيًا



المصدر: مركب بمعرفة الفريق البحثى من تقارير الإتحاد الدول للإتصالات الأخيرة حول المؤشر (قائمة المصادر)

[1] كما حققت مصر تقدماً أقل نسبياً على محاور: القدرات الفنية، ومحور التعاون والشراكات، يراجع:
-ITU (2021). **Op.cit**. p.73.

- **فيما يتعلق بالجاهزية الشبكية،** بوجه عام تحقق مصر معدلات أفضل من المعدلات المتوسطة للشريحة الدنيا من البلدان متوسطة الدخل سواء على مستوى المؤشر الإجمالى أو على مستوى المؤشرات الأربعة الفرعية للمؤشر الرئيس. [1]
- **اتجاهات ايجابية أخرى،** ومن بينها إنتشار وظائف اقتصاد العمل الحر Gig Economy، تحسن إنفاق الحكومة على البحث والتطوير والتعليم العالى، وتوسع الإنترنت فى المدارس وغيرها، بالإضافة إلى اتاحة الطاقة النظيفة الميسرة (الهدف رقم 7 من أهداف التنمية المستدامة).

2. <u>أبرز التحديات:</u>

- **فيما يتعلق بالجاهزية الشبكية،** بوجه عام تحقق مصر معدلات أقل مقارنة بالمتوسط العربي للمؤشر الرئيس للجاهزية الشبكية، كما تحقق معدلات أقل من المعدلات العربية الإجمالية للمؤشرات الأربعة الفرعية. بالإضافة إلى ذلك فإن هناك تحديات أضافية تتمثل فى ضعف التعاملات المالية عبر الإنترنت، قصور فى جودة الحوكمة والقواعد الناظمة، خوادم تأمين الإنترنت، ضعف الصادرات التقنية، ضعف التسوق عبر الإنترنت، بالإضافة إلى فجوات فى هدفين للتنمية المستدامة: المساواة فى النوع (هدف رقم 5)، وإستدامة المدن والمجتمعات (هدف رقم 11) وفق رؤية التقرير. [2]
- **تراجع على مؤشر الإبتكار العالمي،** والذى يرجع بالدرجة الأولى وفق تقرير 2020 إلى تراجع مصر على مؤشرات (مدخلات الإبتكار) الفرعية مثل:المؤسسات، الأسواق،رأس المال البشرى والبحث، والبنية والتحتية وتطور بيئة الأعمال.وقد جاءت مصر فى المرتبة العاشرة بين 12 دولة عربية على المؤشر فى نفس العام.

<u>ثالثاً: الأدوار الرئيسية فى حوكمة وإدارة الأمن السيبرانى فى مصر</u>

تلقى الدراسة الأضواء على أدوار وزارة الإتصالات وتكنولوجيا المعلومات، والمجلس الأعلى للأمن السيبرانى، والمركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات: EG CERT.

---

(1) ويعتبر المؤشر الإجمالى أحد المؤشرات الرائدة فى بيان أثر تكنولوجيا المعلومات والإتصالات على الاقتصادات الوطنية عبر العالم، ومن بينها مصر، يراجع:
-Portulance Institute (2020). Network Readiness Index 2020 Egypt.Washington. Portulance institute.pp.1-6.

(2) Ibid.

1. وزارة الإتصالات وتكنولوجيا المعلومات – أدوار التحول الرقمى والأمن السيبرانى:

تلعب الوزارة أدوارًا متعددة فيما يتعلق بحوكمة وإدارة الأمن السيبرانى والتمكين الرقمى والتحول الرقمى فى الاقتصاد والمجتمع على وجه العموم، ويوضح الجدول التالى بعض أدوار الوزارة وأجهزتها التابعة فى هذا الخصوص:

جدول (3-4)

"أدوار وزارة الإتصالات وتكنولوجيا المعلومات فى الأمن السيبرانى والتحول الرقمى"

المجالات	إضاءات حول مكونات وتوجهات المجالات
الأمن السيبرانى	• تأسيس المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات:EG-CERT-عام 2012 برئاسة وزير الإتصالات وتكنولوجيا المعلومات.
التحول الرقمى	• تنمية البنية التحتية للإتصالات والمعلومات وتحسين الخدمات الرقمية • 7منصات للتحول الرقمى برعاية وزارة الإتصالات وتكنولوجيا المعلومات: المحتوى والبوابات، أملاك الدولة، البيانات الجغرافية،الموظف الحديث، المدفوعات،الميكنة والخدمات، والبيانات
الإتصالات	• التشريعات والأطر الناظمة: قانون تنظيم الإتصالات + الجهاز القومى لتنظيم الإتصالات NTRA+ سياسات المنافسة + التراخيص. • إدارة الطيف الترددى، للبث الإذاعى والتلفيزيونى وخدمات المحمول
الشمول الرقمى	• توسيع المواطنة الرقمية، والتمكين الرقمى فى المجتمع • **مبادرات هامة:** تمكين ذوى الإحتياجات الخاصة رقمياً من خلال مبادرات وأكاديمية متخصصة + بوابات اليكترونية للتنمية المجتمعية+ إدارة المعرفة الزراعية + التشخيص عن بعد + الإستخدام الآمن للأطفال والناشئة للإنترنت + التنمية المتكاملة من خلال تكنولوجيا المعلومات
تنمية صناعة تكنولوجيا المعلومات الرقمية	• تأسيس هيئة تنمية صناعة تكنولوجيا المعلومات ITIDA عام 2004 • أدوار للهيئة فى مجالات: صناعة خدمات التعهيد + زيادة صادرات خدمات تكنولوجيا المعلومات والإتصالات + جذب الإستثمارات الأجنبية • مشروعات مشتركة+حاضنات أعمال+ محفزات أعمال + تشجيع الإبتكار
الإبداع والإبتكار التكنولوجى	• تأسيس مركز الإبداع التكنولوجى وريادة الأعمال عام 2010 • مركز الإبتكار التطبيقى (تهيئة البيئات للمؤسسات الإبتكارية)
الذكاء الإصطناعى	• تأسيس المجلس الوطنى للذكاء الإصطناعى عام 2019 برئاسة وزير الإتصالات • إعداد الإستراتيجية الوطنية للذكاء الإصطناعى(التمكين + أولويات قطاعية)
بناء وتنمية القدرات	• معهد تكنولوجيا المعلومات + المعهد القومى للإتصالات • مركز تقييم وإعتماد هندسة البرمجيات

المجالات	إضاءات حول مكونات وتوجهات المجالات
	• المركز التنافسى للتعلم الإليكترونى
الهوية الرقمية	• الربط مع مخرجات مجمع الإصدارات المؤمنة والذكية، والذى يعد أحد أدوات الدولة فى دعم التحول الرقمى • بدء مشروعات التحول الرقمى للوثائق والعقارات والشرائح الذكية للسيارات وغيرها

المصدر: مركب بمعرفة الفريق البحثى من موقع الوزارة – https://mcit.gov.eg/ar

وقد القى التقرير السنوى للوزارة بعض الأضواء على بعض الإنجازات الهامة لقطاع الإتصالات وتكنولوجيا المعلومات بقيادة الوزارة فيما يتعلق بالتحول الرقمى والأمن السيبرانى، والتى يمكن إيجازها على النحو التالى [1]:

- **أعلى قطاعات الدولة نمواً رغم الجائحة**، فقد حقق قطاع الإتصالات وتكنولوجيا المعلومات خلال عام 2020/2019 ناتج محلى يقدر بنحو 108 مليار جنيه مقابل نحو 93.5 مليار جنيه فى عام 2019/2018، وذلك بمعدل نمو بلغ نحو 15.2 % خلال عام 2020/2019.
- **تأسيس جامعة معلوماتية متخصصة بشراكات مع جامعات عالمية**، وتعتبر أول جامعة متخصصة في مجالات الإتصالات وتكنولوجيا المعلومات فى أفريقيا والشرق الأوسط في مدينة المعرفة بالعاصمة الإدارية الجديدة، ويتم افتتاحها خلال العام الدراسى المقبل.
- **خطوات متعددة لدعم التحول الرقمى**، الاقتصاد الرقمى، التمكين الرقمى والبنية التحتية:

• **زيادة ملموسة فى حجم استثمارات القطاع**، حيث بلغ إجمالي الاستثمارات المنفذة فى قطاع الإتصالات وتكنولوجيا المعلومات 48.1 مليار جنيه خلال عام 2020/2019 مقابل 35.4 مليار جنيه فى عام 2019/2018 بنسبة زيادة قدرها 35.%.

• **التشغيل التجريبي لمنصة مصر الرقمية – يوليو 2020**، لإتاحة 34 خدمة حكومية رقمية، وزيادتها لتصل إلى 550 خدمة رقمية فى 2023. وقد بلغ بلغ عدد المسجلين على منصة مصر الرقمية نحو مليون مواطن فى يناير 2021.

• **تطوير البنية التحتية للإتصالات وتكنولوجيا المعلومات**، بزيادة الإستثمارات والإعتماد على أفضل التكنولجيات خاصة لدعم التحول الرقمى، ونشر خدمات الإتصالات فى المناطق غير المشمولة(11 منطقة جديدة)، وشبكاتالألياف الضوئية،تطوير سرعات

[1] Ministry of Communication and Information Technology. Op.cit. pp.10-65.

الإنترنت، ومنصات جديدة لجهاز تنظيم الإتصالات، ودعم نظم الشمول المالي الرقمية بالتعاون مع الأجهزة المعنية فى الدولة.

- **شراكات عالمية فعالة،** خاصة مع الجانب الأوروبى والآسيوى، حيث تعد الدول الأوروبية وبعض الدول الآسيوية الأكثر تقدماً في تكنولوجيا الإتصالات والمعلومات بما يدعم جهود مصر فى: التحول الرقمى، بناء وتنمية القدرات البشرية، صناعة الإلكترونيات، المدن الذكية والتقنيات البزغة مثل الذكاء الاصطناعي وإنترنت الأشياء.

- **خطوات هامة لدعم الأمن السيبرانى:**

- **خمسة مشروعات سيبرانية جديدة،** يتم تنفيذها من خلال المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات – EG-CERT، يتم الإشارة عنها لاحقاً.
- **مشاركات سيبرانية عالمية وإقليمية متعددة،** من بينها مؤتمرات ومسابقات، وتتضمن مشاركات مع الإتحاد الدولي للإتصالات – ITU، من خلال المركز الوطنى لطوارىء الحاسبات والشبكات.

2. <u>المجلس الأعلى للأمن السيبرانى:</u>

تم إنشاء المجلس الأعلى للأمن السيبرانى وفق قرار رئيس الوزراء رقم 2259 لسنة 2014 برئاسة وزير الإتصالات وتكنولوجيا المعلومات وعضوية ممثلى عدد كبير من وزارات (10 وزارات) بالإضافة إلى جهاز المخابرات العامة، البنك المركزى المصري، وعدد 3 من ذوى الخبرة فى الجهات البحثية والقطاع الخاص. ويختص المجلس بوضع إستراتيجية وطنية لمواجهة الأخطار والهجمات السيبرانية، والإشراف على تنفيذها وتحديثها، ويرفع التقارير إلى مجلس الوزراء.

وتتلخص أبرز مهام المجلس على النحو التالى:

- إعتماد تحديد البنية التحتية للمعلومات والإتصالات الحرجة فى كافة قطاعات الدولة
- إعتماد أطر وإستراتيجيات وسياسات تأمين البنية التحتية للمعلومات والإتصالات الحرجه
- وضع خطط وبرامج تنمية صناعة الأمن السيبرانى، وإعداد الكوادر اللازمة
- التعاون والتنسيق إقليمياً ودولياً مع الجهات ذات الصلة بالأمن السيبرانى
- وضع المعايير الملزمة لكافة الجهات كحد أدنى لتأمين البنية التحتية الحرجة للإتصالات والمعلومات والزامها بإعداد خطط طوارىء.
- وضع آليات رصد المخاطر والمتابعة الدورية للهجمات السيبرانية وتوزيع الأدوار

- وضع وتفعيل معايير وآليات الإعتماديات البينية الموجودة بين عناصر البنية الأساسية الحرجة والقائمين عليها وما يقع خارجها لتجنب التأثيرات المتتالية.

فى إطار المهام السابقة، قد قام المجلس بإعداد (الإستراتيجية الوطنية للأمن السيبرانى – 2017–2021) والتى تركز، كما يوضح الشكل التالى رقم 3–4، على رصد ومواجهة المخاطر السيبرانية، تعزيز الثقة فى البنية التحتية للمعلومات والإتصالات، وتمهيد الطرق لتوفير بيئة مواتية للتنمية المستدامة.

شكل (3–4)

الأهداف الإستراتيجية للإستراتيجية الوطنية للأمن السيبرانى

المصدر: موقع المجلس الأعلى للأمن السيبرانى https://www.escc.gov.eg/

كما تبنت الاستراتيجية 7 أولويات إستراتيجية (شكل رقم 3–5) تمثل ركائز التوجه الاستراتيجي الوطني لمواجهة الأخطار السيبرانية كما حددتها وثيقة الإستراتيجية الوطنية للأمن السيبرانى.

شكل (3-5)

ركائز التوجه الإستراتيجى للمجلس الأعلى للأمن السيبرانى

المصدر: موقع المجلس الأعلى للأمن السيبرانى https://www.escc.gov.eg/

وقد تم ترجمة الركائز الإستراتيجية السبعة السابق الإشارة اليها فى 6 برامج يوضحها الشكل رقم 3-6 وتشمل: تطوير الإطار التشريعى، منظومة حماية سيبرانية وطنية، حماية الهوية الرقمية، إعداد الكوادر البشرية، البحث العلمى والتطوير، وأخيراً التوعية المجتمعية بالخدمات الإليكترونية وأهمية الأمن السيبرانى.

شكل (3-6)

البرامج الرئيسية للإستراتيجية الوطنية للأمن السيبرانى

المصدر: رئاسة مجلس الوزراء(2017). الإستراتيجية الوطنية للأمن السيبرانى 2017-2021.القاهرة .المجلس الأعلى للأمن السيبرانى. ص6.

3. الجهاز القومى لتنظيم الإتصالات: NTRA [1]

يعتبر هيئة قومية مسئولة عن إدارة وتنظيم قطاع الإتصالات فى مصر وفق مقتضيات القانون رقم 10 لسنة 2003 بإصدار قانون تنظيم الإتصالات، مع مراعاة متطلبات الشفافية، المنافسة الحرة، وحقوق المستخدمين. وللجهاز أدوار هامة فى تعزيز مجتمع المعرفة، وتوفير التنوع الاقتصادي للدولة من خلال قيادته لمنظومة النهوض بصناعة الإتصالات، طبقًا للاختصصات والصلاحيات الممنوحة له. ويتبنى الجهاز رؤية تركز على تطوير سوق الإتصالات وتكنولوجيا المعلومات ليصبح من الأسواق الرائدة عالميا في جودة الخدمات المتاحة للمستخدمين، وفتح آفاق الاستثمار في السوق في ظل بيئة تنافسية عادلة وآمنة.

ولتحقيق هذه الرؤية يتبنى الجهاز المهام التالية:

- وضع الخطط واللوائح والقواعد اللازمة لإدارة سوق الإتصالات وتنظيم العلاقة بين أصحاب المصالح في القطاع: مشغلي الخدمات والمستخدمين؛
- منح التصاريح والتراخيص اللازمة للمشغلين لتقديم خدمات الإتصالات؛
- تحديد معايير جودة الخدمة التي يجب توافرها للمستخدم المصري؛
- مراقبة السوق المصري للتأكد من تطبيق معايير المنافسة العادلة، وجودة الخدمات، والحفاظ على حقوق المستخدمين. ويصدر الجهاز تقارير دورية فى هذا الخصوص لتقييم جودة شبكات المحمول على سبيل المثال، وصدر التقرير الأخير ذى الصلة فى ابريل 2021 [2].
- التحكيم وحل النزاعات بين مشغلي الإتصالات وبعضهم، أو بينهم وبين المستخدمين؛
- التأكد من مراعاة المعايير الصحية والبيئية في التقنيات المستخدمة في السوق المصري.

ويلخص الشكل التالى رقم 3–7 محاور رئيسة لمهام عمل الجهاز السابق العرض لها، وتتركز تلك المحاور على: تنفيذ توجهات وسياسات الدولة والحكومة ذات الصلة، ومراعاة مصالح وخدمات المستخدمين، ودعم أدوار صناعة الإتصالات فى التنمية المستدامة.

---

[1] للتفاصيل حول دور الجهاز – يراجع الموقع الإليكترونى:
- https://www.tra.gov.eg/ar

[2] ويحدد التقرير جوانب القصور والسلبيات فى نوعيات الخدمة المقدمة للجمهور وفق معايير الجودة القياسية التى يضعها الجهاز لهذه الخدمات، يراجع:
الجهاز القومى لتنظيم الإتصالات (2021). تقرير نتائج قساسات شبكات المحمول – تقرير ربع سنوى عن الفترة من يناير 2021- مارس 2021.القاهرة: الجهاز. ص 1-178.

شكل (3-7)

المحاور الثلاثة لمجالات عمل الجهاز القومى لتنظيم الإتصالات

المصدر : https://www.tra.gov.eg/ar

بالإضافة إلى ذلك، يلعب الجهاز أدواراً محورية فى مجال الأمن السيبرانى من خلال المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات، والتى سنعرض لها فى البند التالى. كما يلعب الجهاز أدوراً هامة فى تعزيز وتهيئة البيئة للثورة الصناعية الرابعة من خلال أدواره الرئيسية في تنظيم سوق الإتصالات والخدمات الرقمية والعمل على وضع الضوابط التنظيمية في ضوء المعايير القياسية لخدمات الإتصالات والخدمات الرقمية بما يتماشى مع أفضل المعايير العالمية على النحو الذى يضمن توفير على الاتصال الآمن الفعال، وضمان المنافسة الحرة بين مقدمي الخدمات.

4. أدوار المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات – EG CERT

تم تشكيل المركز ضمن الجهاز القومى لتنظيم الإتصالات فى أبريل عام 2009، ليقدم خدمات الدعم اللازم لحماية البنية التحتية القومية للمعلومات خاصة في قطاع تكنولوجيا المعلومات والإتصالات والقطاع المالي، والاستعداد لطوارئ الحاسبات والشبكات ومراقبة الأمن السيبراني والإستجابة للحوادث، والتنبؤ بالاخطار وإصدار تحذيرات مبكرة عن إنتشار البرمجيات الخبيثة والهجمات واسعة النطاق التي تهدد البنية التحتية للاتصالات فى الدولة. والمركز ممثل فى الهيئة الوطنية للإعلام وله دور هام فى حماية الأطفال على الشبكة. ويمكن تصنيف خدمات المركز فى أربعة أنواع وفق الجدول رقم(3-5).

جدول (3-5)

الخدمات النوعية للمركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات

نوعية الخدمات	طبيعة الخدمات
خدمات استباقية	• الإختبارات والإجراءات للكشف المبكر عن الهجمات السيبرانية • الإجراءات والتدابير الإستباقية بما فيها فحص التطبيقات • يصدر المركز تقارير تحذيرية سنوياً (قد تصل إلى 200 تقرير)
خدمات تفاعلية	• اتخاذ الإجراءات وتقديم الدعم للقطاعات للتصدى للهجمات السيبرانية • إجراءات التخفيف من آثار وأضرار الهجمات
خدمات الطب الشرعى الرقمى	• التحقيق الجنائى الرقمى والتحقيقات السيبرانية لدعم انفاذ القانون • فحص جرائم الحاسب الإلى وإعداد التقارير الفنية عنها
التوعية الأمنية الإليكترونية	• برامج للتوعية الأمنية الإليكترونية حول التهديدات السيبرانية • رفع وعى واستشعار المستخدم العادى بالمخاطر السيبرانية • اصدار نشرات تحذيرية من البرمجيات الخبيثة

المصدر: مركب بمعرفة الفريق البحثي من موقع المركز – https://www.egcert.eg/ – وإضافات من نتائج

ويمكن اعتبار المركز الوطني بمثابة الذراع التنفيذي والفنى للمجلس الأعلي للأمن السيبرانى، كما تشارك فرق المركز – ممثلة لمصر – فى المنتديات والمحافل الدولية والإقليمية ذات الصلة، ويقدم المركز كذلك الدعم الفني للفرق المناظرة فى الدول الأخرى خاصة فى أفريقيا.

ورغم الدور المحورى للمركز فى دعم الأمن السيبرانى فى الدولة فإن وقائع ورشة عمل الخبراء التى نظمها المعهد (فبراير 2021–ملحق الدراسة) تشير إلى أن المركز يواجه تحديات جدية فى الواقع العملى ترتبط على الخصوص بعدم تفهم العديد من الجهات الحكومية على الخصوص لطبيعة أدوار أدوار المركز الخدمية، وليس الرقابية أو التدقيقية، بما يقلص الطلب على خدماته الهامة دون مبرر موضوعى،. والمركز ممثل فى الهيئة الوطنية للإعلام وله دور هام فى حماية الأطفال على الشبكة.

ويشير التقرير الأخير لوزارة الإتصالات وتكنولوجيا المعلومات إلى بعض المشروعات الهامة التى يتبناها المركز لتعزيز الأمن السيبرانى الوطنى، وأبرزها[1]:

- الدرع الإلكتروني المصري Egyptian Cyber Shield
- المشروع المصري لفحص الأنظمة IP Scanner
- مشروع أمن الأنظمة اللاسلكيةWireless Systems' Security Project

[1]Ministry of Communication and Information Technology. Op.cit. pp.60-61.

- المشروع المصري لمكافحة البرمجيات الخبيثة Egyptian Anti-Malware Project
- مشروع منصات اختبار الاختراقات Vspect
- نظام الإنذار المبكر عن الهجمات الإلكترونية Cyber Attacks Early Warning System

5. هيئة تنمية صناعة تكنولوجيا المعلومات ITIDA

تلعب الهيئة أدواراً هامة فى تنمية صناعة تكنولوجيا المعلومات وتشمل برامجها تقديم المشورة وإنفاذ السياسات والترويج التجاري في الأسواق الإقليمية والعالمية وتقديم الاستشارات الاستراتيجية للشركات الصغيرة والمتوسطة والشركات متعددة الجنسيات، مما يُسهم في النمو الاقتصادي للبلاد.

ويلقى الجدول التالى بعض الأضواء حول محاور عمل الهيئة المختلفة والتى تشمل: تأسيس الأعمال، تطوير الأعمال،الوصول إلى الأسواق، وتنمية القدرات والمهارات، وهى المحاور التى يدعمها العديد من المراكز النوعية المتخصصة فى الهيئة [1].

جدول (3–6)

محاور عمل هيئة تنمية صناعة تكنولوجيا المعلومات

محاور العمل الرئيسية	محاور العمل الفرعية
تأسيس الأعمال	• مشروعات مشتركة ممولة (تعزيز التعاون بين الشركات والجامعات لدعم الاقتصاد الرقمى). • حاضنات تكنولوجية.(من خلال مركز الإبداع وريادة الأعمال) • برنامج محفزات الأعمال (دعم الأفكار والبدايات فى ريادة الأعمال) • برنامج دعم التعاون البحثى + برنامج الإبتكار المصري الأسبانى
تطوير الأعمال	• برنامج دعم الصادرات المصرية (تشجيع شركات تكنولوجيا المعلومات فى الوصول إلى الأسواق الخارجية) • خدمات SECC الإستشارية (مركز تقييم وإعتماد هندسة البرمجيات)
الوصول إلى الأسواق	• المناقصات الإلكترونية (تحميل وثائق الممارسات العامة للوزارة) • أحداث مجمعة. (قائمة بالفعاليات والمؤتمرات وغيرها ذات الصلة)
تنمية القدرات والمهارات	• تدريب البرمجيات (لطلبة الجامعات فى الصفوف النهائية) • مشاريع التخرج (ربط الطلاب بالشركات بمشروعات بحثية) • تدريب الألياف الضوئية (تأهيل فنيين متخصصين)

[1] للتفاصيل يراجع موقع الهيئة:
-https://itida.gov.eg/Arabi

محاور العمل الرئيسية	محاور العمل الفرعية
	• مبادرة التعلم التكنولوجى (قاعدة بيانات لمهارات تكنولوجيا المعلومات) • التدريب الصيفى (تزويد الطلاب بأحدث الإتجاهات التكنولوجية) • تدريب اللغة الإلمانية (دعم الطلاب للتواصل الخارجى الفنى)
خدمات الدعم	• مكتب حماية حقوق الملكية الفكرية • منطقة المعادى التكنولوجية (منطقة استثمارية تكنولوجية مشتركة) • دعم المنظمات المدنية (التوعية والتدريب لدعم المنظمات غير الحكومية) • التوقيع الإليكترونى (من خلال مركز نوعى لتميز التوقيع الإليكترونى) • واحات السليكون (من خلال شركة واحات السليكون بالتعاون مع هيئة المجتمعات العمرانية الجديدة) • مجمعات الإبداع (لتحفيز شراكات القطاعين فى المناطق التكنولوجية)
الإستثمار فى مصر	• خدمات التعهيد (لتحفيز نشاط الشركات متعددة الجنسية فى مصر) • صناعة الإليكترونيات (بهدف مضاعفة الصادرات التكنولوجية) • حملات ترويجية (منها حملة: Time of Egypt)

المصدر: مركب من موقع الهيئة – يراجع /https://itida.gov.eg

بالإضافة إلى تلك الأنشطة، فقد أطلقت الهيئة مبادرة هامة (مبادرة فرصتنا رقمية)، والهادفة إلى تشجيع المشروعات المتوسطة والصغيرة لتنفيذ مشروعات التحول الرقمى فى مصر بما يعزز دور قطاع تكنولوجيا المعلومات والإتصالات فى تنمية فرص الاقتصاد الرقمى فى مصر.

ويمكن الإشارة بوضوح إلى أن قضايا (أمن المعلومات – الأمن السيبرانى) غير مطروحة بصورة أو أخرى فى أنشطة الهيئة المتعددة، وهو الأمر الذى يحتاج إلى المراجعة فى المرحلة القادمة حيث يمكن للهيئة أن تلعب دوراً محورياً فى طرح فرص استثمارية فى مجال أمن المعلومات خاصة لريادة الأعمال، أو من خلال المشاركات المحلية والخارجية. كما يمكن للهيئة أن تساهم فى جهود بناء وتنمية القدرات فى مجال الأمن السيبرانى بالتعاون مع المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات.

6. <u>البنك المركزي المصري – الحوكمة السيبرانية وأمن المعلومات فى القطاع المالي المصري [1]:</u>

تندرج أولويات (أمن المعلومات) فى البنك المركزى المصري فى إطار أولويات أوسع لإدارة المخاطر فى البنك والتى تأسس لها إدارة مركزية متخصصة عام 2010 تقوم على صيانة السمعة والصورة الذهنية للبنك من خلال تبنى نظم فاعلة للرقابة وإدارة المخاطر الحالية والمستقبلية التى يمكن أن يتعرض لها البنك وتقديم التوصيات اللازمة للتعامل مع تلك المخاطر. وتتوزع تلك المخاطر بين: مخاطر الإئتمان، مخاطر السوق، مخاطر التشغيل، ومخاطر أمن المعلومات.

وبخصوص **(أمن المعلومات)** يسعى البنك لتوفير المتطلبات الأمنية اللازمة لحماية أصوله المعلوماتية وفقاً للمعايير الدولية والقوانين واللوائح الخاصة بأمن المعلومات، وذلك بهدف توفير بيئة عمل آمنة تساعد على تحقيق إستراتيجية وأهداف البنك المركزي فى إطار الأهداف العامة للدولة والتنمية المستدامة من خلال مبادرات تهدف لتعزيز الإعتماد على التكنولوجيا الرقمية ومواكبة الاقتصاد الرقمي بأشكاله المختلفة وتشجيع المعاملات المالية الرقمية.

ولتحقيق الأهداف السابقة تقوم إدارة أمن المعلومات بالبنك المركزى بالمهام التالية:

أ. **حوكمة أمن المعلومات،** بوضع إستراتيجية متكاملة لتعزيز البيئة الآمنة للمعلومات بالبنك.

ب. **خلق الوعي وإدراك التنسيق الفعال بين كافة المستويات الإدارية بالبنك،** من خلال تطبيق أفضل المعايير الدولية التى تهدف إلى الحفاظ على الأصول المعلوماتية.

ت. **إدارة فعالة لمخاطر أمن المعلومات،** بهدف إلى الحد من تلك المخاطر وتوفير الضوابط اللازمة ووسائل المراقبة لحمايتها.

ث. **توعية العاملين فى البنك بمخاطر أمن المعلومات،** والتعريف بأدوارهم ومسئولياتهم تجاه حماية سرية وتوافر وسلامة أصول المعلومات الخاصة بالبنك، بما يعزز توجهات البنك المركزي لتقديم كافة الخدمات والمعاملات المالية بشكل إلكتروني.

ج. **التأكد من متابعة الإدارة العليا لتطورات "أمن المعلومات"**، بهدف ضمان تحقيق والحفاظ على الأمن المعلوماتي في البنك المركزي.

ولم يقتصر الأمر على الاهتمام بأمن المعلومات فى القطاع المالي المصري على توجهات البنك المركزى فقط، بل شهد القطاع المصرفى والتأمينى توجهات أخرى من بينها:

---

[1] وتعتبر الإدارة العليا للبنك المركزي المسئولة عن تحديد درجة تقبل المخاطر ودرجة تحملها، يراجع: موقع البنك المركزى المصري - https://www.cbe.org.eg/ar

أ) **اهتمامات واسعة بتمكين الأمن السيبرانى فى البنوك المصرية،** حيث تترجم تلك البنوك قواعد وتعليمات البنك المركزى السابق الإشارة اليها، ويقوم كل بنك بتعيين مسئول أمن سيبرانى، كما تهتم البنوك المصرية بتطبيق عمليات المراجعة بما فيها المراجعة على نظم المعلومات IT Audit، والاهتمام بتطبيق المواصفات الدولية ذات الصلة مثل: ISO 27001. كما تقوم البنوك المصرية بالتعاون مع البنك المركزى بجهود متعددة لتوعية (العميل الداخلى) و(العميل الخارجى) بخصوص قضايا الأمن السيبرانى، ويضطلع المعهد المصرفى بدور هام فى توفير تدريب متخصص فى مجال الأمن السيبرانى [1].

ب) **اهتمام البورصة المصرية بقضايا الأمن السيبرانى،** حيث تفرض هيئة الرقابة المالية قواعد ومتطلبات للأمن السيبرانى تخص شركات السمسرة والوساطة المالية. كما أن هناك توعية مستمرة للعاملين بخصوص الأمن السيبرانى خاصة فى التعامل مع البريد الإليكترونى [2].

ت) **استحداث خدمات تأمين ضد المخاطر السيبرانية،** فقد أعلن رئيس الهيئة العامة للرقابة المالية أن هناك شركتين تقدمتا إلى الهيئة بوثائق تأمين جديدة ضد الهجمات الإليكترونية (السيبرانية)، إحداهما مصرية، والثانية أجنبية، للإسراع بطرحها فى السوق، سعياً سعيا لإيجاد تأمين ضد مخاطر القرصنة الإلكترونية. كما أن هناك مباحثات مستمرة مع البنك المركزى لبحث أطر التأمين، على الهجوم الإلكتروني، الذي يستهدف تأمين البنوك ضد مخاطر هذا النوع من الهجمات، ووضع آليات التنفيذ مع البنوك المصرية.

ث) **جهود الإتحاد المصري للتأمين بخصوص الأمن السيبرانى فى قطاع التأمين،** فى هذا السياق عقد الإتحاد ندوة حول: " التأمين على الجرائم الإليكترونية" cyber risks " عام 2020 بالإستعانة ببعض الخبراء الدوليين. كما قام الإتحاد المصري للتأمين بنشر مجموعة من النشرات المميزة حول هذا الموضوع الهام، وقدمت اللجنة العامة لتأمينات الحوادث المتنوعة بالإتحاد المصري للتأمين ورقة بحثية حول أهم التغطيات التأمينية التي يمكن ان يتم تقديمها لمنظومة الدفع الالكتروني التي تسعي الدولة الي الانتقال لها تدريجيا خلال الفترة القادمة وذلك برعاية المجلس القومي للمدفوعات.

---

(1) مع التأكيد على الحاجة لمزيد من الوقت لنضج الوعي السيبرانى فى القطاع المصرفى، يراجع: ورشة الخبراء حول الأمن السيبرانى – معهد التخطيط القومى – فبراير 2021. (ملحق الدراسة)

(2) المرجع السابق مباشرة.

ثانياً: أدوار ومبادرات أخرى متعددة

1- **لجنة تكنولوجيا المعلومات والاتصالات – مجلس النواب المصري:** والتى تناقش فى الآونة الراهنة مشروع قانون جديد لتنظيم التجارة الإليكترونية.

2- **مركز المعلومات ودعم اتخاذ القرار: حيث يعطى المركز أنشطة أمن المعلومات إهتماماً خاصاً لدعم الجهات الحكومية فى مجال التحول الرقمى من خلال النظم والتطبيقات وأمن المعلومات، كما يساهم المركز فى التوعية المجتمعية بخصوص المخاطر السيبرانية حيث نشر أوراقاً بحثية حول الجرائم الإليكترونية عام 2018، والإختراقات السيبرانية فى 2020.**

3- **أدوار التنظيمات والجمعيات المدنية / الأهلية وريادات الأعمال، وقد شارك فى فعاليات ورشة الخبراء بالمعهد نماذج من ريادات الأعمال المصرية، ومنها:**

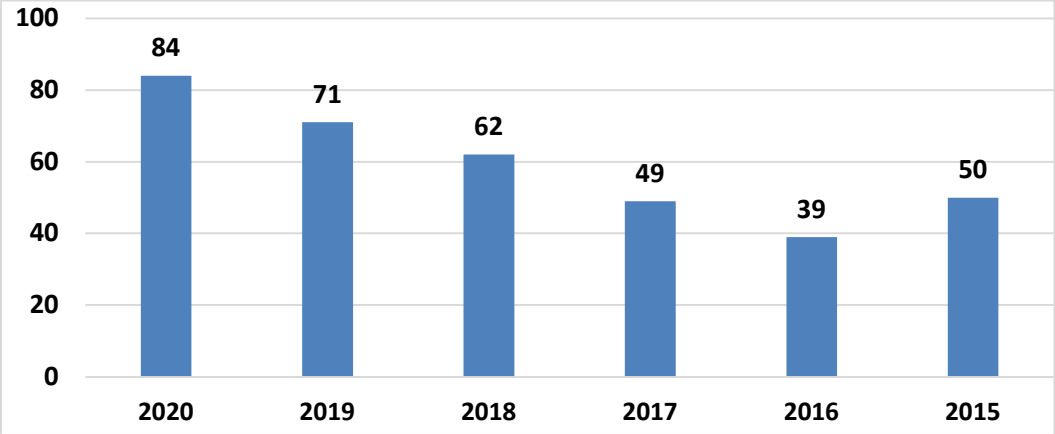
- **النموذج الأول: شركة Digital Planets:** ويمتد نشاطها بين مصر، الإمارات، ولندن فى مجال الخدمات الأمنية المدارة بالشراكة مع شركات عالمية لتقديم الحلول ذات الصلة. بالإضافة إلى شراكات محلية مع (ايتيدا) والمصرية للإتصالات (جوائز)، والإستثمار فى التدريب السيبرانى.
- **النموذج الثانى: شركة ISEC:** ولها إهتمامات خاصة بالتدريب ونشر الوعى السيبرانى بالتعاون مع شركات عالمية، والتعاون مع مؤسسات تعليمية أكاديمية. بالإضافة إلى أنشطة على المستوى العربي (المؤتمر العربي لأمن المعلومات).

ثالثاً: أدوار البحث العلمى المساند:

أدوار النشر العلمى الدولي للباحثين المصريين فى مجال الأمن السيبرانى، سبقت الإشارة فى الفصل الثانى إلى المساهمات العلمية الدولية فى مجال الأمن السيبرانى وأمن المعلومات بما فيها المساهمات العلمية المصرية. ويلقى الشكل التالى 3-8 بعض الأضواء على اسهامات الباحثين المصريين فى مجال الأمن السيبرانى وأمن المعلومات، حيث تم نشر 355 بحثاً خلال الفترة من 2015 وحتى 2020 بحسب قاعدة البيانات العلمية Web-of-Science. كما يظهر الشكل نمواً سنوياً فى السنوات الأربعة الأخيرة حيث شهد عام 2020 أكبر عدد من المشاركات للباحثين المصريين من خلال 84 مشاركة.

شكل (3-8)

تطور المشاركات العلمية الدولية للباحثين المصريين فى مجال الأمن السيبرانى من حيث عدد الأبحاث المنشورة في مصر



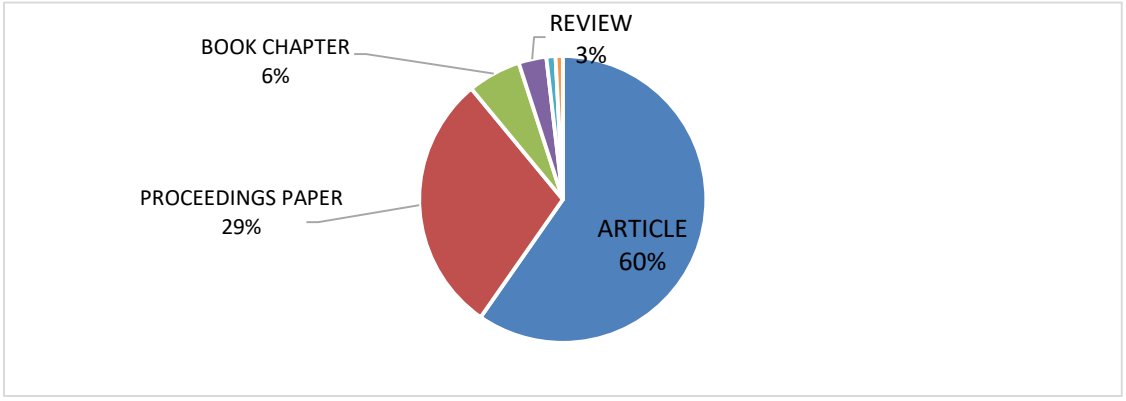
المصدر: مركب بمعرفة الفريق البحثى فى يناير 2021 من:https://access.webofknowledge.com

كما يوضح الشكل التالى 3-9، أن النسبة الأكبر من هذه الأبحاث والمساهمات المصرية قد تم نشرها فى صورة مقالة "Article" بنسبة 60%، أما الأبحاث التى تم نشرها من خلال مؤتمرات علمية "Paper Proceedings" فتصل نسبتها إلى حوالى 29%. كما يوضح تقسيم/تصنيف قاعد البيانات Web-of-Science، فأن أهم المجالات التي تضمنتها تلك الأبحاث على التوالى تشمل: مجال علوم الحاسب –Computer science، يليه مجال الهندسة –Engineering، ثم مجال الإتصالات – Telecommunications.

شكل (3-9)

نوعيات أبحاث النشر الدولي للباحثين المصريين فى مجال الأمن السيبرانى

(توزيع الأبحاث ح سب نوعية البحث)



المصدر: مركب بمعرفة الفريق البحثى فى يناير 2021 من:https://access.webofknowledge.com

رابعاً: أدوار متعددة لأكاديمية البحث العلمى والتكنولوجيا

- **دور مجلس الإتصالات وتكنولوجيا المعلومات،** والذى يهتم بقضايا متعددة مثل: معالجة البيانات الكبيرة، وانترنت الأشياء، وشبكات المجسات اللاسلكية، ووسائط التواصل الإجتماعى، وتكنولوجيا المعلومات صديقة البيئة.
- **دور المركز الوطنى لخدمات الحوسبة السحابية،** ويقدم خدمات الحوسبة السحابية لدعم البحث العلمى بالتعاون مع جهات معنية محلية وخارجية خاصة الأوروبية.

خامساً: جهود بناء القدرات وتنمية الكوادر البشرية والوعى السيبرانى،

- **إطلاق (أكاديمية الأمن السيبراني)** بين المعهد القومي للاتصالات وشركة سيسكو مصر برعاية وزارة الإتصالات وتكنولوجيا المعلومات Cisco –NTI Cybersecurity "Academy. وتعمل الأكاديمية الجديدة على نشر وغرس وتطبيق مهارات الأمن السيبرانى لتحسين جاهزية التعامل مع التحديات العالمية فى هذا الخصوص فى مصر.

ويعتبر المعهد القومي للإتصالات:NTI أحد المعاهد المتخصصة المسئولة عن توفير أنواع مختلفة من اللتدريب ورفع المهارات فى مجال الإتصالات والمعلومات فى مصر بما فيها الأمن السيبرانى[1].

- **مبادرة الأمن السيبرانى المجانية بتقنية التعلم عن بعد،** من خلال تعاون ثلاثى بين وزارة الإتصالات وشركة سيسكو العالمية Cisco وجامعة بنها لتعزيز الثقافة الرقمية للتعامل مع البيانات واستخدام شبكة الانترنت بشكل آمن بما يساهم في تدعيم حماية البيانات الشخصية والخصوصية عند استخدام وسائل الاجتماعات والتواصل عبر الانترنت.

(1) للتفاصيل يراجع موقع المعهد:https://www.nti.sci.eg /

نتائج الفصل الثالث

- **إهتمام رئاسى بالأمن السيبرانى،** حيث أكد رئيس الدولة فى أكثر من مناسبة(أحدثها – مارس2021)على أهمية الأمن السيبران والحفاظ على الأول الرقمية والمعلوماتية للدولة.
- **رؤية دستورية ثلاثية الأبعاد لأمن المعلومات الوطنى،** حيث يربط الدستور بين أمن المعلومات وأبعاد: الاقتصاد الرقمى،الأمن القومى، بالإضافة لدور الدولة الحاكم فى أمن المعلومات.
- **أطر تشريعية متعددة وفجوات تشريعية قائمة،** وأحدثها قانون لحماية البيانات الشخصية(151 لسنة 2020)، ومكافحة جرائم تقنية المعلومات(قانون 175 لسنة 2018)، وتبقى بعض المتطلبات التشلريعية الجديدة اللازمة، وتعديلات فى بعض التشريعات القائمة.
- **أطر تخطيطية متعددة ذات صلة تنتظر الإرتباط الإستراتيجى والتنفيذى،** حيث تتعدد الاهتمامات بدور المعلومات فى تنمية الاقتصادات الرقمية فى وثائق التنمية المختلفة مع إهتمام أقل بالأمن السيبرانى / أمن المعلومات فى إطار رؤى إستراتيجية تترجم إلى برامج عملية يتم تنفيذها فى اطار مديات زمنية محددة ويتم متابعتها وتقييم أدائها من خلال مؤشرات محددة.
- **إستراتيجية وطنية للأمن السيبرانى 2017–2022**، وتمثل تطور نوعى فى تعامل الدولة مع الأمن السيبرانى وصادرة عن (المجلس الأعلى للأمن السيبرانى) تركز على قضايا الأمن الحوسبى والسيبرانى، وتضم الإستراتيجية 7 أولويات تمت ترجمتها فى 6 برامج نوعية.
- **تحسن فى عديد من مؤشرات الإتصالات والمعلومات**،خاصة إنتشار الهواتف المحمولة 93.6%، وإنتشار الإنترنت 57.3%، وتغطية مناطق محرومة من خدمات الإتصالات(11 منطقة).
- تباينات فى مؤشرات الأمن السيبرانى والإتصالات والمعلومات المحلية والعالمية،
  - تحسن فى التعامل مع الهجمات السيبرانى من جانب المركز الوطنى، مع تفاوتات فى مستوى خطور الهجمات حيث تتصدر هجمات حجب الخدمات: DDoS بنسبة 43.8%، وهجمات البرامج الضارة 21%،وهجمات المواقع 19%.
  - تحسن فى مؤشر القوة السيبرانية الوطنية **NCPI** عام 2020، وتحسن فى بعض جوانب مؤشر الأمن السيبرانى العالمي مع ثبات الترتيب العالمي والعربي، كذلك مؤشر جاهزية الحكومة للذكاء الإصطناعى ومؤشر المعرفة العالمي.
  - تراجعات فى مؤشرات أخرى منها: مؤشر الإبتكار العالمي GII، مع العديد من التحديات على مؤشر الجاهزية الشبكية:**NRI** .

- **دور محـورى لـوزارة الإتصـات وتكنولوجيـا المعلومـات وأجهزتهـا**، فـى مجـالات الأمـن السـيبرانى،التحول الرقمـى، الشـمول الرقمـى، الهويـة الرقميـة، تنميـة صـناعة تكنولوجيـا المعلومات والإتصالات، الإبداع التكنولوجى والذكاء الإصطناعى، والتدريب وبناء القدرات.
- **تطورات ايجابية لقطاع تكنولوجيا المعلومات والإتصالات**، حيث حقق أعلى معدلات النمو مقارنة بالقطاعات الأخرى بالدولة رغم جائحة كورونا، وتمت زيادة استثمارات القطاع، وأطلق منصـة مصـر الرقميـة –يوليـو 2020، مـع تطـويرات واسـعة فـى البنـة التحتيـة، وتنويـع الشراكات الإقليمية والعالمية.
- **دور محـورى وتحـديات للمركـز الـوطنى للإسـتعداد لطـوارىء الحاسـبات:EG-CERT**، وتأسس عام 2009 ليلعب دور الذراع التنفيذى والفنى للمجلس الأعلى للأمن السيبرانى، ويتبنى مشروعات هامة (الدرع الإليكترونى، مكافحة البرمجيات الخبيثة وغيرها)، كما يواجه تحديات فى تفهم أدواره بصورة صحيحية انعكست فى نقص الطلب المجتمعى على خدماته.
- **أدوار هامة للبنك المركزى فى الحوكمة السيبرانية فى القطاعات الماليـة**، حيث أسس إدارة مركزية لأمن المعلومات عام 2009 لدعم الرقابة وإدارة مخاطر أمن المعلومات فى القطاع المصرفى وتمكين البنوك العاملة فى مصر من حماية أصولها الرقمية.
- **توجهات لتعزيز الأمن السيبرانى فى مجال** أعمال **البورصة والتأمين**، من خلال مبادرات للتوعيـة وضـوابط وقواعـد ذات صـلة للبورصـة المصـرية، بالإضـافة إلـى مبـادرات لأمـن المعلومات وخدمات التأمين على مخاطر المعلومات من جانب الإتحاد المصري للتأمين وغيره.
- **جهـود ومبـادرات عديـدة مسـاندة لتعزيـز الأمـن السـيبرانى**، ومن بينها الجهود التشريعية بمجلـس النـواب المصـري (لجنـة الإتصـالات وتكنولوجيـا المعلومـات)، ومبـادرات لمركـز المعلومـات ودعـم اتخـاذ القرار،التنظيمـات المهنيـة المعنيـة، الأجهـزة والمجـالس العلميـة المختلفة.
- **فجوات فى إقتصاد وصناعة الأمن السيبرانى**، سواء فى صناعة البرمجيات والأجهزة ذات العلاقة بتأمين المعلومات والإتصالات والدفاع السيبرانى، واكتشاف الثغرات وغيرها.

الفصل الرابع

نتائج الدراسة وسياسات بديلة مقترحة وقضايا جديرة بالدراسة

أولاً: نتائج الدراسة

1. نتائج خاصة بقضايا المفاهيم وعلاقة الأمن السيبرانى بالنظام الدولي والقطاع المالي

- **أهمية مفاهيم الأمن السيبرانى على كافة الأصعدة**، فهى مقدمات وأدوات لازمة لفهم العالم الجديد الذى يزداد ترابطاً من خلال الشبكات والنظم وسلاسل القيمة الرقمية والتقنيات البازغة العابرة بتشابكاتها للحدود، والتى تحمل (القيمة الرقمية العالمية الجديدة) و(الأصول العالمية الرقمية الجديدة)، كما تحمل معها (المخاطر والمهددات السيبرانية الجديدة) فى نفس الوقت.
- **جوهر الأمن السيبرانى**، ويعبر عن قدرة الدول والمنظمات على حماية أنظمة المعلومات والإتصالات والمعلومات والدفاع عنها ضد المخاطر السيبرانية بكفاءة وأقل الأضرار والتكلفة.
- **دوائر تماس واسعة للأمن السيبرانى**، حيث ترتبط بإرتباط 27 مليون جهاز فى العالم بالإنترنت نهاية عام 2021، واستخدام 66% من سكان العالم للهاتف المحمول، وتمدد الاقتصادات الرقمية، وإنتشار التقنيات البازغة وتقنيات الجيل الخامس G5، وغيرها.
- **ترابط الأمن السيبرانى مع أشكال أخرى من الأمن**، حيث يتجاوز أمن الأنظمة والتطبيقات والشبكات إلى: الأمن الفضائى،الأمن الجنائى، الأمن العسكرى، الأمن الجيوسياسى، الأمن الاقتصادى، الأمن الإجتماعى، الأمن البيئى، والأمن الشخصى للمواطن العادى.
- **تنوع المهددات السيبرانية وفداحة تداعياتها**، ومنها الهندسة الإجتماعية،هجمات الفدية،هجمات حجب الخدمات،هجمات الحوسبة السحابية، التصيد والبرامج الضارة، وغيرها، والتى كلفت العالم أكثر من 5 تريليون دولار عام 2020، يتوقع صعودها إلى 6 تريليون عام 2021.
- **تنوع وتطور أدوات الحماية ضد الهجمات السيبرانية**، مع تقدم وتطور الهجمات ذاتها، وتنقسم إلى أدوات الدفاع عن الشبكة، وأدوات فحص ثغرات الويب أو غيرهما من الأدوات.
- **تعولم مخاطر الأمن السيبرانى يهدد النظام العالمي**، وهناك إدراك عالمى متصاعد بخطورة المهددات السيبرانية للإقتصاد العالمي وبنية النظام العالمي، وهناك محاولات من الأمم المتحدة والإتحاد الأوروبى وغيرهما لترتيب نوع من الإصطفاف العالمي ضد هذه المخاطر المتصاعدة.

- **الحوكمة السيبرانية العالمية مطلب ملح**، وقد ظهرت مبادرات متعددة فى هذا الخصوص للأمم المتحدة ووكالاتها، والمنتدى الاقتصادى العالمي، وقمم مجموعة العشرين G20.
- **علاقة الأمن السيبرانى بحقوق الإنسان**، وهو ملف عالمى مطروح لضمان عدم الجور والإجتراء على حقوق المقررة الإنسان وفق المواثيق الدولية بحجة تعزيز الأمن السيبرانى ودرء مخاطره.
- **الدبلوماسية السيبرانية والرقمية**، مداخل مطروحة لتجنب انزلاق العالم لفوضى سيبرانية لضعف التواصل، ونقص تبادل المعلومات والخبرات ورص الصفوف لمواجهة المخاطر السيبرانية.
- **فداحة الخسائر السيبرانية فى القطاعات المالية**، حيث تتكبد المؤسسات المالية أكثر من 9% من صافى دخولها نتيجة الهجمات السيبرانية بما يفرض تحديات متصاعدة وغير مسبوقة على القطاعات المالية فى العالم، وتفرض أولويات جديدة على هذه القطاعات.
- **مبادرات متعددة لحوكمة الأمن السيبرانى فى القطاعات المالية**، سواء لصندوق النقد الدولي، البنك الدولي، بنك التسويات الدولية، مجلس الإستقرار المالي ولجنة بازل للرقابة المصرفية، المنظمة الدولية لهيئات الأوراق المالية، وغيرهم.
- **مخاطر سيبرانية جدية فى القطاعات المالية العربية**، وتتطلب مداخل غير تقليدية للتعامل معها وتضمين إدارة المخاطر السيبرانية ضمن إستراتيجيات وسياسات المصارف العربية، بناء وتنمية القدرات السيبرانية، تبادل الخبرات والمعلومات بين المؤسسات المالية الوطنية والعربية.
- **أهمية المؤشرات العالمية للأمن السيبرانى**، حيث تلقى بعض الأضواء على جوانب القوة والضف وفرص التحسين، ومن أبرزها: مؤشر الأمن السيبرانى العالمي:GCI للإتحاد الدولي للإتصالات، ومؤشر القوة السيبرانية الوطنية: NCPI لمركز بلفر.
- **الإرتباط الإيجابى بين الأمن السيبرانى والاقتصادات الرقمية والتنمية المستدامة**، حيث تمثل البنية التحتية للمعلومات والإتصالات والتقنيات البازغة المكون الرئيس لهذه الاقتصادات الصاعدة، كما تمثل فى ذات الوقت أحد أدوات الأمم المتحدة لتسريع انجاز التنمية المستدامة وفق مؤتمرات الذكاء الإصطناعى للصالح العالم التى نظمتها المنظمة فى السنوات الأخيرة.

- خبرات متعددة مستفادة لمصر،

- نشر ثقافة الوعى السيبرانى على التوازى مع توسع استخدام تكنولوجيا المعلومات والإتصالات والتكنولوجيات البازغة فى الاقتصاد والمجتمع فى مصر.
- تبنى رؤية متكاملة لإدارة البيانات على المستوى القومى وكافة الجهات والأجهزة المعنية فى الدولة العامة والخاصة

- تبنى نظم متكاملة لإدارة المخاطر بوجه عام والمخاطر السيبرانية على وجه الخصوص فى المؤسسات العامة، ومؤسسات قطاعات الأعمال والمنظمات غير الحكومية.
- أهمية الإنخراط بقوة أكبر فى الحوارات والمبادرات العالمية ذات الصلة بالأمن السيبرانى
- تفعيل الدبلوماسية السيبرانية والرقمية، وأدوار مأمولة فاعلة للخارجية المصرية
- متابعة موقف مصر على المؤشرات العالمية ذات الصلة والعمل على سد الفجوات
- توفير تمويل كاف للإنفاق على أمن المعلومات كنسبة من الإنفاق على الأنظمة والشبكات والنظم والبنية التحتية المعلوماتية.

2. <u>نتائج خاصة بالأدوار العالمية المؤثرة، وتحليل التجارب الوطنية لدول العالم المتقدمة والناهضة والنامية فى التعامل مع الأمن السيبرانى</u>

- **دور محورى للأمم المتحدة ووكالاتها المتخصصة فى الأمن السيبرانى،** وعلى الأخص من خلال آليات متابعة تنفيذ مقررات القمم العالمية لمجتمع المعلومات والمعنية بالتعامل مع مخاطر أمن المعلومات، وتشكيل فرق عمل وطنية للإستجابة للحوادث السيبرانية.
- **أولويات أممية لحوكمة مخاطر الإنترنت والتكنولوجيات البازغة لدعم التنمية المستدامة،** ويبرز فى هذا الخصوص مؤتمرات الذكاء الإصطناعى للصالح العام AI 4 GOOD بين عامى 2017–2019 والشراكة العالمية لتفعيل دور تكنولوجيا المعلومات والإتصالات فى التنمية المستدامة.
- **أدوار رائدة للإتحاد الدولي للإتصالات: ITU،** فى مجالات خطط وإستراتيجيات الأمن السيبرانى، المؤشرات والإحصاءات، التعامل السيبرانى مع جائحة كورونا، والحماية السيبرانية للمرأة والشباب والطفل، بخلاف المبادرات السيبرانية الإقليمية .
- **مبادرات أمنية سيبرانية إستراتيجية – دور حلف شمال الأطلنطى NATO،** بتكريس منظومات الدفاع السيبرانى جزء لا يتجزء من المنظومات الدفاعية للحلف وللدول الأعضاء على السواء.
- **مبادرات سيبرانية إقليمية أوروبية،** ومنها تأسيس وكالة أوروبية للأمن السيبرانى: **ENISA،** وإستراتيجية أوروبية للبيانات 2020، ومعايير سيبرانية للجيل الخامس5G–2021.
- **توجهات سيبرانية إقليمية أفريقية غير كافية،** ضمن أجندة أفريقيا للتنمية المستدامة: 2063، واتفاقية(مالاو) بين 2011–2020 للأمن السيبرانى وحماية البيانات الشخصية، وفريق خبراء سيبرانى للإتحاد الأفريقى 2018،وإستراتيجية أفريقية للتحول الرقمى 2020.

- **مبادرات عربية سيبرانية غير كافية**، منها جهود لصياغة إطار عربى استرشادى للأمن السيبرانى، الإتفاقية العربية لمكافحة جرائم تقنية المعلومات،وتأسيس المركز العربي الإقليمي للأمن السيبرانى فى سلطنة عمان 2013 بالتعاون مع الإتحاد الدولي للإتصالات.
- **إسهامات موازية للجماعات العلمية فى العالم ومصر لدعم الأمن السيبرانى**، تم نشر 4830 بحثاً يتناول قضايا الأمن السيبرانى 2015-2020 مع تصدر للولايات المتحدة، وحوالى 16 مساهمة مصرية، كما صدر كتاب دولى حول القضايا بمحررين مصريين 2019.
- **دور مراكز الفكر ومنظمات الأعمال فى التوعية ودعم الأمن السيبرانى**، خاصة دور المنتدى الاقتصادى العالمي WEF بتاسيسه مركز متخصص للأمن السيبرانى ليقود أنشطة متنوعة، وأدوار لشركات عالمية متعددة من بينها: IBM. وعلى المستوى العربي هناك أدوار للإتحاد العربي للإنترنت والإتصالات:ARISPA، والإتحاد العربي لتقنية المعلومات والإتصالات.
- **ملامح هامة فى التجربة الأمريكية**، الربط بين الأمن الوطنى والسيبرانى استراتيجياً مع دور فيدرالى حاكم للدولة،الأمن السيبرانى يدعم منظومة الحياة والقيم الأمريكية، بناء قدرات البحوث والتطوير والكوادر البشرية المساندة،تنمية الاقتصاد الرقمى، والدبلوماسية السيبرانية.
- **خبرات سيبرانية كورية جنوبية**، تشريعات متعددة تشمل الإستغلال الجنسى وحماية الأطفال،مخطط رئيس وسياسات وطنية مصاحبة، أطر للحوكمة المؤسسية السيبرانية تبدأ من رئاسة الدولة، تنمية الاقتصاد الرقمى والبنية التحتية الرقمية والدبلوماسية السيبرانية.
- **ملامح هامة للتجربة الهندية**، الدور الحاكم لقطاع تكنولوجيا المعلومات والإتصالات فى التنمية،إطار تشريعى جامع مع أدوار مؤسسية بما فيها وزارة الإليكترونيات وتكنولوجيا المعلومات، سياسة وطنية عام 2013 جارى تطويرها لإستراتيجية وطنية منذ عام 2020.
- **تجربة اسرائيل ومزايا الاقتصاد السيبرانى**، ربط وثيق بين الأمن السيبرانى والوطنى للتعامل مع مهددات إقليمية حاضرة بقوة، أطر تشريعية ومؤسسية مع التركيز على الدفاع السيبرانى، ابحث والتطوير والكوادر، ميزات ومنافع قتصادية (10% من المبيعات العالمية لأمن المعلومات).
- **خبرات متعددة من تجارب عالمية أخرى**، مركز سيبرانى وطنى لدعم الحكومة وقطاعات الأعمال العامة والخاصة(المملكة المتحدة)، مكتب فيدرالى لأمن المعلومات(ألمانيا)، قانون وتشديدات لحماية البنية المعلوماتية الوطنية(الصين)، ومجلس للأمن القومى مسئول عن السياسات

السيبرانية(اليابان)، ووكالة وطنية مسئولة عن القواعد والإرشادات(ماليزيا)، وإستراتيجية وطنية مع ارشادات متوافقة مع ارشادات الإتحاد الدولي للإتصالات (بنغلاديش).

- **خبرات تجربة المملكة العربية السعودية**، ربط الأمن السيبرانى مع توجهات رؤية المملكة 2030، تشريعات ومؤسسات معنية، إستراتيجية وضوابط ومعايير ناظمة، استضافات ومبادرات إقليمية سيبرانية هامة، ومشاركات معلوماتية وسيبرانية فاعلة فى إطار مجموعة العشرينG20.
- **خبرات تجربة سلطنة عمان**، أطر تشريعية ومؤسسية وطنية خاصة المركز الوطنى للسلامة المعلوماتية والمختبر الوطنى للأدلة الرقمية، ومساهمات إقليمية هامة لإإستضافة السلطنة المركز العربي الإقليمي للأمن السيبرانى منذ عام 2013.
- **خبرات مستفادة للتجربة المصرية**

- الربط الوثيق بين الأمن السيبرانى والأمن الوطنى للدولة والأمن الإقليمي والعالمي
- الربط الوثيق بين الأمن السيبرانى وإستراتيجيات وخطط الدولة التنموية
- دور محورى للدولة فى تخطيط وتوجيه سياسات وقواعد الأمن السيبرانى
- دور هام للأمن السيبرانى فى دعم التنمية المستدامة وأهدافها الأممية والوطنية
- أهمية الدبلوماسية السيبرانية والتواصل من خلالها على المستويين الإقليمي والعالمي

3. 3. نتائج خاصة بالتجربة السيبرانية المصرية

- اهتمام رئاسى بالأمن السيبرانى، حيث أكد رئيس الدولة فى أكثر من مناسبة (أحدثها – مارس2021) على أهمية الأمن السيبرانى والحفاظ على الأول الرقمية والمعلوماتية للدولة.
- رؤية دستورية ثلاثية الأبعاد لأمن المعلومات الوطنى، حيث يربط الدستور بين أمن المعلومات وأبعاد: الاقتصاد الرقمى، والأمن القومى بالإضافة لدور الدولة الحاكم فى أمن المعلومات.
- أطر تشريعية متعددة وفجوات تشريعية قائمة، وأحدثها قانون لحماية البيانات الشخصية(151 لسنة 2020)، ومكافحة جرائم تقنية المعلومات(قانون 175 لسنة 2018)، وتبقى بعض المتطلبات التشلريعية الجديدة اللازمة، وتعديلات فى بعض التشريعات القائمة.
- أطر تخطيطية متعددة ذات صلة تنتظر الإرتباط الإستراتيجى والتنفيذى، حيث تتعدد الاهتمامات بدور المعلومات فى تنمية الاقتصادات الرقمية فى وثائق التنمية المختلفة

مع إهتمام أقل بالأمن السيبرانى / أمن المعلومات فى إطار رؤى إستراتيجية تترجم إلى برامج عملية يتم تنفيذها فى اطار مديات زمنية محددة ويتم متابعتها وتقييم أدائها من خلال مؤشرات محددة.

- استراتيجية وطنية للأمن السيبرانى 2017-2022، وتمثل تطور نوعى فى تعامل الدولة مع الأمن السيبرانى وصادرة عن (المجلس الأعلى للأمن السيبرانى) تركز على قضايا الأمن الحوسبى والسيبرانى، وتضم الإستراتيجية 7 أولويات تمت ترجمتها فى 6 برامج نوعية.
- تحسن فى عديد من مؤشرات الإتصالات والمعلومات،خاصة إنتشار الهواتف المحمولة 93.6%، وانتشار الإنترنت 57.3%، وتغطية مناطق محرومة من خدمات الاتصالات (11 منطقة).
- تباينات فى مؤشرات الأمن السيبرانى والإتصالات والمعلومات المحلية والعالمية
- تحسن فى التعامل مع الهجمات السيبرانى من جانب المركز الوطنى، مع تفاوتات فى مستوى خطورة الهجمات حيث تتصدر هجمات حجب الخدمات: DDoS بنسبة 43.8%، وهجمات البرامج الضارة 21%،وهجمات المواقع 19%.
- تحسن فى مؤشر القوة السيبرانية الوطنية NCPI عام 2020، وبعض جوانب مؤشر الأمن السيبرانى العالمي، كذلك مؤشر جاهزية الحكومة للذكاء الإصطناعى ومؤشر المعرفة العالمي.
- تراجعات فى مؤشرات أخرى منها: مؤشر الإبتكار العالمي GII، مع العديد من التحديات على مؤشر الجاهزية الشبكية:NRI .
- دور محورى لوزارة الإتصات وتكنولوجيا المعلومات وأجهزتها، فى مجالات الأمن السيبرانى، التحول الرقمى، الشمول الرقمى، الهوية الرقمية، تنمية صناعة تكنولوجيا المعلومات والإتصالات، الإبداع التكنولوجى والذكاء الإصطناعى، والتدريب وبناء القدرات.
- تطورات ايجابية لقطاع تكنولوجيا المعلومات والإتصالات، حيث حقق أعلى معدلات النمو مقارنة بالقطاعات الأخرى بالدولة رغم جائحة كورونا، وتمت زيادة استثمارات القطاع، وأطلق منصة مصر الرقمية -يوليو 2020، مع تطويرات واسعة فى البنية التحتية، وتنويع الشراكات الإقليمية والعالمية.

- دور محورى وتحديات للمركز الوطنى للإستعداد لطوارىء الحاسبات:EG-CERT، وتأسس عام 2009 ليلعب دور الذراع التنفيذى والفنى للمجلس الأعلى للأمن السيبرانى، ويتبنى مشروعات هامة (الدرع الإليكترونى، مكافحة البرمجيات الخبيثة وغيرها)، كما يواجه تحديات فى تفهم أدواره بصورة صحيحية انعكست فى نقص الطلب المجتمعى على خدماته.
- أدوار هامة للبنك المركزى فى الحوكمة السيبرانية فى القطاعات المالية، حيث أسس إدارة مركزية لأمن المعلومات عام 2009 لدعم الرقابة وإدارة مخاطر أمن المعلومات فى القطاع المصرفى وتمكين البنوك العاملة فى مصر من حماية أصولها الرقمية.
- توجهات لتعزيز الأمن السيبرانى فى مجال أعمال البورصة والتأمين، من خلال مبادرات للتوعية وضوابط وقواعد ذات صلة للبورصة المصرية، بالإضافة إلى مبادرات لأمن المعلومات وخدمات التأمين على مخاطر المعلومات من جانب الإتحاد المصري للتأمين وغيره.
- جهود ومبادرات عديدة مساندة لتعزيز الأمن السيبرانى، ومن بينها الجهود التشريعية بمجلس النواب المصري (لجنة الإتصالات وتكنولوجيا المعلومات)، ومبادرات لمركز المعلومات ودعم اتخاذ القرار، والتنظيمات المهنية المعنية، والأجهزة والمجالس العلمية المختلفة.
- فجوات فى إقتصاد وصناعة الأمن السيبرانى، سواء فى صناعة البرمجيات والأجهزة ذات العلاقة بتأمين المعلومات والإتصالات والدفاع السيبرانى، واكتشاف الثغرات وغيرها.

ثانياً: سياسات مقترحة لتعزيز الأمن السيبرانى ودعم الاقتصاد الرقمى والمشفر والتنمية المستدامة فى مصر فى ضوء خبرات عالمية وإقليمية مستفادة

1. تبنى إطار مفاهيمى مجتمعى تنموى مستدام جديد لحوكمة الأمن السيبرانى،

يتم من خلاله طرح الأمن السيبرانى كقضية مجتمعية تنموية وليست فنية أو أمنية أو تقنية.

– **التوصية العملية المقترحة:** قيام المجلس الأعلى للأمن السيبرانى بطرح **(ورقة عمل مجتمعية)** للحوار المجتمعى العام حول حوكمة الأمن السيبرانى فى أبعاده التنموية: الإجتماعية، الاقتصادية، السياسية، الأمنية والدفاعية، التقنية، البيئية، والسلوكية، ودوره فى تعزيز التنمية المستدامة وحصانة الدولة.

2. <u>تبنى منطلقات إستراتيجية جديدة لحوكمة الأمن السيبرانى فى ضوء الإطار المفاهيمى الجديد ضمن توجهات التنمية المستدامة للدولة،</u>

وذلك بالتعاون بين المجلس الأعلى للأمن السيبرانى ووزارة التخطيط والتنمية الاقتصادية، والأطراف المعنية فى الدولة، تربط الأمن السيبرانى بالتحول الرقمى فى الاقتصاد والمجتمع، وقضايا الأمن القومى والوطنى والشخصى.

- **التوصية العملية المقترحة:** تشكيل فريق مشترك بين (وزارة الإتصالات وتكنولوجيا المعلومات – المجلس الأعلى للأمن السيبرانى) ووزارة التخطيط والتنمية الاقتصادية لتحديد الأهداف الإستراتيجية للأمن السيبرانى والبرامج والمشروعات المرتبطة بها فى الإستراتيجية الجديدة للأمن السيبرانى(2022-2030)، ومن ثم تضمين هذه البرامج والمشروعات فى إستراتيجية التنمية المستدامة 2030، وخطة التنمية متوسطة المدى الجديد2025 / 2030، وبرنامج عمل الحكومة 2025-2030.(مع إعتبار خصوصيات سرية البرامج الدفاعية والأمنية)

3. <u>التسويق والتوعية المجتمعية للمفهوم التنموى المجتمعى لحوكمة الأمن السيبرانى،</u>

وذلك بالتنسيق والتعاون بين المجلس الأعلى للأمن السيبرانى، والمجلس الأعلى لتنظيم الإعلام والهيئة الوطنية للإعلام، والجهات الحكومية والأهلية المعنية. والتركيز على قضايا: الدور التنموى، وصيانة حقوق الإنسان والأطفال والمرأة، والإدارة الفعالة للمخاطر السيبرانية.

4. <u>استكمال فجوات الحوكمة التشريعية الداعمة لحوكمة الأمن السيبرانى فى مصر،</u>

وذلك إنطلاقاً من المفهوم المجتمعى التنموى الجديد للأمن السيبرانى، من خلال:

- إصدار تشريعات جديدة مساندة،
- **تشريع خاص للأمن السيبرانى،** فى ضوء الإطار المفاهيمى التنموى الجديد.
- **قانون التجارة الإليكترونية،** وربطه مع التشريع الخاص بالأمن السيبرانى
- **قانون حرية تداول المعلومات،** وهو موضع نقاش منذ سنوات طويلة.
- **قانون إدارة البيانات على المستوى القومى،** لتنظيم عمليات حماية وتأمين البيانات على المستوى القومى، وتنظيم إنشاء وإدارة مراكز البيانات فى الدولة، وتنظيم عملية بناء وإدارة المواقع الإليكترونية للجهات الحكومية والقطاع الخاص والمجتمع المدنى، وضوابط حمايتها وتشغيلها فى إطار ضوابط قانون الأمن السيبرانى. بالإضافة إلى التعامل مع البيانات المفتوحة، البيانات الضخمة، البيانات الساتلية والتصوير الجوى،نظم الجغرافيا المكانية ونظم المعلومات الجغرافية واستخدامات الحوسبة السحابية.

- **تشريع وقواعد الهوية الرقمية**، وتنظيم إجراءات جمع والتحفظ ونقل (الأدلة الرقمية) والتعامل معها، وتنظيم وتقنين التعاون / التعامل الرقمى مع العالم الخارجى،
- **تشريع وضوابط حاكمة جديدة**، لإعادة تنظيم إجراءات استيراد وتصنيع المعدات التكنولوجية الرقمية، وحماية أصول وأجهزة وأنظمة التحكم الصناعى(ICS/OT) ضد الهجمات والمخاطر السيبرانية وفق المعايير الوطنية والدولية ذات الصلة.
- **تطوير تشريعات قائمة ذات صلة:**
  - **قانون حماية الملكية الفكرية**، فى ضوء التحولات الرقمية والحاجة لقواعد حماية المحتوى الرقمى والحقوق فى البيئات الرقمية، ومواجهة ثغرات ضعف الإنفاذ.
  - **قانون الإحصاء والتعداد رقم 35 لسنة 1960 المعدل بالقانون رقم 28 لسنة 1982**، وربط التطوير فى العمل الإحصائى والأنشطة الإحصائية بالتطوير فى تشريعات ونظم إدارة البيانات على المستوى الكلى وتوزيع الأدوار فى هذا الخصوص.

5. **<u>دعم الإستراتيجيات والخطط والسياسات والتشريعات بأدلة عملية داعمة، تتضمن إجراءات عملية لأمن المعلومات لدعم الجهات المختلفة، ومنها:</u>**

- معايير وأسعار تأمين خطوط الإتصالات وتسعير اتصالات الإنترنت.
- معايير مصرية لتصنيف وحوكمة البيانات الرقمية داخل كل مؤسسة، بما فيها تصنيف وضبط المخاطر المرتبطة بتسريب البيانات، وضوابط إدارية وأخلاقية على انتقالات العاملين فى إدرات أمن المعلومات.
- معايير وطنية لإختبار كفاءة الأجهزة والتطبيقات المعلوماتية والرقمية
- قواعد متمايزة لشراء تكنولوجيا وخدمات المعلومات فى الجهات بخلاف قواعد قانون المشتريات الحكومية التقليدية.

6. **<u>ترتيبات مؤسسية هامة:</u>**

- وحدات أمن المعلومات فى الجهات الحكومية،

- يمكن تأسيسها من خلال تعديل قرار رئيس مجلس الوزراء رقم 1146 لسنة 2018 والخاص بالتقسيم التنظيمى: نظم المعلومات والتحول الرقمى، وتحويل هذا التقسيم التنظيمى إلى: (نظم وأمن المعلومات والتحول الرقمى).
- يمكن ترتيب (علاقة مؤسسية) تضمن إشراف المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات:EG_CERT على أمن المعلومات فى هذه الوحدات.

7. **سياسات جديدة لدعم (صناعات الأمن السيبرانى) فى الاقتصاد الوطنى،**

- طرح فرص استثمار سيبرانية محددة للقطاعين العام والخاص فى إطار قطاع الإتصالات وتكنولوجيا المعلومات، بناء على دراسات للميزات والفرص الإستثمارية الاقتصادية المتاحة بما فيها التصديرية بمشاركة هيئة تنمية صناعة تكنولوجيا المعلومات.
- طرح حوافز لريادة الأعمال والمشروعات المتوسطة والصغيرة للدخول إلى مجال الصناعات السيبرانية المختلفة بالتعاون مع جهاز تنمية المشروعات المتوسطة والصغيرة، خاصة وأن (المشروعات الرقمية) مشمولة بحوافز تمييزية ضمن قانون هذه المشروعات رقم 152 لسنة 2020.
- مشاركات خارجية وفق ضوابط مع الشركات العالمية الكبرى من خلال قنوات هيئة تنمية صناعة تكنولوجيا المعلومات بالتعاون مع القطاع المصرفى.

8. **سياسات مقترحة لدعم الأمن السيبرانى فى القطاع المالي**

- التوسع فى نشاط خدمات التأمين ضد الهجمات السيبرانية: Cyber Insurance
- دراسة إلزام الشركات فى قطاعات الأعمال العامة والخاصة التى يرتبط عملها بشكل مباشر بالمؤسسات المالية والمصرفية بتبنى لوائح وضوابط الزامية لأمن المعلومات.

9. **سياسات البحوث والتطوير وبناء القدرات الداعمة للأمن السيبرانى**

- **طرح مبادرات عملية لتعزيز الإبتكار فى مجال الأمن السيبرانى،** وتركز على الشباب ويتولى طرحها أجهزة الدولة المعنية بالتنسيق مع المجلس الأعلى للأمن السيبرانى وربطها بأنشطة البحوث والتطوير R&D فى الجامعات ومراكز ومعاهد البحوث.
- إدراج بعض مشروعات وبرامج الأمن السيبرانى ضمن برامج الإستراتيجية القومية للعلوم والتكنولوجيا والإبتكار، ليتم تنفيذها فى إطار برامج الحاضنات التكنولوجية والتحالفات التكنولوجية فى الإستراتيجية.
- **إعداد دراسات مستقبلية حول الأمن السيبرانى وانعكاساته،** تتضمن إستشراف للفرص والمخاطر المرتبطة بالتوسع فى الشبكات والتطبيقات والتقنيات البازغة فى مجالات الحياة.
- **التوسع فى برامج تنمية القدرات السيبرانية،** وعلى مستويات متعددة تضمن البرامج الإحترافية للمتخصصين، وبرامج التوعية والإلمام لغير المتخصصين بمشاركة المعاهد المتخصصة لدى وزارة الإتصالات، ومعاهد وزارة التعليم العالى والبحث العلمى، وكليات الحاسبات والذكاء الإصطناعى.

10. <u>تنشيط الدبلوماسية السيبرانية / الرقمية وتعزيز العلاقة بين وزارة الخارجية والمجلس الأعلى للأمن السيبرانى،</u>

- يمكن لوزارة الخارجية تقديم مقترحات وبرامج محددة فى هذا الخصوص من خلال عضويتها الفعلية فى المجلس الأعلى للأمن السيبرانى.
- يمكن لـ: (غرفة صناعة تكنولوجيا المعلمات) بإتحاد الصناعات المصرية المساهمة بمبادرات محددة فى هذا الخصوص، سواء منفردة أو بالمشاركة مع وزارة الخارجية.
- تشجيع المبادرات المجتمعية الأهلية فى هذا الخصوص واستثمارها على المستوى الإقليمي على وجه الخصوص وربطها بميادرات أهلية عالمية ذات صلة مثل: مبادرة "سيدات فى الأمن السيبرانى" Women in Cyber Security Middle East، وغيرها.

<u>ثالثاً: قضايا متعددة جديرة بالدراسة:</u>

- أثر تقنيات الجيل الخامس والحوسبة السحابية على الأمن السيبرانى فى مصر
- أثر تقنيات الجيل الخامس والحوسبة السحابية على الاقتصاد الرقمى
- الاقتصاد السيبرانى وآفاقه فى مصر – الفرص والمحددات
- ريادة الأعمال السيبرانية والعلاقة مع الإبتكار ونماذج الأعمال الجديدة
- إستشراف تكلفة وخسائر الأمن السيبرانى على الاقتصاد الوطنى
- تمويل إدارة مخاطر الأمن السيبرانى على المستوى الوطنى ومستوى شركات الأعمال
- إدارة مخاطر الأمن السيبرانى فى الشركات الكبرى – دراسات حالة
- العلاقة بين الأمن السيبرانى وحقوق الإنسان والحريات العامة والأمن الإجتماعى
- الإرهاب السيبرانى وتداعياته على الأمن القومى
- الأمن السيبرانى وتأثيراته على أنشطة التواصل الإجتماعى
- آفاق تفعيل الدبلوماسية الرقمية إقليمياً وعالمياً
- علاقة الأمن السيبرانى والتقنيات البازغة بالتنمية المستدامة
- متطلبات حوكمة الأمن السيبرانى فى القطاع المصرفى والمالي

قائمة المراجع

أولاً: مراجع باللغة العربية

1- الاتحاد الدولي للإتصالات وآخرون (2018). دليل لوضع إستراتيجية وطنية للأمن السيبرانى- التزام استراتيجى بالأمن السيبرانى. جنيف:الإتحاد الدولي للإتصالات.

2- الجهاز القومى لتنظيم الإتصالات (2021). تقرير نتائج قياسات شبكات المحمول – تقرير ربع سنوى عن الفترة من يناير 2021- مارس 2021.القاهرة: الجهاز.

3- الهيئة الوطنية للأمن السيبرانى (2020). الإستراتيجية الوطنية للأمن السيبرانى: نظرة عامة. الرياض. الهيئة الوطنية للأمن السيبرانى.

4- الهيئة الوطنية للأمن السيبرانى (2020). ضوابط الأمن السيبرانى للعمل عن بعد. الرياض. الهيئة الوطنية للأمن السيبرانى.

5- أميل أمين (2020). الأمن السيبراني العالمي – حروب خلفية ومساحات إرهابية: قوى تهدد استقرار المجتمعات عبر شبكة الإنترنت وبتقنيات عالية جداً- https://www.independentarabia.com/

6- جامعة الدول العربية(2019). مذكرة الأسباب الموجبة لأمن وسلامة الفضاء السيبرانى – الإنترنت ومسودة مشروع القانون الإسترشادى العربي لحماية الأمن السيبرانى(غير منشورة).بيروت: المركز العربي للبحوث القانونية والقضائية.

7- جمعية الإنترنت(2020). المبادىء التوجيهية المتعلقة بأمن البنية التحتية للإنترنت فى المنطقة العربية. الولايات المتحدة الأمريكية: جمعية الإنترنت.

8- شبكة هيكل ميديا المعرفية – هارفرد بزنس ريفيو (2021). المفاهيم الإدارية – الأمن السيبرانى.

9- صندوق النقد العربي(2020). تقرير الإستقرار المالي فى الدول العربية 2020. أبو ظبى: صندوق النقد العربي.

10- قيصر بهاء (2020). أشهر الهجمات السيبرانية – آلية عملها وطرق تجنبها. بغداد: الفريق الوطنى للإستجابة للأحداث السيبرانية.

11- محمد إسماعيل (2019). الأمن السيبرانى فى القطاع المصرفى. أبو ظبى: صندوق النقد العربي. موجز سياسات –العدد الرابع.

12- محمد حجازى(2021). الأمن السيبرانى بين التشريعات الوطنية والمتطلبات الدولية: القاهرة: ورشة عمل بمركز المعلومات ودعم اتخاذ القرار- أبريل.

13- محمد ماجد خشبة وآخرون – بحث جماعى (2020). استشراف الآثار المتوقعة لبعض التطورات التكنولوجية على التنمية في مصر وبدائل سياسات التعامل معها – بالتطبيق على الذكاء الاصطناعي: AI – وسلسلة الكتل: Blockchain. القاهرة: معهد التخطيط القومى. سلسلة قضايا التخطيط والتنمية رقم 315.

14- صندوق الأمم المتحدة للسكان والجهاز المركزى للتعبئة العامة والإحصاء (2018). تقرير النظام الإيكولوجى للبيانات فى مصر لدعم التنمية المستدامة.القاهرة: صندوق الأمم المتحدة للسكان والجهاز المركزى للتعبئة العامة والإحصاء.

15- مجموعة البنك الدولي(2021). البيانات من أجل عالم أفضل – تقرير عن التنمية فى العالم 2021. واشنطن. البنك الدولي.

16- مركز المعلومات ودعم اتخاذ القرار (2020). أهم اختراقات الأمن السيبرانى لعام 2020.القاهرة: مجلس الوزراء، مركز المعلومات ودعم اتخاذ القرار.

17- وزارة التقنية والإتصالات(2019). التقرير السنوى 2019م. مسقط. وزارة التقنية والإتصالات.

18- وزارة التعليم العالى والبحث العلمى(2019). الاسترتيجية القومية للعلوم والتنولوجيا والإبتكار 2030.القاهرة: وزارة التعليم العالى والبحث العلمى.

ثانيًا: مراجع باللغة الإنجليزية

1- Adelman, Frank et.al. (2020). Cyber Risk and Financial Stability: It's a Small World After All. IMF Staff Discussion note. Washington: IMF.

2- Aldasoro, Iñaki et al. (2020). Operational and cyber risks in the financial sector. Switzerland: BIS - Monetary and Economic Department Working Paper No. 840. https://www.bis.org/publ/work840.pdf

3- Biden, Joseph R. (2021). Executive order on improving the Nation's Cybersecurity.Washington. The White House.

4- Basel Committeeon Banking Supervision (2018). Cyber-resilience: Range of practices. Switzerland: BIS.

5- Bernard, Julie and Nichloson, Mark. (2020). Reshaping the cybersecurity landscape: How digitization and the COVID-19

pandemic are accelerating cybersecurity needs at many large financial institutions. New York: Deloitte. (https://www2.deloitte.com).

6- Ebert, Hannes and Groenendaal, Laura (2020). Cyber resilience and diplomacy in the Republic of Korea: Prospects for EU cooperation. Brussels: EU Cyber Direct.

7- Canadian Security Intelligence Service-CSIS (2021). CSIS public report 2020.Canada: CSIS.

8- Craig, Anthony and Valeriano, Brandon, (2018). Realism and Cyber Conflict: Security in the Digital Age, Feb 3, 2018, https://www.e-ir.info/2018/.

9- European Union Agency for Cybersecurity-ENISA (2021). Security in G5 specifications. Greece. ENISA.

10- _____-ENISA (2020). Trusted and cyber secure Europe – ENISA strategy. Greece: ENISA.

11- FSB. (2020). Effective Practices for Cyber Incident Response and Recovery. Consultative Document. Financial Stability Board: https://www.fsb.org/wp-content/uploads/P200420-1.pdf

12- FTI Consulting and AMCHAM India. (2020). A white paper on India, s National Cybersecurity Strategy 2020.India.FTI.

13- Gurinaviciute, Juta (2021). 5 biggest cybersecurity threats – How hackers utilize remote work and human errors to steal corporate data.www.securitymagazine.com

14- Hossain, Aboul Ella and Elhoseny, Mohamed -Editors (2019). Cybersecurity and Secure Information Systems-Challenges and solutions in a smart environment. Switzerland: Springer- Advanced Sciences and Technologies for Security Applications.

15- IBM. (2021). IBM.x-Force Threat Intelligence Index 2021.USA: IBM.

16- IMF. (2020). Cyber Risk and Financial Stability: It's a Small World after AII.USA: IMF- (IMF Staff Discussion Note).

17- ITU (2021). Global Cybersecurity Index 2020.Geneva: TU. Development Sector.ITU Publications. (2018).

18- Global Cybersecurity Index 2018. Geneva: ITU.Studies &Research.

19- Kaspersky (2021). What is cybersecurity.pp.1-5. www.kaspersky.com/

20- Katz, Raul and Callorda, Fernando (2018). The economic contribution of broadband, digitization and ICT regulation. Geneva: ITU Expert Reports.

21- NATO (2021). Cyber Defence. (https://www.nato.int/cps/en/).

22- PORTULANCE INSTITUTE (2020). Network Readiness Index 2020-Egypt.Washington. Portulance institute.
23- Ravia, Haim et.al. (2021). Cybersecurity 2021- Israel- Law and practice. /https://practiceguides.chambers.com Israel.
24- Signé, Landry and Signé, Kevin (2021). How African states can improve their cybersecurity. Washington: BROOKINGS Institution.
25- Software Testing Help. (2020). Top 11 Most Powerful Cybersecurity Software Tools in 2021. www.softwaretestinghelp.com/cybersecurity-software-tools.
26- UNCTAD (2021). Harnessing the promise of blockchain to change lives. https://unctad.org/.
27- Uddin, Hamid et.al. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. (Risk Management 22:239–309).
28- Valtorta, Katia, et.al. (2020). ICT security in the digital transformation Era-Do organizations need digital security strategies. ArthurD.Little. https://www.adlittle.com/
29- Voo, Julia.et.al. (2020). National Cyber power index 2020-Methodology and analytical considerations. USA: HARVARD Kenedy School.
30- WEF (2021). Principles for board governance of cyber risk. Geneva. WEF. Insight Report.
31- _____ (2021). These are the top cybersecurity challenges of 2021. https://www.weforum.org/
32- WB. (2020). Financial Sector's Cybersecurity: A Regulatory Digest. Washington. World Bank Group.
33- Zimber, Elieen (2021) SMB spend on securing mobile devices will increase at a CAGR of 18% to almost USD9 billion in 2025. https://www.analysysmason.com/.

ثالثًا: مواقع إلكترونية ذات صلة

الجهة	الموقع الإلكتروني
الإتحاد الدولي للاتصالات ITU	https://www.ngi.eu/
البنك المركزي المصري	https://www.cbe.org.eg/ar/
التحالف الأوروبي للذكاء الاصطناعي	https://ecas.ec.europa.eu/
الجهاز القومى لتنظيم الإتصالات	https://www.tra.gov.eg/ar
المجلس الأعلى للأمن السيبرانى	https://www.escc.gov.eg/
المعهد القومى للإتصالات NTI– مصر	https://www.nti.sci.eg
المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات	https://www.egcert.eg/ar/
الهيئة الوطنية للأمن السيبرانى – السعودية	https://nca.gov.sa
المركز الأوروبى للجرائم السيبرانية EC3	https://www.europol.europa.eu /
المركز العربي للبحوث القانونية والقضائية	https://carjj.org/contact
المنتدى الاقتصادي العالمي WEF	https://www.weforum.org
جمعية الإنترنت	http://arabic.china.org.cn/
جهاز تنظيم الإتصالات – مصر	https://www.tra.gov.eg/ar
شركة كسبارسكى	www.kaspersky.com/
صندوق النقد العربي	https://www.amf.org.ae/sites
قسم الأمن السيبرانى / وزارة الإليكترونيات وتكنولوجيا المعلومات: الهند	https://www.meity.gov.in/cyber-security-division
مركز المستقبل للأبحاث والدراسات المتقدمة	https://futureuae.com/ar
وكالة الإتحاد الأوروبى للأمن السيبرانى ENISA	https://www.enisa.europa.eu
وزارة الإتصالات وتكنولوجيا المعلومات	http://www.mcit.gov.eg/Ar/Publications
هيئة الإتصالات وتقنية المعلومات – السعودية	https://www.citc.gov.sa/ar/

ملحق الدراسة

مسودة نتائج ورشة العمل الخاصة ببحث:

"الأبعاد التنموية والإستراتيجية للأمن السيبرانى ودوره في دعم الاقتصادات الرقمية والمشفرة– مسارات التجربة المصرية في ضوء التجارب العالمية "

معهد التخطيط القومي

(الاثنين،3 فبراير 2021)

يقوم معهد التخطيط القومى بإعداد دراسة حول:

" الأبعاد التنموية والاستراتيجية للأمن السيبرانى ودوره في دعم الاقتصادات الرقمية والمشفرة – مسارات التجربة المصرية في ضوء التجارب العالمية ".

وفى إطار سعى الفريق البحثي للتواصل مع الأطراف المعنية بقضايا الدراسة في مصر، فقد تم عقد ورشة عمل خبراء مع مجموعة من الخبراء المتخصصين فى مجال الأمن السيبرانى، والقيادات فى بعض الجهات الحكومية المعنية، ورواد الأعمال، وخبراء من الأكاديميين.

وقد دار نقاش مثمر وفعال بين الخبراء والمشاركين من الجانبين حول الجوانب المختلفة لتأثيرات الأمن السيبرانى وأمن المعلومات بوجه عام وعلاقته بتوجهات تنمية الاقتصاد الرقمي فى مصر، وما يرتبط بذلك من متطلبات وفرص وتحديات.

وقد استهلت أ.د./أمانى الريس– نائب رئيس المعهد للتدريب والإستشارات وشئون المجتمع، وعضو الفريق البحثى فعاليات الورشة بالترحيب بالضيوف داخل المعهد وعبر تقنية ZOOM. كما عرض الباحث الرئيس أهداف الدراسة ومكوناتها، كما طرح العديد من التساؤلات التى بلورها الفريق البحثى على الخبراء المشاركين فى الورشة.

ويمكن إبراز أهم القضايا التي تناولتها الورشة بالنقاش على النحو التالي:

1. خلفيات أساسية – وقضايا التخطيط والسياسات والتشريعات والأدوار

– **الأمن السيبرانى قضية عالمية وإقليمية** ، وتحظى بإهتمامات متفاوتة فى كافة دول العالم، ويصل الأمر فى بعض الدول إلى بناء جيوش سيبرانية منظمة لصد/ أو شن هجمات سيبرانية مضادة (دول الناتو كمثال). كما تتواجد أطر عالمية متقادمة مثل اتفاقية بودابست لمكافحة الجريمة الإلكترونية عام 2001، والإتفاقية العربية لمكافحة جرائم تقنية المعلومات والتى انضمت لها مصر عام 2014.

- **توقعات بزيادة وليس انحسار الهجمات السيبرانية**، خاصة مع زيادة توجهات ومشروعات التحول الرقمى فى كافة دول العالم ومن بينها مصر، ومع وقوف دول خلف جانب كبير من الهجمات السيبرانية لأسباب متعددة (الصين + روسيا+ ايران+ اسرائيل).

- **مخاطر الأمن السيبرانى / الرقمي الوطني جاثمة وأخطر وأقرب مما يتصور الكثيرون**، وعلى ذلك فإن هناك حاجة إلى **(إرادة سياسية)** حقيقية للتعامل مع قضايا الأمن السيبرانى والرقمي فى المجتمع من خلال (خارطة طريق وطنية) متكاملة.

- **الأمن السيبرانى مسئولية جماعية وطنية**، حيث لا ينحصر الاهتمام بالأمن السيبرانى فى (وزارة الإتصالات وتكنولوجيا المعلومات)، ولكنها مسئولية تضامنية بين الوزارة وكافة جهات وأجهزة الدولة وقطاعات الأعمال والمجتمع المدنى ذى الصلة، والمواطن العادى.

- دور إستراتيجية الأمن السيبرانى والمجلس الأعلى للأمن السيبرانى،
  - تشكيل المجلس واطلاق الإستراتيجية كان يحتاج إلى تطوير تشريعى مسبق.
  - تفعيل الإستراتيجية كان يحتاج إلى توفير موارد مالية كبيرة، وقد بدأ توفير بعض الموارد المالية اللازمة فى الآونة الأخيرة.
  - الإستراتيجية لم تترجم إلى سياسات عملية ومشروعات محددة خاضعة للتقييم والمراجعة حتى الآن، ولم تطرح مشروعات فى هذا الخصوص فى برنامج عمل الحكومة.

- **تشريعات هامة لازمة لدعم الأمن السيبرانى**، منها ذات صلة بتحديد إلتزامات مقدمى خدمات المعلومات (بخلاف خدمات الإتصالات)، أطر تنظيمية للهوية الرقمية، إدارة البيانات والنفاذ إلى البيانات، قواعد التشفير، وغيرها.

- **محاور وموضوعات هامة تحتاج إلى معالجات**، وعلى رأسها: أمن نظم التشغيل فى قطاعات الإنتاج والخدمات.

- **دور محورى وهام للمركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات: EG-CERT**، رغم عدم تفهم طبيعة أدواره الخدمية، وليس الرقابية أو التدقيقية، من جانب العديد من الجهات والقيادات بما يقلص الطلب على خدماته الهامة دون مبرر موضوعى. والمركز ممثل فى الهيئة الوطنية للإعلام وله دور هام فى حماية الأطفال على الشبكة.

- **أهمية تكامل أدوار الأجهزة المعنية**، بما فيها أدوار سابقة لـ: (المجلس الأعلى للتحول الرقمى) وأدوار راهنة للمجلس الأعلى للأمن السيبرانى، المجلس القومى للمدفوعات، وغيرها.

2.خبرات هامة فى القطاع المالي وريادات الأعمال فى مجال الأمن السيبرانى:

– مبادرات وخطوات هامة للبنك المركزى لدعم الأمن السيبرانى فى القطاع المصرفى،

- قواعد للأمن السيبرانى من جانب البنك المركزى المصري
- لدى كل بنك فى القطاع المصرفى مسئول أمن سيبرانى
- إهتمام البنوك بعمليات المراجعة بما فيها المراجعة على نظم المعلومات IT Audit، والاهتمام بتطبيق المواصفات الدولية ذات الصلة مثل المواصفة الدولية لإدارة أمن المعلومات: ISO 27001.
- إهتمام البنك المركزى بتدريب كوادر الأمن السيبرانى.
- هناك حاجة إلى مزيد من الوقت والتجربة لنضوج الوعى والممارسة والخبرات بخصوص الأمن السيبرانى فى القطاع المصرفى.
- تصنيف مخاطر الأمن السيبرانى إلى ثلاثة أنواع: خارجية لصد الهجمات، داخلية، ومخاطر سلسلة الإمداد: Outsourcing وتتعلق بقوة المعايير لدى المورد الخارجى.
- تقوم البنوك المصرية بالتعاون مع البنك المركزى بجهود متعددة لتوعية (العميل الداخلى) و(العميل الخارجى) بخصوص قضايا الأمن السيبرانى.
- تقوم البنوك المصرية بالإفصاح عن بيانات الأمن السيبرانى للبنك المركزى والذى يعتبر المسئول عن الإفصاح أو عدم الإفصاح عن هذه البيانات إلى الجهات الأخرى لاحقاً.
- دور هام للمعهد المصرفى فى توفير تدريب متخصص فى مجال الأمن السيبرانى.
- بالإضافة لإستراتيجية البنك المركزى للأمن السيبرانى، يطبق كل بنك إستراتيجية الأمن السيبرانى الخاصة به.

– **خصوصيات التعامل مع الأمن السيبرانى فى البورصة المصرية،** هناك قواعد من هيئة الرقابة المالية للأمن السيبرانى تخص شركات السمسرة والوساطة المالية. كذلك، هناك توعية مستمرة للعاملين بخصوص الأمن السيبرانى والمصادر الأكثر تهديداً واحتمالاً للهجمات السيبرانية. ويخضع الإفصاح عن الهجمات السيبرانية على البورصة وغيرها من المؤسسات المالية والمصرفية بوجه عام إلى إعتبارات كثيرة من الجهات المعنية توخياً لتجنب حدوث هزات فى السوق باعتبارها مؤسسات اعتبارية عامة.

– نماذج فعالة لريادات الأعمال فى مجال الأمن السيبرانى، ويجسدها أكثر من نموذج أعمال مصرى فاعل مثل:

- **النموذج الأول: شركة Digital Planets:** ويمتد نشاطها بين مصر، الإمارات، ولندن فى مجال الخدمات الأمنية المدارة بالشراكة مع شركات عالمية لتقديم الحلول ذات الصلة. بالإضافة إلى شراكات محلية مع (ايتيدا) والمصرية للإتصالات (جوائز)، والإستثمار فى التدريب السيبرانى.
- **النموذج الثانى: شركة خدمات ومنتجات الأمن السيبرانى ISEC:** ولها إهتمامات خاصة بالتدريب ونشر الوعى السيبرانى فى مصر وخارجها بالتعاون مع شركات عالمية، والتعاون مع مؤسسات تعليمية أكاديمية. بالإضافة إلى أنشطة هامة على المستوى العربي (المؤتمر العربي لأمن المعلومات)، والذى يتضمن العديد من الفعاليات الهامة ذات الصلة.

3. تحديات هامة أمام الأمن السيبرانى فى مصر

- **نقص الوعى المجتمعى بالأمن السيبرانى على مستويات متعددة،** ومن بينها مستوى القيادات التنفيذية فى الجهات الحكومية، وهو الأمر الذى يؤدى لضعف التفاعل مع مبادرات متعددة من جانب المركز الوطنى: EG-CERT.

- **تحدى تحويل المخططات الإستراتيجية إلى سياسات ومشروعات عملية،** والعمل على ادراج هذه المشروعات فى خطط التنمية وبرامج العمل الحكومية.

- **نقص الطلب المحلى على خدمات الأمن السيبرانى،** وهو نقص يرتبط بنقص الطلب على الخدمات الرقمية والتحول الرقمى فى قطاعات المجتمع المختلفة الإنتاجية والخدمية سواء فى قطاعات الأعمال أو قطاعات الخدمات العامة.

- **فجوات الأطر التشريعية المساندة،** والتى سبق الإشارة إلى بعضها، ومشكلة تفعيل بعض التشريعات الصادرة ذات الصلة مثل تشريع التوقيع الرقمى الغير مستخدم.

- **تحديات بناء وتنمية القدرات البشرية المتخصصة،** وهو الأمر الذى يحتاج إلى استثمارات كبيرة، ورغم تعدد الجهود الجارية فى جهات متعددة إلا أنها تظل دون المستوى المأمول.

- **نزيف الخبرات الوطنية المتخصصة – هجرة العقول،** وعلى الأخص فى ضوء نقص الطلب الإجتماعى على خدمات الأمن السيبرانى، وتواضع الأجور والمزايا المطروحة فى السوق المصري مما يدفع الخبرات الوطنية للعمل خارج الحدود.

- الفجوة بين سرعة التحول الرقمى وبطء جهود وإجراءات وخطط الأمن السيبرانى الموازية، وهو الأمر الذى يتطلب تفعيل هذه الجهود وبصورة غير تقليدية فى المرحلة القادمة.

– **تحديات الأمن السيبرانى / والرقمى فى قطاعات نوعية هامة،** ومن بينها المنظومة الصحية خاصة فى ضوء التوسع فى **(تطبيقات الصحة الرقمية)** وما يرتبط بها من قضايا هامة مثل : الخصوصية، النفاذ، الحماية، وتأمين البيانات.

4. متطلبات تفعيل الجاهزية السيبرانية فى مصر

– **إطار عام للتوعية والثقافة الرقمية فى المجتمع،** بمشاركة الجامعات وإتحاد الصناعات والأجهزة الإعلامية بما يعزز الطلب المجتمعى على الخدمات الرقمية وعلى خدمات الأمن السيبرانى على التوازى. ويركز هذا الإطار على:

- إبراز وإلقاء الضوء على جرائم ومخاطر الأمن السيبرانى على المجتمع.
- تبنى مبادرات طوعية فعالة لمواجهة مخاطر الأمن السيبرانى فى المجتمع.

– **سياسات تحفيزية واضحة لتشجيع قطاعات وريادات الأعمال فى مجالات الأمن السيبرانى والرقمى،** بما فيها التسهيلات التمويلية بالتنسيق مع الإتحاد ات المهنية المسئولة مثل إتحاد الصناعات المصرية، ويمكن طرح هذه السياسات من خلال شركات مسئولة.

– **مبادرات عملية لتعزيز الإبتكار وريادة الأعمال فى مجال الأمن السيبرانى،** وتركز على الشباب ويتولى طرحها أجهزة الدولة المعنية وربطها بأنشطة البحوث والتطوير R&D فى الجامعات ومراكز ومعاهد البحوث.

– **تأسيس إدارة لأمن المعلومات فى كل جهة أو شركة،** وتعتبر أداة للوعى المؤسسى من جهة وأداة للإستباق والتعامل الفعال مع المخاطر السيبرانية من جهة أخرى، بالإضافة إلى التواصل وتبادل الخبرات عبر الوطن.

– دراسة إلزام الشركات التى يرتبط عملها بشكل مباشر بالمؤسسات المالية والمصرفية بتبنى لوائح الزامية لأمن المعلومات، وهو الأمر الذى يعزز ثقافة وممارسات الأمن السيبرانى فى قطاعات الأعمال المختلفة.

– **مراجعة وتطوير أدوار الجهاز القومى لتنظيم الإتصالات،** ودراسة النظر فى امكانيات تحويله إلى جهاز وطنى غير تابع لوزارة الإتصالات وتكنولوجيا المعلومات، وتوسيع مجالات عمله لتشمل تنظيم المجتمع الرقمى ومتطلبات الأمن الرقمى.

– **متطلبات داعمة فى القطاع التعليمى،** والسعى لتضمين قضايا الأمن السيبرانى فى المقررات الجامعية وقبل الجامعية فى مراحل التعليم المختلفة.بالإضافة إلى تشجيع شركات ريادة الأعمال الصغيرة فى العمل على مشروعات التوعية والتأمين والتدريب للمدرسين والطلاب.

- **تنمية وعى شركات القطاع الخاص المصري بخصوص الأمن السيبرانى،** وعلى الأخص أهمية الإستعانة بخدمات التقييم الأمنى: Security Assessment فى هذه الشركات، والإستعانة بقدرات الجهات الحكومية المعنية فى هذا الخصوص لتخفيض تكلفة التقييم.
- متطلبات هامة أخرى
  - إعداد أدلة إجراءات عملية لأمن المعلومات لدعم الجهات المختلفة.
  - دور فاعل لوزارة الإتصالات وتكنولوجيا المعلومات فى تحديد أسعار تأمين خطوط الإتصالات وتسعير اتصالات الإنترنت.
  - بلورة معايير مصرية لتصنيف وحوكمة البيانات الرقمية داخل كل مؤسسة، بما فيها تصنيف وضبط المخاطر المرتبطة بتسريب البيانات، وضوابط إدارية وأخلاقية على انتقالات العاملين فى إدرات أمن المعلومات.
  - معايير وطنية لإختبار كفاءة الأجهزة والتطبيقات المعلوماتية والرقمية
  - إعداد قواعد متمايزة لشراء تكنولوجيا وخدمات المعلومات فى الجهات بخلاف قواعد قانون المشتريات الحكومية التقليدية.
  - تفعيل وتوسيع دور المبادرات الطوعية الشخصية فى مجال الأمن السيبرانى على غرار مبادرة "سيدات فى الأمن السيبرانى" Women in Cyber Security Middle East، وغيرها من المبادرات.
  - التوسع فى نشاط خدمات التأمين ضد الهجمات السيبرانية: Cyber Insurance

قائمة بالسادة الخبراء المشاركون في ورشة العمل

أولاً: المشاركون من خارج معهد التخطيط القومي – وفق الترتيب الأبجدى:

م	الأسماء	بيان
1	أ. أحمد عطية	مدير عام أمن المعلومات – البورصة المصرية
2	م. أحمد حنفى	المدير تنفيذى لشركة Digital Planets
3	م. إيمان محمد	استشارى أمن المعلومات– شركة فورى
4	د. بهاء حسن	رئيس المؤتمر العربي لأمن المعلومات ورئيس مجلس إدارة شركتى: Arab Security Consultants & ISEC
5	م. حسام الجمل	رئيس مجلس إدارة شركة: ICON

م	الأسماء	بيان
6	أ. حسام السقا	رئيس إدارة أمن المعلومات – بنك مصر
7	د. سامح عبد الرحمن	مدير الإدارة العامة لأبحاث والحلول الفنية- الجهاز القومى لتنظيم الإتصالات – المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات EG-CERT
8	د. سمير جابر	المدير التنفيذى لأنظمة الرصد للهجمات السيبرانية والإنذار المبكر- الجهاز القومى لتنظيم الإتصالات – المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات EG-CERT
9	أ. عبير خضر	رئيس قطاع أمن المعلومات – البنك الأهلى المصري
10	م. محمد الحارثى	استشارى أمن المعلومات
11	د. محمد حجازى	خبير أمن المعلومات
12	م. محمد حنفى	نائب مدير معهد تكنولوجيا المعلومات – وزارة الإتصالات
13	د. محمد خليف	مستشار التحول الرقمى – عضو مجلس إدارة غرفة صناعة تكنولوجيا المعلومات
14	د. محمد نصر رسلان	مدير الإدارة العامة لفحص واكتشاف الثغرات السيبرانية- الجهاز القومى لتنظيم الإتصالات – المركز الوطنى للإستعداد لطوارىء الحاسبات والشبكات EG-CERT
15	أ. محمود يوسف	مدير إدارة أمن المعلومات- البورصة المصرية
16	م. وليد حجاج	خبير أمن المعلومات

ثانيًا: المشاركون من معهد التخطيط القومي:

م	الأسماء	بيان
1	أ.د. أماني الريس	نائب رئيس المعهد – عضو الفريق البحثى
2	أ.د. محمد ماجد خشبة	أستاذ دراسات مستقبلية – باحث رئيس
3	د. عصام الجوهرى	أستاذ مساعد نظم معلومات – عضو الفريق البحثى
4	د. داليا إبراهيم	مدرس محاسبة – عضو الفريق البحثى
5	د. هبة جمال الدين	مدرس سياسات عامة – عضو الفريق البحثى

م	الأسماء	بيان
6	أ. آيه ابراهيم	مدرس مساعد رياضيات وعلوم الحاسب – عضو الفريق البحثى
7	م. أحمد الدسوقى	باحث ماجستير – عضو الفريق البحثى
8	أ. أيمن سعد الدين	باحث ماجستير – عضو الفريق البحثى

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
1	دراسة الهيكل الإقليمي للعمالة فى القطاع العام فى جمهورية مصر العربية	ديسمبر 1977	د. محمد حسن فج النور	.....
2				
3	الدراسات التفصيلية لمقومات التنمية الإقليمية بمنطقة جنوب مصر	أبريل 1978		
4	دراسة تحليلية لمقومات التنمية الإقليمية بمنطقة جنوب مصر	يوليو 1978		
5	دراسة إقتصادية فنية لأفاق صناعة الأسمدة والتنمية الزراعية فى جمهورية مصر العربية حتى عام 1985	أبريل 1978		
6	التغذية والتنمية الزراعية فى البلاد العربية	أكتوبر 1978		
7	تطوير التنجارة وميزان المدفوعات ومشكلة تفاقم العجز الخارجى وسلبيات مواجهته (1970/69 – 1975)	أكتوبر 1978	د. الفونس عزيز	د.رمزى ذكي، د. عبد القادر حمزة وأخرون
8	Improving the position of third world countries in the international cotton economy,	يونيو 1979		
9	دراسة تحليلية لتفسير التضخم فى مصر (1970 1976)	أغسطس 1979	د.رمزى ذكي	.....

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
10	حوار حول مصر فى مواجهة القرن الحادى والعشرون	فبراير 1980	د. على نصار	.....
11	تطوير أساليب وضع الخطط الخمسية باستخدام نماذج البرمجة الرياضية فى جمهورية مصر العربية	مارس 1980	د. محرم الحداد	.....
12	دراسة تحليلية للنظام الضريبى فى مصر (1970/71-1978)	مارس 1980	أ. عبد اللطيف حافظ،	د.أحمد الشرقاوي وأخرون
13	تقييم سياسات التجارة الخارجية والنقد الاجنبى وسبل ترشيدها	يوليو 1980	د. أفونس عزيز	د. صقر أحمد صقر وأخرون
14	التنمية الزراعية فى مصر ماضيها وحاضرها (ثلاثة أجزاء)	يوليو 1980	د. موريس مكرم الله	د. سعد علام وأخرون
15	A study on Development of Egyptian National fleet/	June 1985	.....	.....
16	الإنفاق العام والإستقرار الاقتصادى فى مصر 1970 – 1979	ابريل 1981	د. رمزي ذكي	.....
17	الأبعاد الرئيسية لتطوير وتنمية القرى المصرية	يونيو 1981	أ. لبيب زمزم	د. سليمان حزين وأخرون
18	الصناعات الصغيرة والتنمية الصناعية (التطبيق على صناعة الغزل والنسيج فى مصر	يوليو 1981	د. ممدوح فهمي الشرقاوي	د.رأفت شفيق، د. ثروت محمد علي وأخرون
19	ترشيد الإدارة الاقتصادية للتجارة الخارجية والنقدية الأجنبية	ديسمبر 1981	د. فونس عزيز	د.سيد دحية وأخرون
20	الصناعات التحويلية فى	أبريل 1982	د. محمد عبد الفتاح	د.ثروت محمد على، د.راجية

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	المصري. (ثلاثة أجزاء)		منجي	عابدين خير الله وأخرون
21	التنمية الزراعية فى مصر (جزئين)	سبتمبر 1982	د. موريس مكرم الله	د. عبد القادر دياب، د. أحمد عبد الوهاب برانية وأخرون
22	مشاكل إنتاج اللحوم والسياسات المقترحة للتغلب عليها	أكتوبر 1983	د. محمد عبد الفتاح منجى	د. سعد علام، د. عبد القادر دياب وأخرين
23	دور القطاع الخاص فى التنمية	نوفمبر 1983	د. محمد عبد الفتاح منجى	د. فوزي رياض، د. ممدوح فهي الشرقاوي واخرين
24	تطوير معدلات الاستهلاك من السلع الغذائية وأثارها على السياسات الزراعية فى مصر	مارس 1985	د. سعد طه علام	د. عبدالقادرديباب، د. عبد العزيز إبراهيم
25	البحيرات الشمالية بين الاستغلال النباتى والاستغلال السمكى	أكتوبر 1985	ا.د. احمد عبد الوهاب برانيه	ا.د بركات أحمد الفرا، ا.د عبد العزيز إبراهيم
26	تقييم الاتفاقية التوسع التجارى والتعاون الاقتصادى بين مصر والهند ويوغوسلافيا	أكتوبر 1985	د. أحمد عبد العزيز الشرقاوي	د. محمود عبد الحى صلاح، د. محمد قاسم عبد الحي وأخرون
27	سياسات وإمكانيات تخطيط الصادرات من السلع الزراعية	نوفمبر 1985	د. سعد طه علام	د. عبد القادر دياب،د. محمد نصر فريد وأخرون
28	الإنفاق المستقبلية فى صناعة الغزل والنسيج فى مصر	نوفمبر 1985	د. فوزى رياض فهمى	د. محمد عبد المجيد الخلوى، د. مصطفي أحمد مصطفي وأخرون
29	دراسة تمهيدية لاستكشاف أفاق الاستثمار الصناعى فى إطار	نوفمبر 1985	د. محمد عبد الفتاح منجي	د. فتحي الحسيني خليل، د. رأفت شفيق وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	التكامل بين مصر والسودان			
30	دراسة تحليلية عن تطوير الاستثمار فى ج.م.ع مع الإشارة للطاقة الاستيعابية للإقتصاد القومى	ديسمبر 1985	د. السيد عبد العزيز دحيه	.....
31	دور المؤسسات الوطنية فى تنمية الأساليب الفنية للإنتاج فى مصر (جزئين)	ديسمبر 1985	د. الفونس عزيز قديس	.....
32	حدود وإمكانات مساهمة ضريبية على الدخل الزراعى فى مواجهة مشكلة العجز فى الموازنة العامة للدولة واصلاح هيكل توزيع الدخل القومى	يوليو 1986	د. رجاء عبد الرسول حسن	.....
33	التفاوتات الإقليمية للنمو الاقتصادى والاجتماعى وطرق فياسها فى جمهورية مصر العربية	يوليو 1986	د.علا سليمان الحكيم	.....
34	مدى إمكانية تحقيق اكتفاء ذاتى من القمح	يوليو 1986	د. رجاء عبد الرسول حسن	.....
35	Integrated Methodology for Energy planning in Egypt.	سبتمبر 1986	د.عماد الشرقاوى امين	د. راجيه عابدين
36	الملامح الرئيسية للطلب على تملك الاراضى الزراعية الجديدة والسياسات المتصلة باستصلاحها واستزراعها	نوفمبر 1986		.....
37	دراسة بعنوان مشكلات صناعة	مارس 1988	د.هدى محمد	.....

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	الألبان فى مصر		صالح	
38	دراسة بعنوان آفاق الاستثمارات العربية ودورها فى خطط التنمية المصرية	مارس 1988	د.مصطفى أحمد مصطفى	د. مجدي محمد خليفة، حامد إبراهيم وأخرون
39	تقدير الإيجار الاقتصادى للأراضى الزراعية لزراعة المحاصيل الزراعية الحقلية على المستوى الإقليمي لجمهورية مصر العربية عامى 1985/80	مارس 1988	د.احمد حسن ابراهيم	.....
40	السياسات التسويقية لبعض السلع الزراعية وآثارها الاقتصادية	يونيو 1988	د. سعد طه علام	د. بركات الفرا، د. هدى محمد صالح وأخرون
41	بحث الاستزراع السمكى فى مصر ومحددات تنميته	أكتوبر 1988	د.على ابراهيم عرابي	.....
42	نظم توزيع الغذاء فى مصر بين الترشيد والإلغاء	أكتوبر 1988	د.محمد سمير مصطفى	.....
43	دور الصناعات الصغيرة فى التنمية دراسة استطلاعية لدورها الاستيعاب العمإلى	أكتوبر 1988	د. حسام محمد مندور	د. محمد عبد المجيد الخلوى، د. حسينطهالخبيروأخرون
44	دراسة تحليلية لبعض المؤشرات المالية للقطاع العام الصناعى التابع لوزارة الصناعة	أكتوبر 1988	د. ثروت محمد على	.....
45	الجوانب التكاملية وتحليل القطاع الزراعى فى خطط التنمية الاقتصادية والاجتماعية	فبراير 1989	د.سيد حسين احمد	.....
46	إمكانيات تطوير الضرائب	فبراير 1989	د.احمد حسن	.....

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	العقارية لزيادة مساهمتها فى الإيرادات العامة للدول فى مصر		ابراهيم	
47	مدى إمكانية تحقيق ذاتى من السكر	سبتمبر 1989	د. سعد طه علام	د. هدى محمد صالح وأخرون
48	دراسة تحليلية لاثار السياسات الاقتصادية والمالية والنقدية على تطوير وتنمية القطاع الزراعى	فبراير 1990	د.سيد حسين احمد	د. سيد عزب، د. بركات الفرا وأخرون
49	الإنتاجية والأجور والأسعار الوضع الراهن للمعرفة النظرية والتطبيقية مع إشارة خاصة للدراسات السابقة عن مصر	مارس 1990	د.ابراهيم حسن العيسوى	د. عثمان محمد عثمان، د. سهير أبو العنين وأخرون
50	المسح الاقتصادى والاجتماعى والعمرانى لمحافظة البحر الأحمر وفرص الاستثمار المتاحة للتنمية	مارس 1990	د.احمد برانية	.....
51	سياسات إصلاح ميزان المدفوعات المصرية للمرحلة الآولى	مايو 1990	د.السيد عبد المعبود ناصف	د. فادية محمد عبد السلام، د. مجدى محمد خليفة وأخرون
52	بحث صناعة السكر وإمكانية تصنيع المعدات الرأسمالية فى مصر	سبتمبر 1990	د.حسام محمد مندور	د. محمد عبد المجيبد الخلوى، د. حامد إبراهيم وأخرون
53	بحث الإعتماد على الذات فى مجال الطاقة من منظور تنموى	سبتمبر 1990	د.راجية عابدين خير الله	د. عماد الشرقاوي أمين، د. فائق فريد فرج الله وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	وتكنولوجى			
54	التخطيط الاجتماعى والإنتاجية	أكتوبر 1990	د.وفاء احمد عبد الله	د. خضر عبد العظيم أبو قورة، د. محمد عبد العزيز عيد وأخرون
55	مستقبل استصلاح الاراضى فى مصر فى ظل محددات الأراضى والمياه والطاقة	أكتوبر 1990	د.محمد سمير مصطفى	د. عبد الرحيم مبارك هاشم، د. صلاح اسماعيل
56	دراسات تطبيقية لبعض قضايا الإنتاجية فى الاقتصاد المصري	نوفمبر 1990	د.عثمان محمد عثمان	د. أحمد حسن إبراهيم، د. هدي محمد صبحي مصطفي وأخرون
57	بنوك التنمية الصناعية فى بعض دول مجلس التعاون العربي	نوفمبر 1990	د.رأفت شفيق بسادة	د. حسام محمد المندور
58	بعض آفاق التنسيق الصناعى بين دول مجلس التعاون العربي	نوفمبر 1990	د. فتحي الحسين خليل	د. ثروت محمد على وأخرون
59	سياسات إصلاح ميزان المدفوعات المصري(مرحلة ثانية)	نوفمبر 1990	د.السيد عبد المعبود ناصف	.....
60	بحث اثر تغيرات سعر الصرف على القطاع الزراعى وانعكاساتها الاقتصادية	ديسمبر 1990	د.محمد سمير مصطفى	د. محمود علاء عبد العزيز، د. عبد القادر دياب
61	الإمكانيات والأفاق المستقبلية للتكامل الاقتصادى بين دول مجلس التعاون العربي فى ضوء هياكل الإنتاج والتوزيع	يناير 1991	د.مجدي محمد خليفه	.....

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
62	إمكانية التكامل الزراعى بين مجلس التعاون العربي	يناير 1991	د. سعد طه علام	د. هدى صالح النمر، د. عماد الدين مصطفي
63	دور الصناديق العربية فى تمويل القطاع الزراعى	أبريل 1991	د.سيد حسين احمد	د. محمد نصر فريد، د. بركات أحمد الفرا وأخرون
64	بعض القطاعات الإنتاجية والخدميه بمحافظة مطروح(جزئين) الجزء الأول: القطاعات الإنتاجية	أكتوبر 1991	د.صالح حسين مغيب	د. فريد أحمد عبد العال
65	مستقبل إنتاج الزيوت فى مصر	أكتوبر 1991	د. سعد طه علام	د. براكات أحمد الفرا، د. هدي صالح النمر وأخرون
66	الإنتاجية فى الاقتصاد القومى المصري وسبل تحسينها مع التركيز على قطاع الصناعة (الجزء الأول) الأسس والدراسات النظرية	أكتوبر 1991	د.محرم الحداد	د. أماني عمر زكي، د. محمد ابو الفتح الكفراوي وأخرون
66	الإنتاجية فى الاقتصاد القومى المصري وسبل تحسينها مع التركيز على قطاع الصناعة (الجزء الثانى) الدراسات التطبيقية	أكتوبر 1991	د.محرم الحداد	د. أماني عمر زكي، د. محمد ابو الفتح الكفراوي وأخرون
67	خلفية ومضمون النظريات الاقتصادية الحالية والمتوقعة بشرق أوروبا. ومحددات انعكاساتها الشاملة على مستقبل	ديسمبر 1991	د.سعد حافظ	د. على نصار

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	التنمية فى مصر والعالم العربي			
68	ميكنة الأنشطة والخدمات فى مركز التوثيق والنشر	ديسمبر 1991	د.اماني عمر	د. رمضان عبد المعطي، د. امال حسن الحريري وأخرون
69	إدارة الطاقة فى مصر فى ضوء أزمة الخليج وانعكاساتها جوليا وإقليميا ومحليا	يناير 1992	د.راجيه عابدين خير الله	.....
70	واقع آفاق التنمية فى محافظات الوادى الجديد	يناير 1992	د. عزه عبد العزيز سليمان	د. فريد أحمد عبد العال وأخرون
71	انعكاسات أزمة الخليج(1991/90) على الاقتصاد المصري	يناير 1992	د.مصطفى أحمد مصطفى	د. سلوي محمد مرسي، د. مجدى محمد خليفة وأخرون
72	الوضع الراهن والمستقبلى لإقتصاديات القطن المصري	مايو 1992	د.عبد القادر دياب	د. عبد الفتاح حسين، د. هدى صالح النمر وأخرون
73	خبرات التنمية فى الدول الأسيوية حديثة التصنيع وامكانية الاستفادة منها فى مصر	يوليو 1992	د.ابراهيم حسن العيسوي	د. رمزي زكي، د. حسين الفقير
74	بعض قضايا تنمية الصادرات الصناعية المصرية	سبتمبر 1992	د.فتحى الحسيني خليل	.....
75	تطوير مناهج التخطيط وإدارة التنمية فى الاقتصاد المصري فى ضوء المتغيرات الدولية المعاصرة	سبتمبر 1992	د.عثمان محمد عثمان	د. رافت شفيق بسادة، د. سهير أبو العنين وأخرون
76	السياسات النقدية فى مصر خلال الثمانينات " المرحلة الاولى"	سبتمبر 1992	د.السيد عبد المعبود ناصف	فاديةمحمدعبدالسلام

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	ميكانيكية وفاعلية السياسة النقدية فى الجانب المالي والاقتصادى المصري			
77	التحرير الاقتصادى وقطاع الزراعة	يناير 1993	سعد طه علام	د. سيد حسين أحمد، د. بركات أحمد الفرا وأخرون
78	احتياجات المرحلة المقبلة للإقتصاد المصري ونماذج التخطيط واقتراح بناء نموذج إقتصادى قومى للتخطيط التأشيرى المرحلة الاولى	يناير 1993	د.محرم الحداد	د. على نصار، د. ماجدة إبراهيم وأخرون
79	بعض قضايا التصنيع فى مصر منظور تنموى تكنولوجى	مايو 1993	راجيه عابدين خير الله	د. فتحية زغلول، د. نوال على حله وأخرون
80	تقويم التعليم الاساسى فى مصر	مايو 1993	د.محمد عبد العزيز عيد	د. سالم عبد العزيز محمود، د. دسوقي عبد الجليل وأخرون
81	الآثار المتوقعة لتحرير سوق النقد الاجنبى على بعض مكونات ميزان المدفوعات المصري	مايو 1993	د. اجلال راتب العقيلي	د. الفونس عزيز ، د. فادية عبد السلام وأخرون
82	The Current development in the methodology and applications of operations research obstacles and prospects in developing	Nov 1993	د.اماني عمر	د عفاف فؤاد، د صلاح العدوي وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	countries			
83	الآثار البيئية الزراعية	نوفمبر 1993	د. سعد طه علام	
84	تقييم البرامج للنهوض بالإنتاجية الزراعية	ديسمبر 1993	د.محمد سمير مصطفى	د. هدى صالح النمر وأخرون، د. عبد القادر محمد دياب
85	اثر قيام السوق الأوربية المشتركة على مصر والمنطقة	يناير 1994	د. إجلال راتب العقيلي	د. أحمد هاشم، د. مجدي خليفة وأخرون
86	مشروع إنشاء قاعدة بيانات الأنشطة البحثية بمعهد التخطيط القومى " المرحلة الاولى"	يونيو 1994	د.محرم الحداد	د. عبد القادر محمد دياب، د. أماني عمر زكي وأخرون
87	الكوارث الطبيعية وتخطيط الخدمات فى ج.م.ع (دراسة ميدانية عن زلزال أكتوبر 1992 فى مدينة السلام)	سبتمبر 1994	د.وفاء احمد عبد الله	.....
88	تحرير القطاع الصناعى العام فى مصر فى ظل المتغيرات المحلية والعالمية	سبتمبر 1994	راجيه عابدين خير الله	د. فتحية زعلول، د. ثروت محمد على وأخرون
89	إستشراف بعض الآثار المتوقعة لسياسة الإصلاح الاقتصادى بمصر (مجلدان)	سبتمبر 1994	د. رمزي زكي	د. عثمان محمد عثمان وأخرون، د. أحمد حسن إبراهيم
90	واقع التعليم الاعدادى وكيفية تطويره	نوفمبر 1994	د.محمد عبد العزيز عيد	.....
91	تجربة تشغيل الخريجين	ديسمبر 1994	د.عبد القادر دياب	.....

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	بالمشروعات الزراعية وافق تطويرها			
92	دور الدولة فى القطاع الزراعى فى مرحلة التحرير الاقتصادى	ديسمبر 1994	د.سعد طه علام	د. محمد محمود رزق، د. نجوان سعد الدين وأخرون
93	الأبعاد الاقتصادية والاجتماعية لتحرير القطاع الصناعى المصري فى ظل الإصلاح الاقتصادى	يناير 1995	د.راجيه عابدين خير الله	د. فتحية زغلول، د. نفسية سيد أبو السعود وأخرون
94	مشروع انشاء قاعدة بيانات الانشطة البحثية بمعهد التخطيط القومى (المرحلة الثانية)	فبراير 1995	د.محرم الحداد	د. أماني عمر زكي عمر، د. حسين صالح وأخرون
95	السياسات القطاعية فى ظل التكيف الهيكلى	أبريل 1995	د.محمود عبد الحى صلاح	.....
96	الموازنة العامة للدولة فى ضوء سياسة الإصلاح الاقتصادى	يونية 1995	د.ثروت محمد على	د. محمد نصر فريد، د. نبيل عبد العليم صالح وأخرون
97	المستجدات العالمية (الجات وأوروبا الموحدة) وتأثيراتها على تدفقات رؤوس الأموال والعمالة والتجارة السلعية والخدمية (دراسة حالة مصر)	أغسطس 1995	د.إجلال راتب	د. مصطفي أحمد مصطفي، د. سلوى محمد مرسي وأخرون
98	تقييم البدائل الإجرائية لتوسع قاعدة الملكية فى قطاع الأعمال العام	يناير 1996	فتحي الحسينى خليل	د. صالح حسين مغيب، د. محمد عبد المجيد الخلوى وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
99	أثر التكتلات الاقتصادية الدولية على قطاع الزراعى	يناير 1996	د.سعد طه علام	د. محمود مرعى، د. منى الدسوقي
100	مشروع إنشاء قاعدة بيانات الأنشطة البحثية بمعهد التخطيط القومى (المرحلة الثالثة)	مايو 1996	د.محرم الحداد	د. أماني عمر زكي، د. ماجدة إبراهيم سيد فراج وأخرون
101	دراسة تحليلية مقارنة لواقع القطاعات الإنتاجية والخدمية بمحافظات الحدود	مايو 1996		
102	التعليم الثانوى فى مصر: واقعة ومشاكله واتجاهات تطويره	مايو 1996	د.محمد عبد العزيز عيد	د. لطف الله إمام صالح، د. دسوقي عبد الجليل وأخرون
103	التنمية الريفية ومستقبل القرية المصرية: المتطلبات والسياسات	سبتمبر 1996	د.سعد طه علام	د. بركات احمد الفرا، د. أحمد عبد الوهاب برانية وأخرون
104	دور المناطق الحرة فى تنمية الصادرات	أكتوبر 1996	د.اجلال راتب	د. محمود عبد الحي، د. حسين صالح وأخرون
105	تطوير أساليب وقواعد المعلومات فى إدارة الأزمات المهددة لأطراد التنمية(المرحلة الأولى)	نوفمبر 1996	د.محرم الحداد	د. حسام مندرة وأخرون، د. ماجدة إبراهيم سيد فراج
106	المنظمات غير الحكومية والتنمية فى مصر (دراسة حالات)	ديسمبر 1996	د.نادرة وهدان	د. وفيق أشرف حسونة، د. وفاء عبد الله وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
107	الأبعاد البيئية المستدامة فى مصر	ديسمبر 1996	د.راجية عابدين خير الله	د. نفيسة سيد محمد أبو السعود
108	التغيرات الهيكلية فى مؤسسات التمويل الزراعى: مصادر ومستقبل التمويل الزراعى فى مصر	مارس 1997	د.محمد عبد العزيز عيد	د. وفيق أشرف حسونة، د. لطف الله إمام صالح وأخرون
109	التغيرات الهيكلية فى مؤسسات التمويل الزراعى ومصادر ومستقبل التمويل الزراعى فى مصر	أغسطس 1997	د.ثروت محمد على	إبراهيم صديق على، د. بهاء مرسي وأخرون
110	ملامح الصناعة المصرية فى ظل العوامل الرئيسية المؤثرة فى مطلع القرن الحادى والعشرين	ديسمبر 1997	د.ممدوح فهمي الشرقاوى	د. فتحي الحسن خليل، د. ثروت محمد على وأخرون
111	آفاق التصنيع وتدعيم الأنشطة غير المزرعية من اجل تنمية ريفية مستدامة فى مصر	فبراير 1998	د.سعد طه علام	د. هدي النمر، د. منى الدسوقي وأخرون
112	الزراعة المصرية والسياسية الزراعية فى اطار نظام السوق الحرة	فبراير 1998	د.هدي صالح النمر	د. عبد القادر دياب، د. محمد سمير مصطفي
113	الزراعة المصرية فى مواجهة القرن الواحد والعشرين	فبراير 1998	د.سعد طه علام	د. هدي النمر، د. منى الدسوقي وأخرون
114	التعاون بين الشرق الأوسط وشمال أفريقيا	مايو 1998	د.اجلال راتب	د. محمود عبد الحي، د. فادية عبد السلام وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
115	تطوير أساليب وقواعد المعلومات فى إدارة الأزمات المهددة بطرد التنمية (المرحلة الثالثة)	يونيو 1998	د.محرم الحداد	د. حسام مندرة، د. اماني عمر زكي عمر وأخرون
116	حول أهم التحديات الاجتماعية فى مواجهة القرن21	يونية 1998	د.وفاء احمد عبد الله	د. عبد العزيز عيد، د. نادرة وهدان وأخرون
117	محددات الطاقة الادخارية فى مصر دراسة نظرية وتطبيقية	يونية 1998	د.ابراهيم العيسوى	د. أحمد حسن إبراهيم، د. سهير أبو العنين وأخرون
118	تصور حول تطوير نظام المعلومات الزراعية	يوليو 1998	د.عبد القادر دياب	د. محمد سمير مصطفي، د. أحمد عبد الوهاب برانية وأخرون
119	التوقعات المستقبلية لإمكانيات الاستصلاح والاستزراع بجنوب الوادى	سبتمبر 1998	د.سعد طه علام	د. عبد القادر دياب، د. هدي النمر وأخرون
120	إستراتيجية استغلال البعد الحيزى فى مصر فى ظل الاصلاح الاقتصادى	ديسمبر 1998	د.سيد محمد عبد المقصود	د. السيد محمد الكيلاني، د. علا سليمان الحكيم وأخرون
121	حولت إلى مذكرة خارجية رقم (1601)	ديسمبر 1998	د.ايمان احمد الشربيني	.....
122	Artificial Neural Networks Usage for Underground Water storage & River Nile in Toshoku Area	ديسمبر 1998	د.عبد الله الداعوشى	د.أماني عمر، د. سمير ناصر وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
123	بنـــاء وتطبيـــق نمـــوذج متعـــددالقطاعات للتخطـــيط التأشيرى فى مصر	ديسمبر 1998	د.ماجدة ابراهيم	د. عبـد القـادر حمـزة ، د. سهير أبو العينين وأخرون
124	إقتصاديات القطاع السياحى فى مصروانعكاساتها على الاقتصاد القومى	ديسمبر1998	د.اجلال راتب	د. محمـود عبـد الحـي، د. فادية عبد السلام وأخرون
125	تحديات التنمية الراهنة فى بعض محافظات جنوب مصر	فبراير 1999	د.سيد محمد عبد المقصود	.....
126	الآفـاق والإمكانيـات التكنولوجيـة فى الزراعة المصرية	سبتمبر 1999	د.سعد طه علام	د. هـدى النمـر ، د. عمـاد مصطفي وأخرون
127	إدارة التجـارة الخارجيـة فـى ظـل سياسات التحرير الاقتصادى	سبتمبر 1999	د.اجلال راتب	د. محمـود عبـد الحـي، د. فادية عبد السلام وأخرون
128	قواعـد ونظـم معلومـات التفـاوض فى المجالات المختلفة	سبتمبر 1999	د.محرم الحداد	د. حسـام منـدور، د. محمـد يحيى عبد الرحمن وأخرون
129	اتجاهات تطوير نموذج لإختيار السياسات الاقتصادية للإقتصاد المصري	يناير 2000	د.ماجدة ابراهيم	د. عبـد القـادر حمـزة، د. سهير أبو العنين وأخرون
130	دراسة الفجوة النوعية لقوة العمل فـى محافظـات مصـر وتطورهـا خلال الفترة 1986-1996	يناير 2000	د.عـزه عبـد العزيـز سليمان	د. سيد محمد عبد المقصود ، د. السـيد محمـد الكيلاني وأخرون
131	التعلـيم الفنـى وتحـديات القـرن الحادى والعشرون	يناير 2000	د.محمد عبد العزيز عيد	د. دسـوقي حسـين عبـد الجليل، د. زينات محمد

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
				طبالة وأخرون
132	أنماط الاستيطان فى منطقة جنوب الوادى " توشكى "	يونيو 2000	د.سيد محمد عبد المقصود	د. السيد محمد الكيلاني، د. علا سليمان الحكيم وأخرون
133	فرص ومجالات التعاون بين مصر ومجموعات دول الكوميسا	يونيو 2000	د.محمد محمود رزق	د. ممدوحالشرقاويوأخرون
134	الإعاقة والتنمية فى مصر	يونيو 2000	د.نادرة وهدان	د. وفيق اشرف حسونة، د. وفاء أحمد عبد الله وأخرون
135	تقويم رياض الأطفال فى القاهرة الكبرى	يناير 2001	د.محمد عبد العزيز عيد	د. دسوقي عبد الجليل، د. إيمان منجي وأخرون
136	الجمعيات الأهلية وآوليات التنمية بمحافظات جمهورية مصر العربية	يناير 2001	د.عزه عبد العزيز سليمان	د. محاسن مصطفى. حسنين، د. خفاجى، محمد عبد اللطيف.
137	آفاق ومستقبل التعاون الزراعى فى المرحلة القادمة	يناير 2001	د.احمد عبد الوهاب برانيه	د. مصطفي، عماد الدين.، د. سعد الدين، نجوان.
138	تقويم التعليم الصحى الفنى فى مصر	يناير 2001	د.نادرة وهدان	د. وفيق اشرف حسونة، د. عزة الفندري وأخرون
139	منهجية جديدة للإستخدام الأمثل للمياه فى مصر مع التركيز على مياه الرى الزراعى مرحلة أولى	يناير 2001	د.محمد محمد الكفراوي	د. أماني عمر زكي، د. فتحية زغلول وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
140	التعاون الاقتصادى المصري الدولي _ دراسة بعض حالات الشراكه	يناير 2001	د.اجلال راتب	د. محمود عبد الحي، د. مجدي خليفة وأخرون
141	تصنيف وترتيب المدن المصرية(حسب بيانات تعداد 1996)	يناير 2001	د.السيد محمد كيلاني	د. سيد محمد عبد المقصود، د. علا سليمان الحكيم وأخرون
142	الميزة النسبية ومعدلات الحماية للبعض من السلع الزراعية والصناعية	يناير 2001	د.عبد القادر دياب	د. ممدوح الشرقاوي، د. محمد محمود رزق وأخرون
143	سبل تنمية الصادرات من الخضر	ديسمبر 2001	د.هدى صالح النمر	د. سيد حسين، د. بركات أحمد الفرا وأخرون
144	تحديد الاحتياجات التدريبية لمعلمى المرحلة الثانوية	ديسمبر 2001	د.محمد عبد العزيز عيد	محرم الحداد، د. ماجدة إبراهيم وأخرون
145	التخطيط بالمشاركة بين المخططين والجمعيات الأهلية على المستويين المركزى والمحافظات	فبراير 2002	د.عزه عبد العزيز سليمان	د. محاسن مصطفي حسنين، د. يمن حافظ الحماقي وأخرون
146	أثر البعد المؤسسى والمعوقات الإدارية والتسويق على تنمية الصادرات الصناعية المصرية	مارس 2002	د.ممدوح فهمي الشرقاوى	د. محمد حمدي سالم، د. محمد يحي عبد الرحمن وأخرون
147	قياس استجابة مجتمع المنتجين الزراعيين للسياسات الزراعية	مارس 2002	د.عبد القادر دياب	د. نجوان سعد الدين، د. أحمد عبد الوهاب برانية

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
				وأخرون
148	تطوير منهجية جديدة لحساب الاستخدام الأمثل للمياه فى مصر (مرحلة ثانية)	مارس 2002	د.محمد محمد الكفراوي	د. أماني عمر زكي، د. عبد القادر حمزة وأخرون
149	رؤية مستقبلية لعلاقات ودوائر التعاون الاقتصادى المصري الخارجى" الجزء الأول" حلفية أساسية "	مارس 2002	د.محمود محمد عبد الحى	د. إجلال راتب العقيلي، د. مصطفي أحمد مصطفي
150	المشاركة الشعبية ودورها فى تعاظم أهداف خطط التنمية المعاصرة المحلية الريفية والحضرية	ابريل 2002	د.وفاء احمد عبد الله	د. نادرة عبد الحليم وهدان، د. عزة الفندري وأخرون
151	تقدير مصفوفة حسابات اجتماعية للإقتصاد المصري عام 1998 – 1999	أبريل 2002	د. سهير ابو العينين	.....
152	الأشكال التنظيمية وصيغ وأليات تفعيل المشاركة فى عمليات التخطيط على مستوى القطاع الزراعى	يوليو 2002	د.هدى صالح النمر	د. عبد القادر محمد دياب، د. محمد سمير مصطفي وأخرون
153	نحو استراتيجية للاستفادة من التجارة الإلكترونية فى مصر	يوليو 2002	د.محرم الحداد	د. حسام مندرة، د. فادية عبد العزيز وأخرون
154	صناعة الأغذية والمنتجات الجلدية فى مصر (الواقع والمستقبل)	يوليو 2002	د.ممدوح فهمي الشرقاوى	د. إيمان أحمد الشربيني، د. محمد حسن توفيق

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
155	تقدير الاحتياجات التمويلية لتطوير التعليم ما قبل الجامعى وفقاً لإستراتيجية متعددة الأبعاد	يوليو 2002	د.محمد عبد العزيز عيد	د. ماجدة إبراهيم، د. زينات طبالة وأخرون
156	الاحتياجات العملية والإستراتيجية للمرأة المرية وأولوياتها على مستوى المحافظات	يوليو 2002	د.عزه عبد العزيز سليمان	د. اجلال راتب العقيلي، د. محاسن مصطفي حسنين وأخرون
157	موقف مصر فى التجمعات الإقليمية	يوليو 2002	د.سلوى مرسي محمد فهمي	د. مجديمحمدخليفةوأخرون
158	إدارة الدين العام المحلى وتمويل الاستثمارات العامة فى مصر	يوليو 2002	د.السيد عبد العزيز دحيه	د. نفين كمال، د. سهير أبو العنين وأخرون
159	التأمين الصحى فى واقع النظام الصحى المعاصر	يوليو 2002	د.عزه عمر الفندري	د. وفاء أحمد عبد الله، د. نادرة عبد الحليم وهدان وأخرون
160	تطبيق الشبكات العصبية فى قطاع الزراعة	يوليو 2002	د.محمد محمد الكفراوي	د. اماني عمر زكي، د. عبد القادر حمزة وأخرون
161	الإنتاج والصادرات المصرية من مجمدات وعصائر الخضر والفاكهة ومقترحات زيادة القدرة التنافسية لها بالأسواق المحلية والعالمية	يوليو 2002	د.سمير عريقات	د. مني عبد العال الدسوقي، د. محمد مرعي وأخرون
162	تقسيم مصر إلى أقاليم تخطيطية	يناير 2003	د.سيد محمد عبد المقصود	د. السيد محمد الكيلاني، د. فريد أحمد عبد العال وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
163	تقييم وتحسين أداء بعض المرافق " مياه الشرب والصرف الصحى"	يوليو 2003	د.محرم الحداد	د. حسام منـدور، د. نفيسة أو السعود وأخرون
164	تصورات حول خصخصة بعض مرافق الخدمات العامة	يوليو 2003	د.عبد القادر دياب	د. سيد حسين أحمد، د. ياسر كمال السيد وأخرون
165	تحديد الاحتياجات التمويلية للتعليم العإلى " دراسة نظرية تحليلية ميدانية "	يوليو 2003	د.محمد عبد العزيز عيد	د. ماجدة إبراهيم، د. زينات محمد طلبة وأخرون
166	دراسة أهمية الآثار البيئية للأنشطة السياحة فى محافظة البحر الأحمر " بالتركيز على مدينة الغردقة"	يوليو 2003	د.سلوى مرسي محمد فهمي	د. وفاء أحمد عبد الله، د. أحمد برانية وأخرون
167	العوامل المحددة للنمو الاقتصادى فى الفكر النظرى وواقع الاقتصاد المصري	يوليو 2003	د. سهير ابو العينين	د. نيفين كمال حامد وأخرون، د. فتحية زغلول وأخرون
168	العدالة فى توزيع ثمار التنمية فى بعض المجالات الاقتصادية والاجتماعية فى محافظات مصر " دراسة تحليلية"	يوليو 2003	د.عزه عبد العزيز سليمان	د. سيد محمد عبد المقصود ، د. السيد محمد الكيلاني وأخرون
169	تقييم وتحسين جودة أداء بعض الخدمات العامة لقطاعى التعليم والصحة باستخدام شبكات الأعمال	يوليو 2003	د.عبد القادر حمزه	د. أماني عمر، د. ماجدة إبراهيم وأخرون
170	دراسة الأسواق الخارجية وسبل	يوليو 2003	د.فادية عبد السلام	د. مصطفي أحمد مصطفي

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	النفاذ اليها			وأخرون، د. اجلال راتب
171	أولويات الاستثمار فى قطاع الزراعة	يوليو 2003	د.هدي صالح النمر	أحمد عبد الوهاب برانية، د. سيد حسين
172	دراسة ميدانية للمشاكل والمعوقات التى تواجه صناعة الأحذية الجديدة فى مصر " التطبيق على محافظة القاهرة ومدينة العاشر من رمضان"	يوليو 2003	د.ممدوح فهمي الشرقاوى	د. حسام محمد مندور، د. إيمان أحمد الشربيني وأخرون
173	قضية التشغيل والبطالة على المستوى العالمي والقومى والمحلى	يوليو 2003	د.عزيزة على عبد الرازق	د. اجلال راتب، د. محرم الحداد وأخرون
174	بناء وتنمية القدرات البشرية المصرية " القضايا والمعوقات الحاكمة"	يوليو 2003	د.مصطفى احمد مصطفى	د. إبراهيم حسن العيسوي، د. محمد على نصار وأخرون
175	بناء قواعد التقدم التكنولوجى فى الصناعة المصرية من منظور مداخل التنافسية والتشغيل والتركيب القطاعى	يوليو 2004	د.محرم الحداد	د. قتحية زغلول، د. إيمان الشربيني وأخرون
176	استراتيجية قومية مقترحة للإدارة المتكاملة للمخلفات الخطرة فى مصر	يوليو 2004	د.نفيسه ابو السعود	د. خالد محمد قهمي، د. حنان رجائي وأخرون
177	تحسين الجودة الشاملة لبعض مجالات اقطاع الصحى	يوليو 2004	د.عبد القادر حمزه	د. أماني عمر، د. محمد الكفراوي وأخرون
178	مخاطر الأسواق الدولية للسلع الغذائية للسلع الغذائية الإستراتيجية وإمكانيات وسياسات وأدوات مواجهتها	يوليو 2004	د.عبد القادر دياب	د. ممدوح الشرقاوي، د. سيد حسين وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
179	إمكانيات وأثار قيام منطقة حره بين مصر والولايات المتحدة الأمريكية والمناطق الصناعية المؤهلة (ودروس مستفادة للإقتصاد المصري)	يوليو 2004	د.فادية عبد السلام	د. اجلال راتب العقيلي، د. سلوى محمد مرسي وأخرون
180	نحو هواء نظيف لمدينة عملاقة	يوليو 2004	د.محمد سمير مصطفى	د. السيد محمد الكيلاني، د. عبد الحميد القصاص وأخرون
181	تحديد الاحتياجات بقاعات الصرف – التعليم ما قبل الجامعى – التعليم العالى (عدد خاص)	يوليو 2004	د.زينات محمد طباله	د. لطف الله إمام صالح، د. عزة عمر الفنردي
182	تحديد الاحتياجات بقطاعى الصرف الصحى والطرق والكبارى لمواجهة العشوائيات(عدد خاص)	يوليو 2004	د.محرم الحداد	د. نفيسة أبو السعود، د. نعيمة رمضان وأخرون
183	خصائص ومتغيرات السوق المصري _ دراسة تحليلية لبعض الأسواق المصرية الجزء الأول " الإطار النظرى والتحليلى "	يناير 2005	د.محرم الحداد	د. حسام مندور، د. فادية عبد السلام وأخرون
184	خصائص ومتغيرات السوق المصري (دراسة تحليلية لبعض الأسواق المصرية) الجزء الثانى: الإطار التطبيقى " سوق الخدمات التعليمية – سوق الخدمات السياحة – سوق البرمجيات"	يناير 2005	د.محرم الحداد	د. حسام المندور، د. فادية عبد السلام وأخرون
185	خصائص ومتغيرات السوق	يناير 2005	د.محرم الحداد	.....

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	المصري (دراسة تحليلية لبعض الأسواق المصرية الجزء الثالث: الإطار التطبيقى " يوق الأدوية – سوق السلع الغذائية والزراعية – سوق حديد التسليح والأسمنت"			
186	الملكية الفكرية والتنمية فى مصر	أغسطس2005	د. لطف الله امام صالح	.....
187	تقدير الطلب على العمالة – قوة العمل – البطالة فى ظل سيناريوهات بديلة	يونية 2006	د.عبد الحميد سامى القصاص	د. ماجدة إبراهيم سيد، د. زينات طبالة وأخرون
188	الحاسبات الإقليمية كمدخل للامركزية المالية	يونية 2006	د.علا سليمان الحكيم	د. السيد محمد الكيلاني، د. فريد أحمد عبد العال وأخرون
189	المعاشات والتأمينات فى جمهورية مصر العربية (الواقع وإمكانيات التطوير)	يونيه 2006	د.محمود عبد الحى	د. زينات طبالة، د. سمير رمضان وأخرون
190	بعض القضايا المتصلة بالصادرات(دراسة حالة الصناعات الكيماوية)	يونيه 2006	د.فاديه محمد عبد السلام	د. اجلال راتب العقيلي، د. مصطفي أحمد مصطفي وأخرون
191	مشروع تنمية جنوب الوادى " توشكى " بين الأهداف والإنجازات	يونية 2006	د.هدى صالح النمر	د. عبد القادر دياب، د. سيد حسين وأخرون
192	اللامركزية كمدخل لمواجهة بعض القضايا البيئية فى مصر (التوزيع الإقليمي للاستثمارات الحكومية وارتباطها ببعض قضايا البيئة)	يونية 2006	د.نفيسه ابو السعود	د. أحمد حسام الدين نجاتي، د. عزة يحيي وأخرون
193	نحو تطبيق نظام الإدارة البيئية	يونية 2006	د.نفيسه ابو السعود	د. أحمد حسام الدين نجاتي،

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	(الأيزو 14000) " على معهد التخطيط القومى" كنموذج لمؤسسة بحثية حكومية			د. زينب محمد نبيل
194	تكاليف تحقيق أهداف الألفية الثالثة بمصر	يونية 2006	د.محرم الحداد	د. حسام مندور، د. حنان رجائي وأخرون
195	السوق المصرية للغزل	يونية 2006	د.عبد القادر دياب	د. عبد القادر حمزة، د. محمد الكفراوي وأخرون
196	المعايير البيئية والقدرة التنافسية للصادرات المصرية	أغسطس 2007	د.سلوى مرسي محمد فهمي	د. سمير مصطفي، د. فادية عبد السلام وأخرون
197	استخدام أسلوب البرمجة الخطية والنقل فى البرمجة الرياضية لحل مشاكل الإنتاج والمخزون	أغسطس 2007	د.محمد محمد الكفراوي	د. عبد القادر حمزة، د. أماني عمر وأخرون
198	تقييم موقف مصر فى بعض الاتفاقيات الثنائية	أغسطس 2007	د.اجلال راتب	د. نجلاء علام، د. نبيل الشيمي وأخرون
199	التضخم فى مصر بحث فى أسباب التضخم، وتقييم مؤشراته، وجدوى استهدافه مع أسلوب مقترح باتجاهاته	أغسطس2007	د. إبراهيم العيسوى	د. سيد عبد العزيز دحية، د. سهير أبو العنين وأخرون
200	سبل تنمية مصادر الإنتاج الحيوانى فى ضوء الآثار الناجمة عن مرض أنفلونزا الطيور فى مصر	أغسطس 2007	د. صادق رياض ابو العطا	د. هدي النمر، د. محمد مرعي وأخرون
201	مستقبل التنمية فى محافظات الحدود (مع التطبيق على سيناء)	أغسطس2007	د.فريد احمد عبد العال	د. السيد محمد الكيلاني ، د. علا سليمان الحكيم وأخرون
202	سياسات إدارة الطاقة فى مصر	أغسطس2007	د.راجيه عابدين	د. فتحية زغلول، د. نجوان

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	فـــى ظـــل المتغيـــرات المحليـــة والإقليمية والعالمية		خير الله	سعد الدين وأخرون
203	جدوى إعادة هيكلة قطاع التأمين دراسة تحليلية ميدانية	أكتوبر 2007	د. محرم الحداد	د. حسـام منـدور، د. إيمـان أحمد الشربيني وأخرون
204	حـول تقـدير الاحتياجـات لأهـم خدمات رعاية المسنين (بالتركيز على محافظة القاهرة)	أكتوبر 2007	د.عزه عمر الفندري	د. وفـاء أحمـد عبـد الله، د. نادرة وهدان وأخرون
205	خدمات ما بعد البيع فى السوق المصـري (دراسـة حالـة للسـلع الهندسية والكهربائية) (بالتطبيق علـى صـناعة الأجهـزة المنزليـة وصناعة السيارات)	أكتوبر 2007	د. محمـــد عبـــد الشفيع عيسى	د. نجـلاء عـلام، د. عبـد السلام محمد السيد وأخرون
206	العناقيـد الصـناعية والتحالفـات الإسـتراتيجية لتـدعيم القـدرة التنافسـية للمشـروعات الصـغيرة والمتوسـطة فـى جمهوريـة مصـر العربية	فبراير 2008	د.ايمـــان احمـــد الشربيني	د. سحر عبد الحليم البهائي، د. أحمد سليمان وأخرون
207	تقييم فاعلية الخطة الإستراتيجية القومية للسكان فى مصر	سبتمبر 2008	د. محمـود ابـراهيم فرج	د. عبـد الغنـي، عبـد الغنـي محمـد.، د. نادية فهمـي وأخرون
208	الإسـقاطات القوميـة للسـكان فـى مصـر خـلال الفتـرة (2006 – 2031)	سبتمبر 2008	د.فريال عبد القادر احمد	د. سـعاد أحمـد الضـوي، د. عبد الغني محمد عبد الغني وأخرون
209	إدارة الجودة الشاملة وتطبيقها فى تقييم أداء بعض قطاعات المرافق العامة فى مصر	سبتمبر 2008	د. محرم الحداد	د. حسام المندور، د. اجلال راتب وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
210	الخصائص السكانية وانعكاساتها على القيم الاجتماعية	نوفمبر 2008	د.نادرة وهدان	د. زينات طبالة ، د. عزة الفندري وأخرون
211	التجارب التنموية فى كوريا الجنوبية، ماليزيا والصين: الإستراتيجيات والسياسات – الدروس المستفاده	نوفمبر 2008	د.فاديه عبد السلام	د. محمد عبد الشفيع، د. لطف الله إمام صالح وأخرون
212	مستوى المعيشة المفهوم والمؤشرات والمعلومات والتحليل دليل قياس وتحليل معيشة المصريين	نوفمبر 2008	د.ابراهيم العيسوي	د. السيد دحية، د. سيد حسين وأخرون
213	أولويات زراعة المحاصيل المستهلكة للمياه وسياسات وأدوات تنفيذها	فبراير 2009	د. عبد القادر دياب	د. هدي صالح النمر، د. سيد حسين
214	السياسات الزراعية المستقبلية لمصر فى ضوء المتغيرات المحلية والإقليمية	أغسطس 2009	د. نجوان سعد الدين عبد الوهاب	د. سعد طه علام، د. ممدوح الشرقاوي وأخرون
215	اتجاهات ومحددات الطلب على الإنجاب فى مصر (1988 – 2005)	أغسطس 2009	د. محمود ابراهيم فرج	د. فادية محمد عبد السلام، د. منى توفيق يوسف وأخرون
216	آليات تحقيق اللامركزية فى تخطيط وتنفيذ ومتابعة وتقييم البرنامج السكانى فى مصر	أغسطس 2009	د. عبد الغنى محمد عبد الغنى	د. شحاته محمد شحاته، د. كامل البشار وأخرون
217	نظم الإنذار المبكر والإستعداد والوقاية لمواجهة بعض الأزمات الاقتصادية والاجتماعية المختلفة	أكتوبر 2009	د. محرم الحداد	د. حسام مندورة، د. إجلال راتب وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
218	الشراكة بين الدولة والفاعلين الرئيسيين لتحفيز النمو والعدالة فى مصر	فبراير 2010	د.ايمان احمد الشربيني	د. عزة عمر الفندري، د. زينات محمد طلبة وأخرون
219	التغيرات الاقتصادية والاجتماعية والبيئية فى خريطة المحافظات وآثارها على التنمية	فبراير 2010	د. سيد محمد عبد المقصود	فريد أحمد عبد العال، د. خضر عبد العظيم أبو قورة وأخرون
220	بعض الاختلالات الهيكلية فى الاقتصاد المصري " من الجوانب القطاعية والنوعية والدولية"	مارس 2010	د. محمد عبد الشفيع عيسى	د. ممدوح فهمي الشرقاوي، د. لطف الله إمام صالح وأخرون
221	الإسقاطات السكانية وأهم المعالم الديموجرافية على مستوى المحافظات فى مصر 2012 – 2032	يولية 2010	د.مجدي عبد القادر	د. محمود إبراهيم فراج، د. منى توفيق
222	المواءمة المهنية لخريجى التعليم الفنى الصناعى فى مصر " دراسة ميدانية "	يوليه 2010	د.دسوقى عبد الجليل	د. زينات طبالة، د. إيمان الشربيني وأخرون
223	المشروعات القومية للتنمية الزراعية فى الأراضى الصحراوية	يوليه 2010	د. عبد القادر محمد دياب	د. ممدوح شرقاوي، د. هدي النمر وأخرون
224	نحو إصلاح نظم الحماية الاجتماعية فى مصر	سبتمبر 2010	د.خضر عبد العظيم ابو قوره	د. على عبد الرازق جلبى، د. زينات محمد طبالة وأخرون
225	متطلبات مواجهة الأخطار المحتملة على مصر نتيجة للتغير المناخى العالمي	أكتوبر 2010	د. محرم الحداد	د. حسام منذور، د. نفيسة أبو السعود وأخرون
226	آفاق النمو الاقتصادي فى مصر بعد الأزمة المالية والاقتصادية	يناير 2011	د.ابراهيم العيسوي	د. السيد دحية، د. سهير أبو العنين وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	العالمية			
227	نحو مزيج أمثل للطاقة فى مصر"	يناير 2011	د. نفين كمال	د. علـى نصـار، د. محمـود صالح وأخرون
228	مجتمـع المعرفـة وإدارة قطـاع المعلومات والإتصالات فى مصر	أغسطس 2011	د. محرم الحداد	د. سـيد دحيـة، د. حسـام مندور وأخرون
229	المدن الجديدة فـى إعـادة التوزيـع الجغرافى للسكان فى مصر	أغسطس 2011	د.مجدي عبد القادر	عزيـزة علـى عبـد الـرزاق، د. منـي عبـد العـال الـرزاق وأخرون
230	تحقيق التنمية المستدامة فى ظل إقتصاديات السوق من خلال إدارة الصادرات والواردات فى الفترة من عـام 2000 حتـى عـام 2011/2010	أكتوبر 2011	د.اجلال راتب	د. عبـد العزيـز إبـراهيم، د. محمـد عبـد الشـفيع عيسـي وأخرون
231	تجديد علم الاقتصاد نظرة نقدية إلـى الفكـر الاقتصـادى السـائد وعرض لبعض مقاربات تطوير	يونيه 2012	د.ابراهيم العيسوي	د. سهير أبو العينين
232	مقتضـيات واتجاهـات تطـوير إستراتيجية التنمية فى مصر فى ضوء الدروس المستفاده من الفكر الاقتصادى ومن تجارب الدول فى مواجهـة الأزمـة الاقتصـادية العالمية	يونيه 2012	د.ابراهيم العيسوي	د. السـيد دحيـة، د. نفـين كمال وأخرون
233	تطوير جودة البيانات فى مصر	مارس 2012	د.امـاني حلمـى الريس	د. علـى نصـار، د. زينـات طبالة وأخرون
234	ملامـح التغيـرات الاجتماعيـة المعاصـرة ومردوداتهـا علـى	يونيه 2012	د.وفـاء احمـد عبـد الله	د. خضـر عبـد العظـيم أبـو قـورة، د. لطـف الله إمـام

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	التنمية البشرية			صالح
235	السوق المحلية للقمح ومنتجاته	يونيه 2012	د. عبد القادر محمد دياب	د. ممدوح الشرقاوي، د. هدى النمر وأخرون
236	أثر تطبيق اللامركزية على تنمية المحافظات المصرية (بالتطبيق على قطاع التنمية المحلية)	يونيه 2012	د.فريد احمد عبد العال	د. سيد عبد المقصود، د. علا سليمان الحكيم وأخرون
237	إدارة الموارد الطبيعية فى ضوء استدامة البيئة والأهداف الإنمائية للألفية	يونيه 2012	د.نفيسه سيد ابو السعود	د. سحر البهائي، د. أحمد عبد الوهاب برانية وأخرون
238	رؤية مستقبلية للأدوار المتوقعة للجهات الممولة للمشروعات متناهية الصغر والصغيرة والمتوسطة فى مصر فى ظل التغيرات الراهنة	يونيه 2012	د. ايمان أحمد الشربينى	د. نجوان سعد الدين، د. محمد حسن توفيق
239	تطوير النظام القومى لإدارة الدولة بالمعلومات وتكنولوجياتها كركيزة أساسية لتنمية مصر	سبتمبر 2012	د. محرم الحداد	د. زلفي شلبي، د. سيد دياب وأخرون
240	(الرؤية المستقبلية للعلاقات الاقتصادية الخارجية ودوائر التعاون الاقتصادى المصري فى ضوء المستجدات العالمية والإقليمية والمحلية)	سبتمبر 2012	د.اجلال راتب	د. فادية عبد السلام، د. محمد عبد الشفيع وأخرون
241	المجتمع المدنى ومستقبل التنمية فى مصر	سبتمبر 2012	د.وفاء احمد عبد الله	
242	التغيرات الهيكلية للقوة العمل على مستوى المحافظات فى مصر	سبتمبر 2012	د.مجدي عبد القادر	د. زينات طبالة، د. عزت زيان وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	وآفاق المستقبل			
243	تطوير إستراتيجية التنمية الصناعية بمصر مع التركيز على قطاع الغزل	نوفمبر 2013	د. محرم الحداد	د. زلفي شلبي، د. محمد عبد الشفيع وأخرون
244	أثر المناطق الصناعية على تنمية المحافظات المصرية(بالتطبيق على محافظات إقليم قناة السويس)	نوفمبر 2013	د.فريد احمد عبد العال	د. سيد عبد المقصود، د. علا سليمان الحكيم وأخرون
245	نموذج رياضى احصائى للتنبؤ بالأحمال الكهربائية باستخدام الشبكات العصبية	نوفمبر 2013	د.محمد محمد ابو الفتوح الكفراوي	
246	دور الجمعيات الأهلية فى دعم التعليم الأساسى " دراسة ميدانية"	نوفمبر 2013	د.دسوقى عبد الجليل	د. خضر عبد العظيم أبو قورة، د. لطف الله إمام صالح وأخرون
247	" دور السياسات المالية فى تحقيق النمو والعدالة فى مصر" مع التركيز على الضرائب والاستثمار العام	نوفمبر 2013	د.سهير ابو العينين	د. نفين كمال، د. هبة الباز وأخرون
248	"بناء قواعد تصديرية صناعية للإقتصاد المصري"	نوفمبر 2013	د.اجلال راتب	د. فادية عبد السلام، د. محمد عبد الشفيع وأخرون
249	الصناعات التحويلية والتنمية المستدامة فى مصر	ديسمبر 2013	د. ممدوح فهمي الشرقاوى	د. نجوان سعد الدين، د. إيمان احمد الشربيني وأخرون
250	الصناديق والحسابات الخاصة"فلسفة الإنشاء – الأسباب – جدواها ومستقبلها"	ديسمبر 2013	د.ايمان احمد الشربيني	د. عزيزة عبد الرزاق، د. محمد حسن توفيق
251	الاقتصاد الأخضر ودورة فى	فبراير 2014	د. حسام الدين	د. محمد سمير مصطفى، د.

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	التنمية المستدامة		نجاتى	نفيسة أبو السعود وأخرون
252	إدارة الزراعة المصرية فى اطار التعيرات المحلية والدولية	فبراير 2014	د. عبد القادر محمد دياب	
253	تفعيل العلاقات الاقتصادية المصرية مع دول مجموعة البريكس	ديسمبر 2014	د.اجلال راتب	د. فادية عبد السلام ، د. مصطفى أحمد مصطفى وأخرون
254	التخطيط للتنمية المهنية للمعلمين فى مصر" معلم التعليم الأساسى نموذجا"	ديسمبر 2014	د.دسوقى عبد الجليل	د. خضر عبد العظيم أبو قورة، د. لطف الله إمام صالح وأخرون
255	استكشاف فرص النمو من خلال الخدمات اللوجستية بالتطبيق على الموانئ المصرية	ديسمبر 2014	د.منى عبد العال دسوقى	د. علي نصار، د. أحمد فرحات وأخرون
256	التغيرات الاقتصادية والاجتماعية في الريف المصري بعد ثورة يناير 2011	يناير 2015	د.حنان رجائي عبد اللطيف	د. سعد طه علام، د. عبد الفتاح حسين وأخرون
257	التدهور البيئى فى مصر منهج دليلى لتقدير تكاليف الضرر	ابريل 2015	د.محمد سمير مصطفى	د. أحمد عبد الوهاب برانية، د. نفيسة سيد أبو السعود وأخرون
258	بطاقة الأداء المتوازن كأداة لإعادة هندسة القطاع الحكومى فى مصر "دراسة حالة" " معهد التخطيط القومى"	مايو 2015	د.ايمان احمد الشربيني	
259	تقييم الأهداف الإنمائية لما بعد 2015 فى سياق توجهات التنمية فى مصر	يوليو 2015	د. هدى صالح النمر	د. علاء الدين محمود زهران، د. خالد عبد العزيز عطية وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
260	العلاقات الاقتصادية المصرية التركية بالتركيز على تقييم اتفاقية التجارة الحرة	أغسطس 2015	د. أجلال راتب	د. فادية عبد السلام ، د. سلوى محمد مرسي وأخرون
261	إطار لرؤية مستقبلية لاستخدام مصادر الطاقة الجديدة والمتجددة فى مصر	أكتوبر 2015	د. نفين كمال	د. سهير أبو العينين، د. نفيسة أبو السعود وأخرون
262	السوق المحلية للسلع الغذائية" جوانب القصور، والتطوير "	سبتمبر 2014	د. عبد القادر محمد دياب	د. هدى صالح النمر، د. أحمد عبد الوهاب برانية وأخرون
263	المرصد الحضرى لمدينة الأقصر محافظة الأقصر	ابريل 2016	د. سيد عبد المقصود	د. فريد أحمد عبد العال، د. محمود عبد العزيز عليوه وأخرون
264	الطاقة المتجددة بين نتائج وإبتكارات البحث العلمى والتطبيق الميدانى فى الريف المصري	إبريل 2016	د. عبد القادر محمد دياب	د. هدي صالح النمر، د. أحمد عبد الوهاب برانية وأخرون
265	نحو تحسين أوضاع الأمن الغذائى والزراعة المستدامة والحد من الجوع والفقر فى مصر – سبل وآليات تحقيق الثانى من أهداف التنمية المستدامة– (2016 – 2030)	يوليو 2016	أ.د. هدى صالح النمر	د. عبد العزيز إبراهيم، د. بركات أحمد الفرا وأخرون
266	التغيرات فى أسعار النفط وأثارها على الاقتصاد (العالمي والعربي والمصري)	يوليو 2016	د. حسن صالح	د. إجلال راتب، د. فادية عبد السلام وأخرون

سلسلة قضايا التخطيط والتنمية رقم (326)– معهد التخطيط القومي

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
267	مستقبل التنمية فى المنطقة الجنوبية لمحافظة البحر الاحمر (الشلاتين وحلايب)	يوليو 2016	أ.د. منى دسوقى	د. سيد عبد المقصود، د. فريد أحمد عبد العال وأخرون
268	نحو إطار متكامل لقياس ودراسة أثر أهداف التنمية المستدامة لما بعد 2015 على أوضاع التنمية المستدامة فى مصر خلال الفترة 2015/ 2030	يوليو 2016	د. ماجد خشبة	د. على نصار، د. هدى النمر وأخرون
269	متطلبات تطوير الحاسبات القومية فى مصر	يوليو 2016	د. سهير أبو العينين	د. عبد الفتاح حسين، د. أمل زكريا
270	آليات التنمية الإقليمية المتوازنة	أغسطس2016	د. فريد عبد العال	د. سيد محمد عبد المقصود، د. أحمد عبد العزيز البقلى وأخرون
271	تفاعلات المياه والمناخ والانسان فى مصر (اعادة التشكيل من أجل إقتصاد متواصل)	أغسطس2016	د سمير مصطفى	د. نفيسة سيد محمد أبو السعود، د. أحمد حسام الدين محمد نجاتي وأخرون
272	تفعيلإستراتيجية الذكاء الاقتصادى على المستوى المؤسسوالقومى فى مصر	أغسطس2016	د محرم الحداد	د. محمد عبد الشفيع عيسي، د. زلفي عبد الفتاح شلبي وأخرون
273	اشكالية المواطنة فى مصر – الحقوق والوجبات	أغسطس2016	د.دسوقى عبد الجليل	د. خضر عبد العظيم أبو قورة، د. لطف الله إمام صالح وأخرون
274	كفاءة الاستثمار العام فىمصر (المحددات والفرص وامكانيات التحسين)	سبتمبر 2016	د.أمل زكريا	د. هدى صالح النمر، د. هبة صالح مغيب وأخرون
275	الإجراءات الداعمة لاندماج	أكتوبر 2016	د.إيمان الشربينى	د. ممدوح الشرقاوى، د. زلفى

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	المشروعات الصغيرة والمتناهية الصغر غير الرسمية فى القطاع الرسمى فى مصر			شمبى وأخرون
276	الإدارة المتكاملة للمخلفات الصلبة ودورها فى دعم الاقتصاد القومى	يوليو2017	د. نفيسة أبو السعود	د. محمد سمير مصطفى، د. مها الشال وأخرون
277	متطلبات التحول لإقتصاد قائم على المعرفة فى مصر	يوليو2017	د.علاء زهران	د. محمد ماجد خشبة، د. خالد عبد العزيز عطية وأخرون
278	آليات وسبل اصلاح قطاعالأعمال العام فى جمهورية مصر العربية	يوليو2017	د. أحمد عاشور	د. أمل زكريا عامر ، د. سهير أبو العينين وأخرون
279	سبل وآليات تحقيق أنماط الاستهلاك المستدام فى مصر	أغسطس2017	د.هدى صالح النمر	د. علاء الدين زهران، د. خالد عبد العزيز عطية وأخرون
280	الخيارات الإستراتيجية لاصلاح منظومة التعليم ما قبل الجامعى فى مصر	أغسطس2017	ا.د. دسوقى عبد الجليل	د. خضر عبد العظيم أبو قورة، د. محرم صالح الحداد وأخرون
281	المسئولية المجتمعية للشركات ودورها فى تحقيق التنمية المحلية فى مصر	سبتمبر 2017	د.حنان رجائى عبد اللطيف	د. سعد طه علام، د. نجوان سعد الدين وأخرون
282	تنمية وترشيد استخدامات المياه فى مصر	سبتمبر 2017	د عبد القادر دياب	د. أحمد برانية، د. بركات الفرا وأخرون
283	اتفاقية منطقة التجارة الحرة الإفريقية وآثارها على الاقتصادات الافريقية عموما والاقتصاد	سبتمبر 2017	د محمد عبد الشفيع	د. اجلال راتب، د. فادية عبد السلام

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	المصري خصوصا			
284	دراسة مدى تطبيق الحوكمة على الإنتاج والإستهلاك المستدام للموارد الطبيعية فى مصر	أكتوبر 2017	د.حسام نجاتى	د. سحر البهائي، د. حنان رجائي وأخرون
285	صناعة الرخامفمصر "الواقع والمأمول" بالتطبيق على المنطقة الصناعية بشق الثعبان	ديسمبر 2017	د إيمان أحمد الشؤبينى	د. ممدوح الشرقاوى، د. محمد نصر فريد وأخرون
286	تطوير منظومة التعليم العالى فى مصر	ديسمبر 2017	د.محرم صالح الحداد	د. دسوقى عبد الجليل، د. محمد عبد الشفيع عيسى وأخرون
287	الطاقة المحتملة للصحارى المصرية بين تخمة الوادىوقحالة البيئة	ديسمبر 2017	د.محمد سمير مصطفى	د. عبد القادر دياب، د. أحمد عبد العزيز البقلي
288	نحو تحسين أنماط الانتاج المستدام بقطاع الزراعة فى مصر	يونيو 2018	د هدى صالح النمر	د. علاء الدين محمد زهران، د. خالد عبد العزيز عطية وأخرون
289	مبادرة الحزام والطريق وانعكساتها المستقبلية الاقتصادية والسياسية على مصر	يونيو 2018	د محمد ماجد خشبة	د. محمد على نصار، د. هبة جمال الدين وأخرون
290	دراسة تحليلية لموقع مصر فى التجارة البينية بين الدول العربية باستخدام تحليل الشبكات	يونيو 2018	د أمانى حلمى الريس	د. فادية محمد عبد السلام، د. حسن محمد ربيع حسن وأخرون
291	سعر الصرف وعلاقته بالاستثمارات الأجنبية فى مصر	يوليو 2018	د فادية عبد السلام	د. حجازى الجزار، د. محمود عبد الحى صلاح وأخرون
292	التغير الهيكلى لقطاع المعلومات فى مصر (بالتركيز على العمالة)	يوليو 2018	د محرم الحداد	د. اجلال راتب، د. محمد عبد الشفيع عيسى وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
293	التأمين وإدارة المخاطر فى الزراعة المصرية	يوليو 2018	د سمير عريقات	د. سعد طه علام، د. أحمد عبد الوهاب برانية وأخرون
294	اهمية المشكلات النفسية والاجتماعية لدى الشباب المصري 18-35 سنة – دراسة تطبيقية على محافظة القاهرة	أغسطس2018	د. دسوقى عبد الجليل	د. خضر عبد العظيم أبو قورة، د. لطف الله إمام صالح وأخرون
295	التعاون المصري الافريقى فى مجال استئجار الأراضى والتصنيع الغذائى	سبتمبر 2018	د. سمير مصطفى	د. نفيسة سيد أبو السعود، د. حمداوى بكري وأخرون
296	لا مركزية الإدارة البيئية فى مصر وسبل دعمها	سبتمبر 2018	د.نفيسة أبو السعود	د. محمد سمير مصطفي، د. سحر إبراهيم البهائي وأخرون
297	تقييم السياسات النقدية المصرية منذ عام 2003مع إهتمام خاص بدورها فى مساندة أهداف خطط التنمية	سبتمبر 2018	د.حجازى عبد الحميد الجزار	د. علي فتحي البجلاتي، د. أحمد عاشور وأخرون
298	الممارسات الاحتكارية فى أسواق السلع الغذائية الأساسية فى مصر	أسبتمبر 2018	د. عبد القادر دياب	د. أحمد عبد الوهاب برانية، د. هدى صالح النمر وأخرون
299	سياسات تنمية الصادرات فى مصر فى ضوء المستجدات الإقليمية والعالمية	أكتوبر 2018	د. نجلاء علام	د. محمد عبد الشفيع، د. مجدى خليفة وأخرون
300	تفعيل منظومة جودة التصدير فى المشروعات الصغيرة والمتوسطة فى مصر بالتطبيق على قطاع المنسوجات	ديسمبر 2018	د. إيمان الشربينى	د. زلفى شلبى، د. محمد حسن توفيق وأخرون
301	دور العناقيد الصناعيةفى تنمية	فبراير2019	د. محمد حسن	د. إيمان الشربيني، د. سمير

سلسلة قضايا التخطيط والتنمية رقم (326)- معهد التخطيط القومي

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
	القدرة التنافسية لصناعة الأثاث فى مصر – بالتطبيق على محافظة دمياط		توفيق	عريقات وأخرون
302	سياحة التراث الثقافى المستدامة مع التطبيق على القاهرة التاريخية	يونيو 2019	د. سلوى محمد مرسى	د. إجلال راتب العقيلى، د. زينب محمد نبيل الصادى وأخرون
303	تطور منهجية جداول المدخلات والمخرجات ومقتضيات تفعيل استخدامها فى مصر	يوليو 2019	د. حجازى عبد الحميد الجزار	د. سهير ابوالعيين ، د. أحمد ناصر وأخرون
304	مستقبل القطن المصري فى سياق إستراتيجية التنمية الزراعية فى مصر	يوليو 2019	د. سعد طه علام	د. سمير عبد الحميد عريقات، د. نجوان سعد الدين وأخرون
305	التغير الهيكلى لقطاع المعلومات فى مصر بالنركيز على الصادرات	أغسطس2019	د. محرم الحداد	
306	منافع وأعباء التمويل الخارجى فى مصر	أغسطس2019	د. فادية عبد السلام	د. محمود عبد الحى، د. محمد عبد الشفيع عيسى وأخرون
307	نحو منهجيه لقياس المؤشرات وتصور متكامل لنمذجة السيناريوهات البديلة لتحقيق أهداف أأمم المتحدة للتنمية المستدامة 2030 – حالة مصر	أغسطس2019	د عبد الحميد القصاص	د. أحمد سيمان، د. علا عاطف وأخرون
308	تطوير التعليم الأساسى فى مصر فى ضوء الاتجاهات التربوية الحديثة	سبتمبر 2019	د. دسوقى عبد الجليل	د. خضر عبد العظيم أبو قورة، د. لطف الله محمد طبالة وأخرون

م	عنوان السلسلة	التاريخ	الباحث الرئيسي	الباحثون المشاركون
309	النمو السكانى والتغيرات الاجتماعية والاقتصادية والعمرانية فى مصر خلال 2006-2017	سبتمبر 2019	د. عزت زيان	د. أحمد عبد العزيز البقلي، د. حامد هطل وأخرون
310	الزراعة التعاقدية كمدخل للتنمية الزراعية المستدامة فى مصر	أكتوبر 2019	د. هدى النمر	د. بركات أحمد الفرا، د. محمد ماجد خشبة وأخرون
311	فرص ومجالات التعاون الزراعي المصري الأفريقي وآليات تفعيله	مارس 2020	د. هدى النمر	د. أحمد عبد الوهاب برانيه د. بركات أحمد الفرا و أخرون
312	متطلبات تنمية القرية المصرية في إطار رؤية مصر 2030	مارس 2020	د. حنان رجائي عبد اللطيف	د. سعد طه علام د. سمير عبد الحميد عريقات واخرون
313	الاسرة المصرية وادوار جديده فى مجتمع يتغير (بالتركيز على منظومة القيم)	يونيو 2020	أ.د/ زينات محمد طبالة	أ.د/ دسوقى عبد الجليل أ.د/ عزة عمرالفندرى واخرون
314	الاستثمار في المشروعات البيئية في مصر وفرص تنميتها	يونيو 2020	أ.د. نفيسة سيد أبوالسعود	أ.د. خالد محمد فهمي د. منى سامي أبو طالب واخرون
315	"إستشراف الآثار المتوقعة لبعض التطورات التكنولوجية على التنمية في مصر وبدائل سياسات التعامل معها" (بالتطبيق على الذكاء الاصطناعي: AI – وسلسلة الكتل: Blockchain)	يونيو 2020	أ.د. محمد ماجد خشبة	أ.د. عبد الحميد القصاص –أ.د امانى الريس

Abstract

The Developmental and Strategic Dimensions of Cyber security and its Role in Supporting Digital and Crypto Economies - The Egyptian Experience Paths in the Light of Global Experiences.

This study aims to identify the mechanisms and means of developing cyber security to support Sustainable Development, the national digital and knowledge economy and national security.

The report (The Future of Knowledge: A Foresight Report) referred to the four technologies ruling in shaping the future as: Artificial Intelligence-AI, Blockchain, Cyber Security, and Biotechnology.

The World Economic Forum: WEF also indicated that the year 2020 is considered a turning point in the global interest in cyber security, especially in light of the increase in global Internet users (4.7 billion people in January 2021), the escalation of cyber-attacks, and the shift towards adopting the causes of the Fourth Industrial Revolution 4.0. In parallel with this global interest, this interest has escalated across the Arab world through multiple initiatives. Egypt realized early the importance of (cyber security), so it established the (EG-CERT) in 2009, then the (Supreme Council for Cyber security) in 2015, and the first national conference on cyber security in 2019. The Minister of Communications and Information Technology emphasized that the expansion of digitalization in society and the economy increased the risks and costs of cyber attacks.

Egypt ranked 23rd in the world on the Global Cyber security Index - GCI in the 2018 report, compared to 14th in the 2017 report. The draft update of the Sustainable Development Strategy: Egypt Vision 2030 referred to the link between (Information/ Cyber Security) and issues of transformation towards a digital economy, a knowledge-based economy and the development of digital infrastructure in Egypt.

The Planning Methods Center, on the initiative of the Department of Futures Studies, has prepared a study on Artificial Intelligence and Block chain in 2020, as well as addressing cyber security issues for the current academic year 2020/2021.

The research deals with cyber security issues in their various developmental dimensions, especially the interrelationships between cyber / digital security and the development of digital, encrypted and knowledge-based economy in Egypt, as well as in their contexts related to digital transformation in government sectors, national security contexts and cyber wars that are

considered among the most important threats to national security in the coming decades.

Keywords: Emerging Technologies, Cyber Threats, Cybersecurity, Digital Economies, and Crypto Economies.

Arab Republic of Egypt

Institute of National Planning

Planning and Development Issues Series

The Developmental and Strategic Dimensions of Cyber Security and its Role in Supporting Digital and Crypto Economies - The Egyptian Experience Paths in the Light of Global Experiences

No. (326) – August 2021