# إستراتيجيات تركيا في مجال الأمن السيبراني العالميّ: النظرية والتطبيق

نذير آق يشيلمَن*

*جامعة سلجوق ، تركيا .

ملخص: تتناول هذه الورقة مجموعة من قضايا الأمن السيبراني المترابطة. وتتوقف عند سؤال محوري: «هل إستراتيجية الأمن السيبراني التركي مصممة بشكل صحيح للتعامل مع البيئة الأمنية الجديدة في عالم الفضاء السيبراني الفوضوي؟». مرت إستراتيجية الأمن الوطني السيبراني في تركيا بالعديد من التغييرات منذ عام 2013، تمثل محاولات لمعالجة مشهد تطور الأمن السيبراني. وقد نجحت هذه الإستراتيجيات في بعض المجالات، مثل البنية القانونية وبناء القدرات والهيكل التنظيمي، لكنها كانت أقل نجاحًا من حيث التدابير الفنية. تطبق هذه المقالة نظام التحليل الكلي الذي يشمل كلًا من البحث الكمي والنوعي لتحليل إستراتيجيات الأمن السيبراني في تركيا من الناحية النظرية والتطبيقية. تشير نتائج هذا التحليل إلى أن تركيا لا تزال عرضة لهجوم سيبراني كبير محتمل.

**الكلمات المفتاحية**: التكنولوجيا، الهجوم السيبراني، الأمن السيبراني، تركيا.

# Türkiye's Global Cybersecurity Strategies: Theory and Practice

**NEZIR AKYEŞILMEN** *

ORCID NO : 0000-0001-8184-5280

**ABSTRACT**: *This paper addresses a set of interrelated cybersecurity issues; central among them is the question, "Is Türkiye's cybersecurity strategy properly devised to cope with the new security environment in the anarchic world of cyberspace?" Türkiye's national cybersecurity strategy has undergone several changes since 2013, each representing an attempt to address the evolving cybersecurity landscape. These strategies have been successful in some areas, such as Türkiye's legal, capacity-building, and organizational structure, but have been less successful in terms of technical measures. This article applies a macro-analysis framework that encompasses both quantitative and qualitative research to analyze Türkiye's cybersecurity strategies in theory and practice. The findings of this analysis suggest that Türkiye is still vulnerable to a possible major cyber-attack.*

*Selçuk University, Türkiye.

*Keywords*:*Technology, Cyber-attack, Cybersecurity, Türkiye.*

رؤيـــة تركيـــة
2022-(4/11)
75 - 108



DOI:10.36360/1560-011-004-005

## مدخل

أصبح عالمنا اليوم أكثر اعتمادًا على التقنيات السيبرانية، إذ يضم ما يزيد على خمسة مليارات شخص متصلين بالإنترنت، ويتم يوميًّا إنتاج أكثر من عشرة مليارات غيغابايت من المعلومات عبر الإنترنت[1]، وعدد الأجهزة النشطة المتصلة بالإنترنت مرشح للمزيد، والمتوقع أن يتجاوز 24 مليار بحلول عام 2030، والتحول الرقمي المتزايد السريع يتناول المعاملات التجارية والتجارة والتمويل والترفيه والاتصالات والسياسة والأمن والعديد من العمليات الأخرى.

حملت الرقمنة مزايا وراحة جديدة لحياتنا، لكنها أدت أيضًا إلى مخاطر وتهديدات جديدة. ففي كل يوم، يجري اختراق ما يزيد على 250 ألف صفحة ويب[2]. ووفقًا لتشك بوينت بوصفها مزود حلول الأمن السيبراني للحكومات والشركات الخاصة على مستوى العالم، يحدث في المتوسط 70 مليون هجوم إلكتروني كل يوم[3]. وقد وصل سوق الجرائم الإلكترونية إلى 6 تريليونات دولار في جميع أنحاء العالم في عام 2021[4]. التقنيات الجديدة مثل الحوسبة السحابية، وبلوكتشين، والبيانات الضخمة، وتكنولوجيا الهاتف المحمول، وإنترنت الأشياء (IoTs أو IoE)، والآن ميتافريس، تعمل جميعًا على زيادة اعتمادنا على المجال الرقمي، وتعقيد مشهد التهديدات السيبرانية. في مقال صدر مؤخرًا عن «الفوضى الإلكترونية»، قال جوزيف ناي: «شهد العالم هجمات إلكترونية منذ الثمانينيات، لكن سطح الهجوم اتسع بشكل كبير، فهو يشمل الآن كل شيء من أنظمة التحكم الصناعية إلى السيارات إلى المساعدين الرقميين الشخصيين»[5]. ومنذ ذلك الحين تشهد الحوادث الإلكترونية تزايدًا كبيرًا في السياسة الدولية، بدءًا من «دودة موريس» عام 1987، وهجمات فتى المافيا على الشركات عبر الوطنية في عام 2000، وهجمات الحرمان من الخدمات (DDoS) على إستونيا في عام 2007، وضربة ستوكسنت ضد المنشآت النووية الإيرانية في عام 2010، وكشف موقع ويكيليكس في عام 2011، والهجمات الروسية المزعومة التي تشير إلى التدخل في الانتخابات الرئاسية الأمريكية عام 2016.

إن مفاهيم، مثل الهجمات السيبرانية والجرائم الإلكترونية والصراعات الإلكترونية وحتى الحرب الإلكترونية- أصبحت جزءًا من محادثاتنا اليومية في السنوات الأخيرة، وحولت عالم الفضاء السيبراني إلى عالم شديد الفوضى، وأصبح مكانًا مهددًا بشكل متزايد. وكما يقول ناي: «ترسم القصص الأخبارية السيئة التي لا هوادة فيها صورة لعالم الإنترنت باعتباره عالمًا لا يخضع لأي حكم، ويزداد خطورة يومًا بعد يوم مع النتائج القاتمة، ليس على الفضاء الإلكتروني فحسب، بل كذلك على الاقتصادات والجغرافيا

السياسية والمجتمعات الديمقراطية والأسئلة الأساسية المتعلقة بالحرب والسلام»[6]. وقد أجبرت كل هذه العمليات المدمرة أصحاب المصلحة في الفضاء الإلكتروني، ولاسيّما الدول، على اتخاذ التدابير اللازمة لضمان الأمن السيبراني. وقد أصبح الأمن السيبراني في العقد الماضي أحد أهم القضايا على جداول أعمال الأمن الوطنية والدولية في جميع أنحاء العالم.

تعمل هذه الورقة على استكشاف الوثائق الإستراتيجية للأمن السيبراني الوطني في تركيا والسياسات والإستراتيجيات والتدابير والهياكل التنظيمية في هذا المجال، وتسعى للإجابة عن السؤال البحثي الأساسي، وهو: هل إستراتيجية الأمن السيبراني التركية مصممة بشكل صحيح للتعامل مع البيئة الأمنية الجديدة في عالم الفضاء الإلكتروني الفوضوي؟

في العقد الماضي، ركزت البحوث المتعلقة بإستراتيجيات الأمن السيبراني الوطنية في تركيا بشكل أساسي على القدرات العسكرية والهجومية للبلاد من خلال نهج أمني «سلبي»، أي التركيز على قدرة تركيا على ردع أو منع الهجمات الإلكترونية من خلال إنشاء الأمن السيبراني. تهدف هذه الورقة إلى تحليل إستراتيجية الأمن السيبراني الوطنية في تركيا من خلال نهج شامل لجميع السياسات والإستراتيجيات والتدابير والعمليات اللازمة من منظور قانوني وتقني وتنظيمي وبناء القدرات، الذي يركز على التعاون بين أصحاب المصلحة من فهم أمني إيجابي، لا يركز (على سبيل المثال) على هدف منع الحوادث الإلكترونية مجردًا عن الجهود المبذولة للحفاظ على الحريات في الفضاء السيبراني. الغرض من هذا البحث هو الكشف عن نقاط الضعف والقوة في الإستراتيجية الوطنية للأمن السيبراني في تركيا، وتطوير مقترحات السياسة والتوصيات لتحسينها.

## منهجية البحث وأسئلته

تطبق هذه الدراسة كلًّا من أساليب البحث الكمي والنوعي. وستعتمد في تحليلها ونتائج دراستها على المصادر الأولية والثانوية بما في ذلك وثائق إستراتيجية الأمن السيبراني الوطنية واللوائح القانونية والإدارية وأدبيات هذا المجال. سيجري تطبيق التحليل الكلي في تقييم الإستراتيجيات الوطنية للأمن السيبراني والسياسات التركية التي ستغطي ما يأتي:

(١) التوافق بين جميع الخطط والوثائق واللوائح والقوانين والتوجيهات الإستراتيجية الإلكترونية الوطنية.

(٢) قدرة تركيا على حماية الفضاء الإلكتروني والبنية التحتية الحيوية .

(٣) مؤلفات عن فعالية الإستراتيجيات السيبرانية الوطنية في الفضاء السيبراني .

(٤) إمكانيات التعاون في قضايا الأمن السيبراني .

(٥) السلطة المكرسة لمؤسسات الأمن السيبراني المختلفة .

(٦) مقترحات السياسة واللوائح القانونية .

جرى تصميم أسئلة البحث لتقييم ما إذا كانت إستراتيجية الأمن السيبراني وبنيته في تركيا تستجيب للتحديات والتهديدات الحالية . هل تمتلك تركيا الأدوات واللوائح والمعايير والسياسات الوطنية والدولية المناسبة الكافية لمواجهة التهديدات الإلكترونية الحالية؟ كيف يمكن أن تتحول الأنظمة والسياسات والمؤسسات الأمنية الحالية في تركيا إلى ضمان الأمن السيبراني؟

## النظر في الأدبيات

كان ينبغي أن نبدأ بالتحديات التي تطرحها ندرة الأدبيات المتوفرة حول هذا الموضوع لو كانت هذه الورقة قد كُتِبَت قبل 10 سنوات . الميزة الرئيسة التي يتمتع بها تحليل أسئلة البحث المقترحة اليوم ، لا تكمن في وفرة المعلومات فحسب ، بل كذلك توفر الغالبية العظمى من الأدبيات ذات الصلة المتاحة عبر الإنترنت ، ويمكن الوصول إليها بسهولة من خلال الوسائط الرقمية والمجلات الأكاديمية وصفحات الويب الخاصة بالشركات والحكومات . فالتحدي اليوم لا يكمن في ندرة الأدبيات ، ولكن في تحديد ما هو موثوق في الأدبيات الكثيرة المتوفرة[7] . وفي هذا المجال ، يمكن تصنيف البحث المتاح حول الموضوع المطروح إلى ثلاثة أقسام : تعريف الأمن السيبراني ، وتطور الأمن السيبراني في العلاقات الدولية (IR) ، وبنية هيكل الأمن السيبراني وإستراتيجياته في تركيا . ويجري توفير استكشاف هذه المجالات في الأدبيات أدناه لوضع سياق عمل الدراسة الحالية .

## الأمن السيبراني: المفهوم الأكثر إثارة للجدل للفضاء السيبراني

الفضاء السيبراني ، أي الفضاء الذي يجري فيه تفعيل الأمن السيبراني ، هو بحد ذاته مصطلح متنازع عليه ، وليس له تعريف مقبول على نطاق واسع في الأدبيات المعاصرة لهذا المجال . وقد جرى تطوير مناهج مختلفة من قبل عدد كبير من الخبراء والمؤسسات والتخصصات لفهم هذا المصطلح وضبطه ، باعتباره يشير إلى مجال عالمي واسع معقد

للغاية. وجرى تقديم مفهوم الفضاء الإلكتروني لأول مرة من قبل ويليام جيبسون في روايته الخيالية الشهيرة نيورومانسر في عام 1984. يصف جيبسون الفضاء الإلكتروني بأنه شبكة عالمية معقدة من أجهزة الكمبيوتر، جرى إنشاؤها ومشاركتها من قبل مليارات المستخدمين من جميع أنحاء العالم[8]. منذ ذلك الحين، جرى اقتراح العديد من التعريفات التي توسع مفهوم جيبسون الأولي. تزعم إحدى الدراسات أنها وجدت 28 تعريفًا مختلفًا للفضاء السيبراني في العقد الماضي. يعطي كل تعريف أولوية لبعد من أبعاد الفضاء السيبراني، مثل الأجهزة، والبرمجيات، والبروتوكولات، والشبكات، والمعلومات، والمستخدم، والترابط، والإنترنت، وما إلى ذلك. تقدم كل دراسة تعريفًا عمليًّا يخدم أو ينفذ مصالح مطورها. يقف كرامر أمام هذا العدد الكبير من التعريفات، ويدعو إلى أنه «يجب استخدام التعريفات بوصفها وسيلة مساعدة للسياسة والتحليل، لا بوصفها قيدًا لها»[9]. يتجاوز نطاق هذه الورقة تحليل جميع التعريفات التي جرى تطويرها في دراسات أخرى، وتناولها بالتفصيل. وتعمد بدلًا من ذلك، إلى بيان أكثرها فائدة، لاعتمادها، والانتقال إلى مناقشات الأمن السيبراني.

> **"يُعَدّ الفضاء السيبراني خطابًا ديناميكيًا يجسد أو يعيد تجسيد الواقع الاجتماعي من خلال إعطاء معنى للهياكل والعمليات الاجتماعية للمستخدمين"**

## تعريف الفضاء السيبراني: هل هو فضاء؟

ما الذي يطرحه مفهوم الفضاء الإلكتروني أولًا في ذهنك؟ هل الفضاء السيبراني مكان أو منطقة أو فضاء؟ هل يمكن تصميمه أو تقديم خريطته أو تمثيله ماديًّا؟ هل يمكن تحديد ذلك؟ «بالنسبة لبعض الجغرافيين، يُعَدّ الفضاء السيبراني خطابًا ديناميكيًّا يجسد أو يعيد تجسيد الواقع الاجتماعي من خلال إعطاء معنى للهياكل والعمليات الاجتماعية وهويات للمستخدمين، على الرغم من عدم وجود حدود ملموسة»[10]. ينظر الكثير من الناس إلى الفضاء السيبراني على أنه مجال افتراضي، وهذا ليس خطأً محضًا. فالفضاء السيبراني إلى جانب بُعده الافتراضي، يتطلب بنية تحتية مادية (شبكة مادية عالمية تتكون من أجهزة كمبيوتر، وأسلاك، وأقمار صناعية، وخوادم، ومودم... إلخ) وكلها تجعل الشبكة الافتراضية ممكنة، وكلها موجودة بالضرورة في مكان ما على الأرض. وهذه البنية المعقدة تدعم البروتوكولات التي يقبلها المستخدمون وتحددها باعتبارها مكونات لهذا العالم. يلاحظ إيريك شميدت، الرئيس التنفيذي لشركة غوغل، مدى تعقيد عالم الإنترنت بادعائه بأن «الإنترنت هو أول شيء بنته البشرية ولم تفهمه، وهي أكبر تجربة شهدناها على الإطلاق في الفوضى»[11]. حاول العديد من الخبراء والمؤسسات البارزة اكتشاف خريطة للأبعاد المختلفة للعالم السيبراني ورسمها، وجعلَ ذلك مفهومًا للجميع بمستويات متفاوتة من النجاح.

يقدم كوهلر تعريفًا يشمل الأجهزة والبرامج وطبقات المعلومات. ويعدّ الفضاء السيبراني «مجالًا عالميًّا داخل بيئة المعلومات يجري تأطير طابعه المميز والفريد، من خلال استخدام الإلكترونيات والطيف الكهرومغناطيسي لإنشاء المعلومات وتخزينها وتعديلها وتبادلها واستغلالها عبر الاعتماد المتبادل والشبكات المترابطة باستخدام المعلومات وتكنولوجيات الاتصال»[12]. وضعت وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA، المعروفة سابقًا باسم وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات)، تعريفًا مشابهًا للفضاء السيبراني ولكنه أقصر: «الفضاء السيبراني هو مجموعة الأصول الملموسة وغير الملموسة التي تعتمد على الوقت، وتخزن و/أو تنقل المعلومات الإلكترونية»[13]. بالنسبة لحلف الناتو، «يعد الفضاء السيبراني أكبر من الإنترنت، فلا يتضمن الأجهزة والبرامج وأنظمة المعلومات فحسب، بل يتضمن كذلك الأشخاص والتفاعل الاجتماعي داخل هذه الشبكات»[14].

أدخلت تركيا ثلاثة تعريفات مختلفة، لكنها مترابطة بشكل وثيق، للفضاء السيبراني في وثائق إستراتيجية الأمن السيبراني الوطنية التي نُشِرت في السنوات العشر الماضية. تحدّد وثيقة الإستراتيجية الوطنية للأمن السيبراني (NCSD) في تركيا وخطة العمل (2013–2016) الفضاء السيبراني على أنه «البيئة التي تتكون من أنظمة المعلومات التي تمتد عبر العالم بما في ذلك الشبكات التي تربط هذه الأنظمة»[15]. تضيف وثيقة NCSD لخطة عام (2016–2019) بعض العناصر الجديدة، واصفًا المجال على أنه «البيئة الرقمية المكونة من أنظمة المعلومات المنتشرة في جميع أنحاء العالم والفضاء، والشبكات التي تربط هذه الأنظمة أو أنظمة المعلومات المستقلة»[16]. وتُعرِّف وثيقة NCSD لخطة العمل (2020–2023) الفضاء السيبراني على أنه «الأنظمة والخدمات المتصلة، إما بشكل مباشر أو غير مباشر بالإنترنت، والاتصالات السلكية واللاسلكية وشبكات الكمبيوتر»[17]. يبدو أن التعريف الوارد في الخطة الإستراتيجية (2016–2019) هو الأكثر شمولًا ودقة مقارنة بالتعريفات الأخرى. وإذا أخذنا بعين الاعتبار أن التكنولوجيا الإلكترونية تتطور وتتغير باستمرار، فمن الطبيعي أن تتغير عناصر التعريفات بمرور الوقت.

يُعَدّ الفضاء السيبراني شديد التعقيد والترابط عالميًّا- مجالًا متعدد الأبعاد، فيه طبقات عديدة، وميزات فريدة، تحدث فيها عمليات أكثر تعقيدًا من أي وقت مضى، وعمليات داخل النظام البيئي السيبراني. لفهم الأمن السيبراني بشكل كامل، يجب تقييم كل خاصية للفضاء السيبراني. بادئ ذي بدء، يُعَدّ الفضاء السيبراني على عكس الفضاء المادي، مجالًا افتراضيًّا. علاوة على ذلك، فإن البشر هم فاعلون نشطون داخل الفضاء السيبراني وفيه، فيسهمون في توسيع الفضاء السيبراني في كل لحظة. يشير أوساف إلى أن «الفضاء

السيبراني هو من صنع الإنسان، وهو في قيد الإنشاء باستمرار. إنه يتغير من لحظة إلى أخرى»[18].

الميزة الأساسية الثانية للفضاء السيبراني هي بنيته الفوضوية. فهو فضاء لامركزي متعدد المراكز. وهذه الفوضوية ليست بمعنى العلاقات الدولية المادية فحسب، بل تعني أيضًا غياب المؤسسات الحاكمة مثل القانون الدولي والمنظمات الدولية والدبلوماسية والقوى العظمى... إلخ. ولهذا السبب، تصف نازلي شكري المجال السيبراني بأنه فوضوي مفرط، والميزات السيبرانية عند غياب السيطرة السيادية أو أي سلطة مركزية تفتح الطريق لعالم من الصراع والعنف الشديد في جميع أنحاء العالم. ونشير إلى هذه الميزة بوصفها واحدة من الفوضى السيبرانية[19]. بعبارة أخرى، «الفضاء الإلكتروني يخلو من أنظمة الحوكمة، ولا توجد فيه قواعد أو ممارسات تنظيمية، ولا توجد فيه آليات لتتبع الأضرار، ويخلو من أدنى الحوافز للقيام بذلك»[20]. ومن السمات المميزة الأخرى للفضاء السيبراني هيمنة الجهات الفاعلة الخاصة كما تشير شكري: «نظام الدولة ضعيف، والقطاع الخاص (الربحي، غير الربحي، القانوني، وغير القانوني) هو المسيطر»[21]. ويشرح ناي

بإيجاز معظم هذه الخصائص بقوله : «يتمتع المجال السيبراني الجديد من بين الخصائص الكثيرة ؛ بتآكل المسافة (المحيطات لم تعد توفر الحماية) ، وسرعة التفاعل (أسرع بكثير من الصواريخ في الفضاء) ، والتكلفة المنخفضة (التي تقلل من الحواجز أمام الدخول) ، وصعوبة الإسناد (مما يعزز الإنكار ويبطئ الردود)»[22] . وعلى هذا النحو ، يجري قبول الفضاء السيبراني على نطاق واسع بوصفه المجال التشغيلي الخامس[23]» ، إلى جانب المجالات الأربعة التقليدية المتمثلة بالأرض والبحر والجو والفضاء»[24] .

## الأمن السيبراني: أمنُ مَن؟

في فيلم وثائقي جرى بثه على قناة أنيمال بلانيت ، قال المقدم تعليقًا على النظرة القلقة لفهد ينتظر مع جرائه الصغار على بعد 30 مترًا من أسد : «لا يوجد طفل بأمان في السافانا ، ولا يمكن لأحد هنا أن يتكهن هنا من نيات جاره الحقيقية» . الشيء نفسه ينطبق بالفعل على الفضاء السيبراني ؛ لأنه ألغى المسافات ، وجعل الجميع جيرانًا للجميع . لذلك ، بالإشارة إلى الفيلم الوثائقي ، «لا يوجد مستخدم آمن في الفضاء الإلكتروني ؛ لأنه في هذا المجال ، لا أحد يعرف حتى من هو جاره ، ناهيك عن نية جاره»[25] .

يبين الاقتباس أعلاه بشكلٍ مثاليٍّ مدى ضعف الوضع الأمني في الفضاء السيبراني . التهديدات موجودة دائمًا ، وهي حقيقية ووشيكة . لذلك ، يحذر كلود شانون قائلًا : «افترض أن العدو يعرف النظام ، ويعامل كل مضيف وخادم واتصال على أنه يحتمل أن يكون معاديًا»[26] . يُعرَف هذا النهج باسم «عدم الثقة» في مجتمع الأمن السيبراني[27] .

جرى تطوير تعريفات مختلفة للأمن السيبراني عبر وثائق إستراتيجية وطنية مختلفة للأمن السيبراني ، من قبل العديد من المنظمات الدولية والخبراء . الفضاء السيبراني والمصطلحات المرتبطة به ، مثل الأمن السيبراني ، وأخلاقيات الإنترنت ، والسياسة السيبرانية ، والصراع السيبراني ، والحرب السيبراني أو الإلكتروني ، وهي مفاهيم مثيرة للجدل وغير مؤكدة وغامضة . الأمن السيبراني هو مصطلح أكثر تعقيدًا من مصطلح الفضاء السيبراني ، ويصعب تحديده بالمثل . فهو في الواقع ، يعني أشياء مختلفة تبعًا للجهات الفاعلة المعنية ، بما في ذلك الدول والمنظمات الدولية والشركات الخاصة وحتى المستخدمين . يرى كريجن وآخرون أنّ :

«الأمن السيبراني هو مصطلح مستخدم على نطاق واسع ، تعريفاته شديدة التغير ، وذاتيةٌ في الغالب ، وغير مفيدةٍ في بعض الأحيان . . . إن عدم وجود تعريف موجز ومقبول على نطاق واسع يجسد الأبعاد المتعددة للأمن السيبراني التي تعوّق التقدم التكنولوجي

والعلمي من خلال تعزيز وجهة النظر التقنية السائدة للأمن السيبراني مع فصل التخصصات التي يجب أن تعمل بشكل متضافر لحل تحديات الأمن السيبراني المعقدة»[28] .

طوّر الاتحاد الدولي للاتصالات (ITU) من أجل الاستخدام العملي، تعريفًا شاملًا وواضحًا للأمن السيبراني يشمل تقريبًا كل جانب من جوانب الأمن السيبراني : «الأمن السيبراني هو مجموعة من الأدوات والسياسات ومفاهيم الأمان والضمانات الأمنية والمبادئ التوجيهية وإدارة المخاطر والأساليب والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية والمنظمة وأصول المستخدم»[29] . يُعَدّ تعريف الاتحاد الدولي للاتصالات أحد أكثر التعريفات شيوعًا في الأدبيات . يصف الاتحاد الدولي للاتصالات أيضًا الأصول التي يحميها الأمن السيبراني بالضبط :

«تتضمن المؤسسة وأصول المستخدم أجهزة الحوسبة المتصلة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المرسلة و / أو المخزنة في البيئة الإلكترونية . يسعى الأمن السيبراني جاهدًا لضمان تحقيق وصيانة الخصائص الأمنية للمؤسسة وأصول المستخدم ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية»[30] .

تستخدم تركيا في كل من الوثائق الإستراتيجية الوطنية للأمن السيبراني NCSD الثلاث تعريفًا مشابهًا وواسع النطاق للأمن السيبراني : «حماية أنظمة المعلومات التي تشكل الفضاء السيبراني من الهجمات، وضمان السرية والنزاهة وتوافر المعلومات/ البيانات التي تجري معالجتها في هذه البيئة، واكتشاف الهجمات وحوادث الأمن السيبراني، وتفعيل آليات الاستجابة المضادة، واستعادة الأنظمة للظروف السابقة لحادث الأمن السيبراني»[31] .

لا يركز التعريف المستند إلى الوثائق الإستراتيجية الوطنية للأمن السيبراني NCSD الثلاث هذا فقط على حماية الأنظمة من الحوادث السيبرانية . كما أنه يشدد على الأهداف الرئيسة الثلاثة للأمن السيبراني، والمعروفة باسم ثلاثية الخصوصية والنزاهة والتوافر (CIA) : «التوافر والنزاهة، وقد تشمل المصداقية وعدم التنصل والسرية»[32] .

التعريف الذي اقترحه مايكل فيل وإيان براون مشابه جدًّا للتعريف التركي، مع التركيز على حماية أنظمة المعلومات والإجراءات المضادة ضد الهجمات الإلكترونية :

«يغطي الأمن السيبراني مجموعة واسعة من القضايا التقنية والتنظيمية والحوكمة التي

يجب مراعاتها لحماية أنظمة المعلومات الشبكية من التهديدات العرضية والمتعمدة . إنه يتجاوز تفصيلات التشفير وجدران الحماية وبرامج مكافحة الفيروسات وأدوات الأمان التقنية المماثلة»[33] .

يشير فيل وبراون عن حق إلى أن «فهم الأمن السيبراني هو هدف متحرك ، تمامًا مثل فهم الحوسبة والمجتمع . ما الذي يجري تهديده بالضبط؟ وكيف؟ ومن يقوم به؟ كل ذلك في حالة تغير مستمر»[34] . لذلك ، تتغير التعريفات من شخص إلى آخر ، ومن دراسة إلى أخرى ، ومن وقت إلى آخر .

على الرغم من التغييرات التي تجري على التعريفات والأساليب المختلفة التي طورتها جهات فاعلة مختلفة في الفضاء الإلكتروني ، فإن جميع التعريفات تشمل عناصر مكافحة الإجراءات الضارة ، ومنع الهجمات الإلكترونية ، وتمكين استعادة النظام . تتوافق هذه التعريفات بشكل عام مع فهم أمني سلبي . هناك مراجع نادرة للحرية وحقوق الإنسان في تعريفات و/ أو إستراتيجيات الأمن السيبراني .

## ظهور الأمن السيبراني في العلاقات الدولية

يركز تطور الأمن السيبراني في العلاقات الدولية على الهجمات السيبرانية والصراعات السيبرانية الرئيسة التي شكلت ظهور الأمن السيبراني على المستويين الوطني والدولي[35] . جرى تطوير الفضاء السيبراني لمشاركة المعلومات ، وكانت الشفافية هي السمة الأساسية له ، لما يقرب من 20 عامًا ، من عام 1969 إلى عام 1988 ، عندما جرى إنشاء برنامج دودة موريس بوصفه أول برنامج ضار ، وجرى إطلاقه على الشبكة[36] . بعبارة أخرى ، كان أول عقدين من الإنترنت خاليًا من البرامج الضارة ، ومن ثَمّ كان يُعَدّ مجانيًّا وآمنًا . بدأت فكرة الأمن السيبراني نفسها لأول مرة مع دودة موريس . وعلى الرغم من أن الفضاء السيبراني ، وهو نتاج الحرب الباردة ، قد جرى إنشاؤه في المقام الأول للإسهام في الأمن المادي ، فإنه بمرور الوقت أصبح مصدر قلق أمني جديد : الأمن السيبراني[37] .

في الفضاء الإلكتروني ، تكون الجريمة دائمًا متقدمة على الدفاع : «الهجوم له اليد العليا . جرى تصميم الإنترنت بحيث يكون تعاونيًّا وقابلًا للتوسع بسرعة ولديه حواجز منخفضة أمام الابتكار التكنولوجي ، وكانت إدارة الأمن والهوية من الأولويات الدنيا »[38] . إلى جانب الحاجة المتزايدة للأمن السيبراني ، تطورت آلياته تدريجيًّا من المستوى الفردي إلى المستوى الوطني والعالمي من أواخر الثمانينيات حتى الوقت الحاضر . وشكلت العديد من الهجمات السيبرانية والنزاعات السيبرانية الرئيسة ، هذه العملية في العلاقات


الدولية .

## من دودة موريس إلى فتلى المافيا (1988 إلى 2000)

حدثت نقطة تحول في تاريخ الأمن السيبراني في 2 نوفمبر 1988 . أعلن أكاديميون في جامعات أمريكية رائدة أن جميع أجهزة الكمبيوتر الخاصة بهم إما تباطأت أو توقفت عن العمل ، وأنهم واجهوا صعوبة في الوصول إلى المعلومات . ويسود الاعتقاد بأن أكثر من 10 بالمئة من أجهزة الكمبيوتر في الولايات المتحدة (حوالي 6–60) ألفًا فقدت وظائفها[39] . وقد جرت تسمية البرامج الضارة المهاجمة نسبة لمطورها ، روبرت تابان موريس[40] ، أحد طلاب الدراسات العليا في جامعة كورنيل .

كانت لدودة موريس[41] بوصفها الأوى من نوعها ، تأثير عميق في أمن الكمبيوتر والإنترنت . في أعقاب ذلك ، جرى إنشاء العديد من فرق الاستجابة للطوارئ الحاسوبية ، وبدأ الناس في توخّي مزيد من الحذر والتفكير بشأن الأمن في الفضاء السيبراني . «حتى إن بعض الأشخاص يصفون الحادثة بأنها الانفجار الكبير للأمن السيبراني»[42] . كانت الدودة بمثابة مكالمة إيقاظ بخصوص أمان الكمبيوتر والإنترنت للمسؤولين والمهنيين والمستخدمين[43] . «بعد فترة وجيزة من حادثة دودة موريس ، قدمت وكالة مشروعات

البحوث الدفاعية المتقدمة الأمريكية DARPA التمويل لفريق الاستجابة للطوارئ الحاسوبية CERT، الذي كان منذ ذلك الحين بمثابة غرفة تبادل لمعلومات الثغرات الأمنية. على الرغم من أن فريق CERT لا يوفر العلاج الشافي، فقد أصبح مصدرًا موثوقًا للمعلومات حول الثغرات الأمنية والإصلاحات لمجموعة متنوعة من البرامج»[44].

أدّت دودة موريس إلى ظهور الأمن السيبراني على المستوى الفردي في التسعينيات، وشكلت مفهوم الأمن بوصفه ضرورة في الفضاء السيبراني. ومن هنا، أصبح الأمن السيبراني يُنظَر إليه على نطاق أوسع من حيث كمبيوتر الشخص وأمن الإنترنت في ذلك الوقت، وكان يقتصر على حماية البيانات والمعلومات الشخصية، أو على الأكثر حماية المجتمعات الصغيرة حول العالم. في غضون وقت قصير من ظهور دودة موريس، جرى تطوير عدد كبير من الفيروسات (الديدان) والبرامج الضارة الأخرى من أنواع مختلفة وذات تأثيرات مختلفة. وهكذا، نتيجة لهجمات رفض خدمات الموزع DDoS على بعض الشركات العالمية من قبل فتى المافيا Mafia Boy البالغ من العمر 15 عامًا، تغير مشهد الأمن السيبراني بشكل كبير مع بداية القرن الحادي والعشرين.

## من الفردية إلى المؤسسية: الأمن السيبراني في مطالع الألفية الثالثة

كان مايكل كالشي (فتى المافيا) يبلغ من العمر 15 عامًا فقط عندما تمكن من إغلاق العديد من المواقع الإلكترونية الكبرى لشركات عالمية، بما في ذلك Dell وAmazon وYahoo وCNN وE-Tarde وBuy.com وeBay، في سلسلة من هجمات الحرمان من الخدمة (DoS) في عام 2000[45]. «في ذلك الوقت، كانت Yahoo أكبر محرك بحث في العالم»[46]. يقدر المبلغ المالي للضرر الناجم عن هجوم فتى المافيا بحوالي مليار إلى ثلاثة مليارات دولار[47]. حوّل هذا الهجوم مسار الأمن السيبراني من المستوى الفردي إلى المستوى المؤسسي والتنظيمي والشبكي. بدأت الشركات الخاصة في توخي مزيد من الحذر بشأن أمن أصولها في المجال السيبراني. ساعدت تفصيلات الحادثة ونشرها على نطاق واسع في وسائل الإعلام على نشر الخوف من فكرة الأمن السيبراني في جميع أنحاء العالم. واستمر هذا الاتجاه طوال العقد الأول من القرن الحادي والعشرين. ومرة أخرى، تولت الجريمة المسؤولية عن هجمات رفض خدمات الموزع DDoS على إستونيا (2007) وستوكس نت Stuxnet على المنشأة النووية الإيرانية (2010) إلى تغيير مشهد وتصور الأمن السيبراني تمامًا.

منذ هجمات رفض خدمة الموزع DDoS ضد إستونيا في عام 2007، سيطرت «إسرائيل»

على نظام الرادار السوري (2007 و2011)، واستخدمت روسيا الهجمات السيبرانية جنبًا إلى جنب مع الهجمات المادية في جورجيا في عام 2008 (المعروفة الآن باسم الحرب الهجينة)، وأخيرًا، في عام 2010، جرى نشر ستوكس نت (أي دودة الكمبيوتر الخبيثة التي حصل قبولها كأول سلاح إلكتروني) ضد المنشآت النووية الإيرانية، وبدأت الدول تنظر إلى الأمن السيبراني على أنه مشكلة تتعلق بالأمن القومي. وقضية ويكيليكس (2011)، وقضية سنودن (2013)، والتدخل الروسي في الانتخابات الرئاسية الأمريكية عام 2016 وغيرها من الحوادث المهمّة دفعت صانعي السياسة إلى اعتبار الفضاء الإلكتروني عالمًا للنزاع والأمن والحرب. في عام 2009، أعلن الرئيس باراك أوباما آنذاك عن إستراتيجية أمريكية جديدة للتصدي للتهديد الذي يشكله الفضاء السيبراني، وقال: «من الواضح الآن أن هذا التهديد السيبراني هو أحد أخطر التحديات الاقتصادية والأمن القومي التي نواجهها بوصفنا أمة»[48]. كما حذر قادة آخرون المجتمع من التهديدات السيبرانية المستمرة. وادعى مايك مولين، رئيس هيئة الأركان المشتركة في عام 2011، «أن أكبر تهديد وجودي موجود، على ما أعتقد، هو الإنترنت.» في العام التالي، أشار مارتن ديمبسي إلى أن «الهجوم السيبراني يمكن أن يوقف مجتمعنا في مساره». وحذر وزير الدفاع السابق ليون بانيتا بشدة في عام 2012 من «بيرل هاربور الرقمي» الوشيك[49]، وأعلن في عام 2013 أن الإنترنت «بلا شك، ساحة معركة المستقبل»[50]. وبدأت الدول في إدراك أن المجال السيبراني حيوي للأمن الوطني والدولي، ولتطوير أدوات وسياسات حماية الأمة وأصولها من التهديدات السيبرانية.

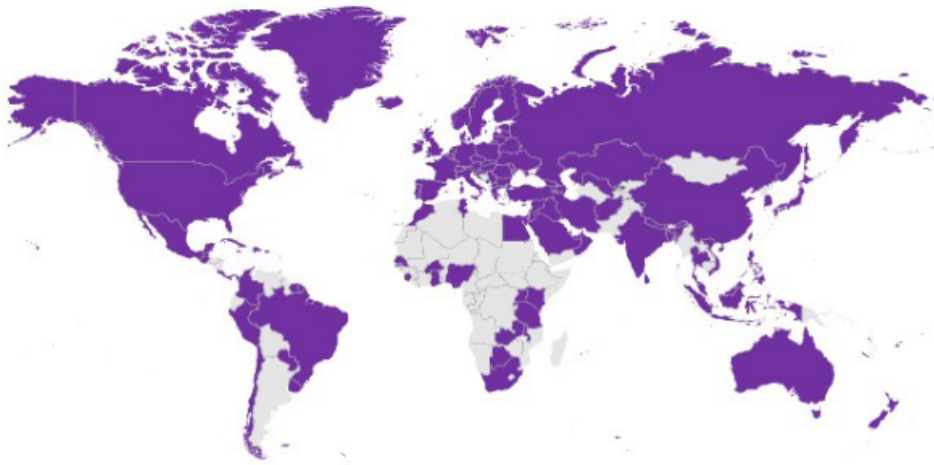
## تطوير الإستراتيجيات الوطنية للأمن السيبراني:

بعد هجمات رفض خدمة الموزع DDoS عام 2007 على إستونيا وهجمات ستوكس نت Stuxnet في عام 2010، ظهرت جهود جادة لإنشاء تدابير الأمن السيبراني الوطني والدولي. بدأت المنظمات الدولية مثل الاتحاد الدولي للاتصالات وحلف الناتو ومنظمة التعاون والتنمية في الميدان الاقتصادي ووكالة الاتحاد الأوروبي للأمن السيبراني ENISA في تطوير برامج وأدلة للأمن السيبراني؛ لمساعدة أعضائها على ضمان الأمن السيبراني. وقد بيّن الاتحاد الدولي للاتصالات أن الهدف من برنامجه للأمن السيبراني هو جعل الفضاء السيبراني أكثر أمانًا للجميع، فيوفر لأعضائه «فرصة وأدوات لزيادة قدرات الأمن السيبراني على المستوى الوطني، من أجل تعزيز الأمن والمرونة، وبناء الثقة في استخدام تكنولوجيا المعلومات والاتصالات، وهو ما يجعل العالم الرقمي أكثر أمانًا للجميع»[51]. وقد بدأت الدول في تطوير الإستراتيجيات الوطنية للأمن السيبراني (NCSS)، وهي مجموعة من السياسات والأدوات والتطبيقات التي تطبقها الحكومات لجعل الفضاء السيبراني الوطني أكثر حرية وأمانًا. ووفقًا للاتحاد الدولي للاتصالات،

يحدد NCSS «إطارًا لتنظيم أولويات الجهود وترتيبها لإدارة المخاطر التي يتعرض لها الفضاء السيبراني أو البنية التحتية للمعلومات الحيوية»[52]. ويرسم الناتو إطار عمل أكثر شمولًا حيث «يجب أن تمكّن الإستراتيجية الوطنية للأمن السيبراني الكيانات الحكومية من تحديد الأهداف الإستراتيجية، وترجمة هذه الرؤية إلى سياسات متماسكة وقابلة للتنفيذ، وتحديد الموارد اللازمة لتحقيق هذه الأهداف وتقديم إرشادات لاستخدام هذه الموارد وتمييز كيفية ارتباط الإستراتيجيات الوطنية NCSS بإستراتيجيات أخرى ذات صلة»[53].

بدأت معظم الحكومات في تطوير وثائق إستراتيجياتها NCSS الخاصة بها على مدار العقد الماضي. وعدد قليل من البلدان اليوم ليس لديها إستراتيجياتها الخاصة في هذا المجال. يوضح (الشكل1) انتشار NCSSs في جميع أنحاء العالم.

الشكل 1 : الخريطة العالمية للبلدان التي تعتمد إستراتيجيات وطنية للأمن السيبراني



المصدر : «المستودع الوطني لإستراتيجيات الأمن السيبراني»، الاتحاد الدولي للاتصالات (ITU)[54]

طوّرت تركيا أولى وثيقة لإستراتيجيتها للأمن السيبراني NCSS في عام 2013، وأنتجت ثلاث وثائق حتى الآن[55]. تغطي وثيقة NCSS المعمول بها حاليًّا السنوات (2020–2023). والقسم الآتي يحلّل هذه الوثائق.

## الأمن السيبراني العالمي وتوقعات الطاقة السيبرانية: أين تقف تركيا؟

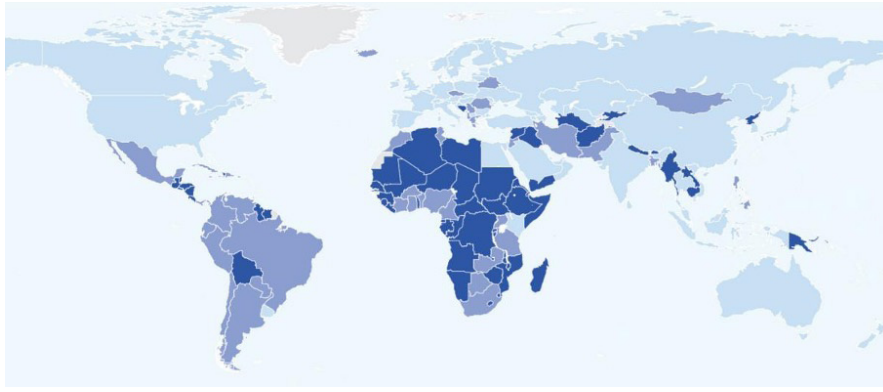
ستجري مناقشة إستراتيجيات الأمن السيبراني في تركيا في هذا القسم بعد تقديم نظرة عامة

حول العالم. ستستند المناقشات إلى تحليل كلي للأركان الخمسة التي يستخدمها الاتحاد الدولي للاتصالات في مؤشره العالمي للأمن السيبراني (GCI). لكل ركيزة عدة مؤشرات؛ سيجري تقييم إستراتيجية تركيا لمعالجة كل ركيزة وتنفيذها لهذه الإستراتيجية في الممارسة العملية على أساس هذه المؤشرات.

كان الأمن السيبراني العالمي واحدًا من بنود جدول أعمال الدول في السنوات العشر الماضية في العلاقات الدولية. كافحت الدول في البداية من أجل تأسيس أمنها السيبراني، لكنها بدأت أيضًا في زيادة قوتها في المجال السيبراني من خلال وسائل وإستراتيجيات مختلفة. يجري تقييم القوة السيبرانية على أساس القدرة الهجومية والدفاعية للدول في الفضاء السيبراني.

ينشر الاتحاد الدولي للاتصالات مؤشره العالمي للأمن السيبراني GCI منذ عام 2015 وأنتج حتى الآن أربعة مؤشرات (في 2015 و2017 و2018 و2020). إن GCI ليس مؤشرًا للأمن السيبراني في حد ذاته، ولكنه مؤشر «التزام» بالأمن السيبراني نظرًا لمنهجية البيانات التي جرى الحصول عليها من الدول الأعضاء البالغ عددها 193 دولة. يقوم على استبيان يتكون من 150 سؤالًا. في المؤشرات الأخيرة بدأ الاتحاد الدولي للاتصالات أيضًا في الحصول على البيانات من المصادر المفتوحة. يقيس GCI التزامات الأمن السيبراني للدول الأعضاء عبر خمس ركائز: التدابير القانونية، التدابير التقنية، التدابير التنظيمية، تدابير تنمية القدرات، وإجراءات التعاون[56].

الخريطة 2: الخريطة الحرارية للالتزام الوطني بالأمن السيبراني



المصدر: «المستودع الوطني لإستراتيجيات الأمن السيبراني»، الاتحاد الدولي للاتصالات (ITU)، ص 13[57]

جرى تصنيف تركيا حاليًّا في المرتبة رقم 11 بنتيجة 97 .49[58] . فقد ازداد أداء الأمن السيبراني الخاص بها ، فارتفعت من المركز 43 في عام 2017 إلى المركز الحادي عشر في عام 2020 .

يجب تأكيد أن المؤشر العالمي للأمن السيبراني GCI يقيس الالتزام بالأمن السيبراني لا الأمن السيبراني نفسه . فتشير درجتها العالية فقط إلى أن تركيا ملتزمة بشدة بالأمن السيبراني . ويُعَدّ الالتزام علامة إيجابية للأمن السيبراني ، ولكن المحدد الحقيقي هو الإجراء . ستوضح البيانات المأخوذة من مؤشر الأمن السيبراني الوطني (NCSI) ومؤشر الطاقة السيبرانية الوطني (NCPI) الواردة أدناه ، ما إذا كان هذا الالتزام ينعكس في العمل أو لا .

جرى إعداد مؤشر حالة اتصال الشبكة NCSI من قبل أكاديمية الحوكمة الإلكترونية (شركة استشارية للتحول الرقمي في إستونيا) وتقيس قدرات الأمن السيبراني للحكومات . ويستند إلى 12 مؤشرًا ، بما في ذلك تطوير سياسة الأمن السيبراني ، وتحليل التهديدات السيبرانية والمعلومات ، والاستجابة للحوادث السيبرانية ، وحماية الخدمات الرقمية ، والعمليات العسكرية السيبرانية[59] . يقيس المعهد الوطني للإحصاء والمعلومات «مستوى الأمن السيبراني لبلد ما ، ويحدد المجالات الرئيسة ذات الأولوية التي يجب معالجتها من أجل تحسين حالة الأمن السيبراني . يوفر الفهرس أيضًا نظرة عامة على مدى استعداد البلدان لمنع الهجمات والجرائم الإلكترونية ومكافحتها»[60] . ووفقًا لتقييمها ، فإن الدول العشر الأولى الأكثر استعدادًا للدفاع ضد الهجمات السيبرانية هي اليونان (10.96) وليتوانيا (51.93) وبلجيكا (51.93) وجمهورية التشيك (21.92) وإستونيا (91.90) وألمانيا (91.90) والبرتغال (61.89) وإسبانيا (31.88) وبولندا (01.87) وفنلندا (71.85) . وقد نالت تركيا المرتبة 57 في NCSI بنتيجة 54 .55[61] .

الخريطة 3 : قدرة الدول على الأمن السيبراني


المصدر : أكاديمية الحوكمة الإلكترونية[62]

من ناحية أخرى، تقيس NCPI القدرة السيبرانية لـ30 دولة بناءً على سبعة أهداف وطنية تسعى إليها الدول باستخدام الوسائل السيبرانية، وهي:

(١) مسح الجماعات المحلية ومراقبتها.

(٢) تقوية الدفاعات السيبرانية الوطنية وتعزيزها.

(٣) التحكم في بيئة المعلومات ومعالجتها.

(٤) جمع المعلومات الاستخبارية الأجنبية للأمن القومي.

(٥) مكاسب تجارية أو تعزيز نمو الصناعة المحلية.

(٦) تدمير أو تعطيل البنية التحتية للعدو وقدراته.

(٧) تحديد القواعد والمعايير التقنية السيبرانية الدولية.[63]

بناءً على هذه الأهداف، تقيس NCPI على وجه التحديد نيات البلدان وقدراتها في مجال المراقبة والدفاع والتحكم والاستخبارات والتجارة والجريمة والمعايير[64]. ووفقًا لـNCPI، تحتاج البلدان لكي تصبح قوة سيبرانية إلى: «قدرات لتحقيق أهدافها المرجوة. تتعلق القدرات السيبرانية بإنشاء اتصالات البنية التحتية للمعلومات الإلكترونية والحاسوبية والشبكات والبرمجيات والمهارات البشرية ومراقبتها. لذلك، تستثمر البلدان في مجموعة واسعة من الموارد، منها مجالات متنوعة، مثل القدرات السيبرانية العسكرية والدفاع السيبراني والمراقبة، فضلًا عن القدرات البشرية وتعزيز المؤسسات والسياسة المحلية»[65].

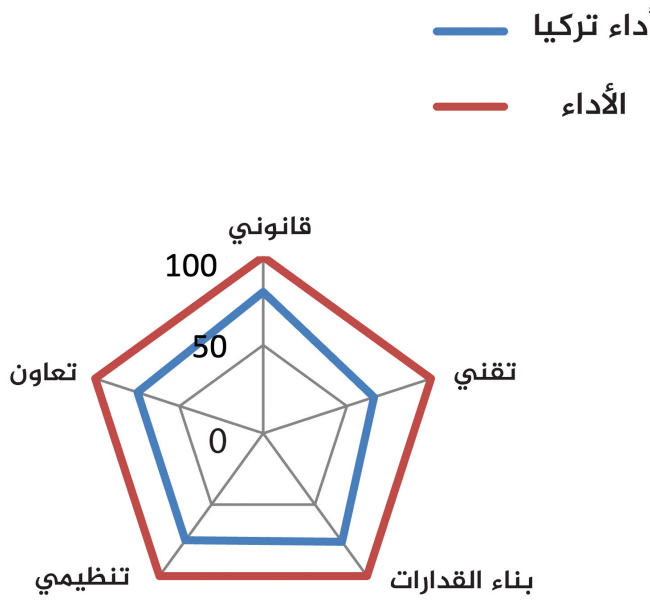
الدول العشر الأولى الأكثر شمولًا بين الدول التي تتمتع بأعلى مستوى من النيات والقدرات عبر هذه الأهداف السبعة في عام 2022 هي؛ الولايات المتحدة (43)، الصين (34)، روسيا (23)، المملكة المتحدة (19)، أستراليا (18)، هولندا (17)، فيتنام (16)، جمهورية كوريا (16)، فرنسا (15)، إيران (14). وأخذت تركيا المرتبة 23 من بين 30 دولة، برصيد (9)[66]. ترتيب تركيا في الأهداف الفرعية، هو: المراقبة (9)، والدفاع (15)، ومراقبة المعلومات (17)، والاستخبارات (22)، والتجارة (24)، والجريمة (25)، والمعايير (24). مقارنة بقدرات مؤشر تركيا لعام 2020 ازداد المؤشر في المراقبة والدفاع والتحكم في المعلومات والاستخبارات والتجارة بينما انخفضت في الجريمة والأعراف[67].

أظهر الأداء التركي زيادة مطردة في كل من المؤشر العالمي للأمن السيبراني GCI الخاص بالاتحاد الدولي للاتصالات وNCPI التابع لمركز بليفر Belfer ، ورغم ذلك بقي مؤشر NCSI التابع لأكاديمية الحوكمة الإلكترونية في السنوات العديدة الماضية بدون تغيير . فيما يأتي ، جرى تحليل البيانات ذات الصلة بكل مؤشر عبر الركائز الخمس للمؤشر العالمي GCI الذي يحاول الحصول على نظرة شاملة لأداء الأمن السيبراني في تركيا .

## مشهد الأمن السيبراني في تركيا

تغطي الأدبيات المتعلقة بالأمن السيبراني في تركيا تحليلًا للوائح القانونية والإدارية الحالية التي تشكل وثائق سياسة الدولة وإستراتيجيتها . يبلغ أداء تركيا الإجمالي في مجال الأمن السيبراني كما هو موضح في الشكل1 ، حوالي 75/ 100 . وهذا المستوى من الأداء جيد ، وإن لم يكن مثاليًا . تحتاج تركيا إلى تحسين بعض المؤشرات في جميع الركائز الخمس ، وهذا ما سنناقشه فيما يأتي . ويبدو أن الحلقة الأضعف هي الدعامة الفنية ، بينما يظهر أقوى أداء في الإجراءات القانونية . تقع الركائز الثلاث الأخرى بينهما ، ولكنها تحتاج أيضًا إلى التطوير لتحسين الأمن السيبراني الوطني في تركيا .

الشكل 1 : قدرة الأمن السيبراني في تركيا




المصدر : استنتاجات توصّل إليها المؤلف من الركائز الخمس التي وضعها الاتحاد الدولي للاتصالات

ستحلل هذه الدراسة بعد ذلك نقاط القوة والضعف في إستراتيجية تركيا للأمن السيبراني بناءً على الركائز الخمس لمعايير الاتحاد العالمي للاتصالات الدولية (GCI) : التدابير القانونية، والتدابير التقنية، والبنية التنظيمية، وبناء القدرات، والتعاون. جرى تفضيل ركائز GCI الخاصة بمعايير الاتحاد للتحليل؛ نظرًا لكونها أدوات شاملة ومناسبة بدرجة كافية لقياس القدرة السيبرانية للجهة الفاعلة. وقد جرى تأكيد مكانة تركيا في العالم في القسم السابق. وبعد إجراء تقييم منظم لإستراتيجيات تركيا، سيجري التعامل مع الفرص والتهديدات التي تواجهها.

## تنظيمات قانونية

تشير التقديرات إلى أن تكلفة الجرائم السيبرانية في جميع أنحاء العالم قد ارتفعت من مليار دولار[68] في عام 2020 إلى ما يصل إلى 6 مليارات دولار في عام 2021[69]. يُعَدّ الفضاء السيبراني مجالًا جذابًا ومركزًا للمجرمين؛ لأن ارتكاب جريمة في الفضاء السيبراني هو أمر رخيص ومربح ومنخفض المخاطر. من أجل توفير منطقة سيبرانية مجانية وآمنة يُعَدّ القانون أداة فعالة. لذلك، تحتاج الحكومات إلى تنظيم هذا المجال من خلال العمليات القانونية. فتسمح الإجراءات القانونية للحكومات «بوضع آليات استجابة أساسية من خلال التحقيق في الجرائم ومقاضاة مرتكبيها وفرض عقوبات على عدم الامتثال أو خرق القانون»[70]. تتضمن اللوائح تحديد «الأنشطة غير المشروعة في الفضاء السيبراني، إلى جانب تحديد الأدوات الإجرائية اللازمة للتحقيق في مثل هذه التشريعات ومقاضاتها وإنفاذها. وكذلك إنشاء خطوط أساسية للأمن السيبراني، وآليات امتثال لمجموعة من أصحاب المصلحة الوطنيين. وإجراءات لضمان الاتساق مع الالتزامات الدولية»[71]. ولا بد هنا من تعاون أصحاب المصلحة في سبيل الحصول على إطار قانوني فعال، ولاسيّما على المستوى الدولي. وقد جرى حتى الآن إحراز تقدم ضئيل على هذا المستوى؛ بسبب الخلافات بين الدول الوطنية حول اللوائح في الفضاء السيبراني. ومن ثَمّ فإن مجال القانون السيبراني يقتصر على اللوائح الوطنية، التي هي أقل فعالية من التعاون في تنظيم شبكة عالمية.

بدأت تركيا بتطوير لوائح قانون الإنترنت في أوائل التسعينيات. وكان قرار مجلس الوزراء رقم 2012/ 3842 الصادر في يونيو 2012 هو أكثر اللوائح شمولًا بشأن مبادرات الأمن السيبراني الوطنية. كما أصدرت الحكومة التركية لوائح قائمة بذاتها، مثل قانون الاتصالات الإلكترونية (رقم 5809)، وقانون التوقيع الإلكتروني (رقم 5070)، وقانون تنظيم المطبوعات على الإنترنت وقمع الجرائم المرتكبة عن طريق هذه المنشورات (رقم 5651)، وقانون تنظيم التجارة الإلكترونية (رقم 6563)، وقانون حماية البيانات الشخصية

(رقم 6698) . كما جرى إجراء تغييرات على التشريعات القائمة لمعالجة الفضاء السيبراني ، بما في ذلك القانون الجنائي التركي (رقم 5237) ، وقانون التجارة التركي (رقم 6102)[72] .

سنَّت تركيا تشريعات شاملة لمعالجة اللوائح القانونية في الفضاء السيبراني . ومع ذلك ، فإن الغرض من الإجراءات القانونية ليس فقط إصدار اللوائح ، بل كذلك تنفيذها وتطبيقها ، وقد كان أداء تركيا جيدًا في البعد القانوني . وفقًا لأطر المراقبة الدولية . وحقّقت تركيا أداءً مثاليًّا من حيث مساعيها القانونية وفقًا لمعايير الاتحاد العالمي للاتصالات الدولية GCI لعام 2020 ، وحصلت على 20 نقطة من أصل 20 نقطة[73] . ومع ذلك ، فإن درجة تركيا في مؤشر الأمن السيبراني الوطني NCSI لعام 2020 بلغت حوالي 80 نقطة من أصل 100[74] . تغطي أقسام المراقبة والتجارة في مؤشر الطاقة السيبرانية الوطني NCPI اللوائح القانونية . ومتوسط درجات تركيا في هذا المؤشر هو حوالي 60 من أصل 100[75] . أي (+60 +80 100)/ 3= 80 . ومن ثَمّ ، فإن الأداء القانوني العام لتركيا بناءً على تقييم هذه المصادر الثلاثة يبلغ حوالي 80/ 100 .

يبدو أن تركيا حققت نجاحًا كبيرًا في حماية البيانات الشخصية ومكافحة الجرائم السيبرانية ، لكنها ضعيفة نسبيًّا في الاستجابة للحوادث السيبرانية وتحليل التهديدات السيبرانية وإدارة الأزمات السيبرانية[76] . وعلى الرغم من أن لوائحها القانونية شاملة من وجهة نظر أمنية سلبية ، فإن أجهزتها القانونية تبدو ضعيفة من حيث تصوّر الحقوق والحريات على الإنترنت .

## التدابير الفنية

تغطّي هذه الركيزة البنية التحتية التقنية لمكافحة المخاطر والحوادث السيبرانية التقنية ، ومن ذلك فرق الاستجابة للطوارئ الحاسوبية CERTs ، والشهادات ، والآليات التقنية ، والقدرات المنشورة لمعالجة البريد الإلكتروني العشوائي ، وحماية الأطفال عبر الإنترنت . فكما يؤكد معايير الاتحاد العالمي للاتصالات الدولية GCI ، فإن «البلدان تبقى عرضة للخطر بدون توفر المهارات التقنية المناسبة لاكتشاف الهجمات السيبرانية والاستجابة لها»[77] . يُعَدّ تطوير البرامج والأجهزة الوطنية أمرًا حيويًّا للأمن السيبراني نظرًا لأن الأمن السيبراني لا يستهلكه المتسللون السيئون فحسب ، بل تستهلكه أيضًا الدول القومية وشركات تكنولوجيا المعلومات . أي أن جميع أصحاب المصلحة في الفضاء السيبراني يشكلون تهديدًا ويقومون بهجمات إلكترونية . ومن ثَمّ ، يؤدّي الأمن السيبراني الوطني والمنتجات التقنية دورًا رئيسًا في الأمن السيبراني الوطني .

قامت تركيا بتطوير فرق الاستجابة للطوارئ الحاسوبية CERTs الخاصة بها[78]، وأطر إصدار الشهادات، وتشريعات وآليات حماية الطفل عبر الإنترنت[79]. فِرَق الاستجابة لحوادث الكمبيوتر (CIRTs) «مسؤولة عن اتخاذ تدابير لضمان أمن المعلومات لقطاع معين أو مؤسسة معينة، وحماية قطاع أو مؤسسة معينة ضد الهجمات السيبرانية، واتخاذ تدابير لتقليل الضرر في حالة وقوع هجوم، والرد على الهجمات المحتملة، وضمان تدفق المعلومات مع شركاء مختلفين، وضمان الاستعداد والتوافر على مدار الساعة طوال أيام الأسبوع»[80].

الأداء الفني التركي أضعف نسبيًّا مقارنة بأدائها القانوني. يصنف معايير الاتحاد العالمي للاتصالات الدولية GCI لعام 2020 تركيا بـ19. 54/ 20 (~ 98)، بينما يضع مؤشر الأمن السيبراني الوطني NCSI لعام 2020 الدولة في المرتبة 50/ 100 في فعالية فرق استجابة الطوارئ الحاسوبية CIRT والسلامة والأمن السيبراني (50/ 100)، ووحدة تحليل التهديدات الإلكترونية (20/ 100). ومن هنا فإن درجة مؤشر الأمن السيبراني الوطني NCSI التركي للقدرة التقنية هي 120/ 3 = 40/ 100. ودرجة دفاعها NCPI لعام 2020 هي 30، في حين أن أعلى دولة لديها 50 نقطة (من أجل التسهيل، جرى مضاعفة كلا الرقمين 30/ 50 للحصول على المستوى نفسه مثل المؤشرات الأخرى)، ومن ثَمّ، يمكن الاستقراء بأن الأداء العام لتركيا هو 66/ 100.

## التدابير التنظيمية

تشمل المنظمات واللوائح الإدارية وثائق الإستراتيجيات الوطنية للأمن السيبراني NCSS التي تحكم وتنسق أنشطة ومبادرات الأمن السيبراني الوطنية. ومن هنا، فإن التدابير التنظيمية تقيس الإستراتيجيات والمنظمات الوطنية التي تنفذ الأمن السيبراني. يمكن أن يؤدي الافتقار إلى الإعداد التنظيمي المناسب إلى تنسيق غير فعال ويؤدي إلى انعدام الأمن. تتطلب هذه الركيزة أهدافًا وغايات شاملة تضعها الحكومة إلى جانب خطة شاملة للتنفيذ والتوزيع والقياس. ويجب أن تكون الوكالات الوطنية حاضرة لتنفيذ الإستراتيجية، وتقييم النتائج. وفي غياب إستراتيجية وطنية ونموذج حوكمة وهيئة إشرافية، تتعارض الجهود في مختلف القطاعات، ممّا يمنع الجهود المبذولة للحصول على تنسيق فعال في تطوير الأمن السيبراني[81].

قامت تركيا بتطوير ثلاث وثائق للإستراتيجية الوطنية للأمن السيبراني NCSS منذ عام 2013. تحدد الإستراتيجية وخطة العمل الوطنية للأمن السيبراني (2020–2023) ثمانية أهداف إستراتيجية:

(١) حماية البنى التحتية الحيوية وتعزيز قوتها .

(٢) تطوير القدرات الوطنية .

(٣) شبكة الأمن السيبراني العضوية .

(٤) أمن تقنيات الجيل القادم .

(٥) محاربة جرائم الإنترنت .

(٦) تطوير ودعم التقنيات المحلية والوطنية .

(٧) دمج الأمن السيبراني في الأمن القومي .

(٨) تطوير التعاون الدولي .[82]

لسوء الحظ ، لا يتضمن التقرير الأخير خطة عمل معلنة ، وهو حذف يُفهم على أنه انتهاك للشفافية في الفضاء السيبراني . في الوثيقتين السابقتين من وثائق للإستراتيجية الوطنية للأمن السيبراني NCSS ، جرى إعلان عمليات التنفيذ والمنظمات وخطط العمل[83] .

يؤدّي العديد من المنظمات دورًا في تنفيذ الإستراتيجية الوطنية للأمن السيبراني NCSS في تركيا . فوزارة النقل والبنية التحتية هي المسؤولة عن إعداد وإدارة «أنشطة الأمن السيبراني على المستوى الإستراتيجي مع المجلس الوطني للأمن السيبراني (الذي أُنشِئ في عام 2013) والفريق الوطني للاستجابة لحوادث الكمبيوتر (National CIRT) بإدارة مؤسسة تقنيات المعلومات والاتصالات (BTK) ، وهيئة تكنولوجيا المعلومات والاتصالات»[84] . المنظمات الأخرى المشاركة في الأمن السيبراني تشمل الفرق الوطنية والقطاعية للاستجابة لحوادث الكومبيوتر CERTs ، والمجلس الوطني للأمن السيبراني ، ومكتب التحول الرقمي للرئاسة ، ورئاسة الصناعات الدفاعية ، ومجلس البحث العلمي والتكنولوجي (TUBİTAK) ، وفرع الشرطة لمنع الجريمة السيبرانية والشخصية . وهيئة حماية البيانات (KVKK) ووزارة الدفاع الوطني والقوات المسلحة التركية (TSK) ورئاسة منظمة المخابرات الوطنية (MİT)[85] . يجادل شنتورك وجيل وصاغر أوغلو بأن «أحد أهم القضايا [في تفعيل الأمن السيبراني] هو تعيين سلطة مركزية واحدة تكون مسؤولة عن الأمن السيبراني الوطني العام . يجب أن تنسق هذه السلطة جميع جهود المنظمات الأخرى وأنشطتها التي لديها مهام تتعلق بالأمن السيبراني مثل الاعتماد والتدقيق والمعايير والمواصفات وحماية كل من الأنظمة العامة والخاصة ، وكذلك البنى التحتية الحيوية»[86] .

وزارة النقل والبنية التحتية هي المنسق الوطني التركي للأمن السيبراني، ولكن هناك بعض المخاوف بشأن فعاليتها وقدرتها على تنظيم جميع المؤسسات ذات الصلة. وقد جرت العادة أن يكون المنسقون الوطنيون الأقوياء مسؤولين أمام أعلى سلطة في الهيكل الحكومي. ولكن بدلًا من وجود مؤسسة مسؤولة بشكل مباشر أمام الرئيس، مثل مكتب التحول الرقمي للرئاسة، يجري إسناد هذه المهمة إلى وزارة في تركيا.

يصنف معايير الاتحاد العالمي للاتصالات الدولية GCI أداء الحكومة التركية في الإطار التنظيمي بـ 17 .96/ 200. ووفقًا لـNCSI، فإن تطوير سياسة الأمن السيبراني في تركيا هو 86/ 100، وعملياتها العسكرية السيبرانية هي 17/ 100 وحماية البيانات الشخصية هي 100/ 100، وعليه فالمعدل العام في تركيا هو 76/ 100.

## بناء القدرات

يتعلق بناء القدرات بزيادة الوعي، وتوفير التدريب والتعليم، والحوافز، وحملات تطوير ثقافة الأمن السيبراني بين جميع مستخدمي الإنترنت أو المواطنين الرقميين. يُعَدّ ما يزيد على نصف سكان العالم اليوم، أي ما يقرب من 5 .3 مليارات شخص من مستخدمي الإنترنت. ويجري في كل يوم إجراء ما يزيد على سبعة مليارات عملية بحث على غوغل، وتتم مشاركة ما يزيد على 10 مليارات غيغا بايت من المعلومات عبر الإنترنت، ويجري اختراق أكثر من 250 ألف صفحة ويب[87]. ووفقًا لتشيك بوينت، يحدث أكثر من 60 مليون هجوم إلكتروني في المتوسط كل يوم[88]. ويُعَدَ المستخدم أو الفرد الحلقة الأضعف في الأمن السيبراني، وهو مفتوح للهجمات السيبرانية للهندسة الاجتماعية مثل التصيّد الاحتيالي ورسائل البريد العشوائي. لذلك، «يُعَدّ بناء قدرات الأمن السيبراني أمرًا أساسيًّا؛ لأنه يسهم في تقليل مشكلات الفجوة الرقمية والمخاطر الإلكترونية وما شابهها»[89]. ويجري قياس بناء القدرات من خلال «عدد برامج البحث والتطوير والتعليم والتدريب والمهنيين المعتمدين ووكالات القطاع العام»[90].

أطلقت تركيا العديد من المبادرات لزيادة الوعي، وأجرت برامج البحث والتطوير، وطوّرت دورات تدريبية رسمية وغير رسمية، وقدّمت التعليم الفني، وأطلقت عددًا قليلًا من الحملات. ووفقًا لمعايير الاتحاد العالمي للاتصالات الدولية GCI لعام 202، تبلغ درجة تنمية القدرات في تركيا 20/ 20. وحسب تصنيف NCSI لعام 2020 في تركيا من حيث التطوير التعليمي والمهني، الذي يتضمن عددًا من البرامج في الجامعة وكذلك في المدارس الابتدائية والثانوية، هو 50/ 100. لذلك، متوسط درجة تركيا في بناء القدرات هو 75/ 100.

## التعاون

لا تهيمن الدول على الفضاء السيبراني، وهو في الواقع، مجال لأصحاب المصلحة المتعددين، فهذا الفضاء مأهول بجهات خاصة قوية تتمتع بقدرات أكبر من الدول، لذلك تحتاج الدول إلى التعاون مع الجهات الفاعلة غير الحكومية، بما في ذلك الشركات الخاصة والمنظمات الدولية وتكنولوجيا المعلومات (IT) والمنظمات غير الحكومية (NGOs) والخبراء، لضمان الأمن القومي في الفضاء السيبراني. وعالمية شبكة الإنترنت توجب تعاونًا عالميًّا لضمان الأمن. ومن ثَمّ، هناك حاجة للتعاون على المستوى الدولي بين الدول وجميع أصحاب المصلحة الآخرين: «لا يمكن ضمان أمن النظام البيئي السيبراني العالمي أو إدارته من قبل أي صاحب مصلحة واحد، ويحتاج إلى تعاون وطني وإقليمي ودولي لتوسيع مدى الوصول والتأثير»[91]. يشمل التعاون الشراكات بين القطاعين العام والخاص، والاتفاقيات الثنائية والمتعددة الأطراف، والشراكات بين القطاعين العام والخاص، وأفضل الممارسات. وكما تحث معايير الاتحاد العالمي للاتصالات الدولية GCI، «يمكن أن يؤدي تعاون أكبر إلى تطوير قدرات أقوى بكثير في مجال الأمن السيبراني، مما يساعد على ردع التهديدات المتكررة والمستمرة عبر الإنترنت، وتمكين عمليات التحقيق والقبض على العملاء الخبيثين ومقاضاتهم بشكل أفضل»[92].

لقد تعاونت الحكومة التركية بالفعل مع الجهات الخاصة في بعض المشروعات. فقد تم على سبيل المثال في التعاون الوطني، إطلاق مشروع لمكافحة البريد الإلكتروني العشوائي في عام 2009 من قبل مؤسسة تقنيات المعلومات والاتصالات BTK بمشاركة العديد من المؤسسات العامة والخاصة»[93]. تنخرط تركيا أيضًا في التعاون الدولي من خلال عضويتها في حلف شمال الأطلسي، والشراكة مع المجلس الأوروبي. وتم تقدير مبادرات تركيا للتعاون على المستويين الوطني والدولي من قبل GCI لعام 2020 بدرجة 20/ 20، ومن قبل NCSI بمعدل 50/ 100، بناءً على إسهام الدولة في الأمن السيبراني العالمي ومن ذلك أنشطة التعاون. ومن هنا فإن متوسط أداء تركيا من حيث التعاون هو 75/ 100.

## خاتمة

يكشف التحليل الكمي والنوعي الذي جرى إجراؤه هنا أن تركيا تتناول الفضاء السيبراني في حساباتها الأمنية بوصفه المجال التشغيلي الخامس إلى جانب الأرض والبحر والجو والفضاء. والفضاء السيبراني بأبعاده المادية والافتراضية والمنطقية والمعلوماتية- يُعَدّ

فضاءً معقدًا للغاية، بحيث لا يمكن فهمه بالكامل من قبل تخصص واحد. بدلًا من ذلك، هناك حاجة إلى نهج متعدد التخصصات لفهمه ومعالجته. والفضاء السيبراني في الواقع معقد للغاية لدرجة أنه الشيء الوحيد الذي أوجده البشر ولا يفهمونه. وعلى الرغم من أن الفضاء السيبراني كان حقيقة في حياتنا لأكثر من 50 عامًا؛ لم يجري تطوير نظرية شاملة للفضاء السيبراني.

عدّت الدول الفضاء السيبراني قضية سياسية منخفضة الأهمية، ولم يبدأ الاعتراف بأهميتها إلا بعد مرور وقت طويل. فقد أصبحت الدول قبل عقد من الزمان فقط، تعترف بها على أنها مسألة سياسات عليا، وأنها قضية حاسمة بالنسبة للقضايا الأمنية والعسكرية والإستراتيجية . ونتيجة لذلك، يتبوّأ الأمن السيبراني الآن موقعًا آمنًا كأحد أهم بنود جدول الأعمال العالمي. وجرى دمج الأمن السيبراني الآن في رؤى وخطط الأمن القومي في جميع أنحاء العالم. وكما أن مصطلح الأمن السيبراني متعدد الأبعاد، فإن العمل في الأمن السيبراني يحدث على مستويات متعددة: مستويات فردية ومجتمعية وحكومية وعالمية. ويبقى المستخدم الفردي هو الحلقة الأضعف في الأمن السيبراني. لذلك، يُعَدّ بناء قدرات الأمن السيبراني على المستويين الفردي والمجتمعي أمرًا ضروريًّا للأمن السيبراني الوطني والعالمي.

بناءً على النتائج والتحليلات الواردة في هذه الورقة، جرى اقتراح التوصيات الآتية لكل ركيزة رئيسة مستخدمة في مؤشر معايير الاتحاد العالمي للاتصالات الدولية GCI:

فيما يتعلق بالتدابير القانونية، تُعَدّ تركيا ضعيفة نسبيًّا في الاستجابة للحوادث السيبرانية، وتحليل التهديدات السيبرانية، وإدارة الأزمات السيبرانية. ومن ثَمّ، فهي بحاجة إلى مزيد من تطوير اللوائح القانونية بشأن تحسين التعاون والتنسيق في المجتمع السيبراني. تحتاج تركيا أيضًا إلى التركيز بشكل أكبر على الحقوق والمسؤوليات عبر الإنترنت لتشمل فهمًا أمنيًّا إيجابيًّا لا مجرد فهم أمني سلبي. يسهم تطوير الإجراءات القانونية في جاهزية الدولة في مجال الأمن السيبراني، لكن التنفيذ السليم، وكذلك إنشاء أبعاد معيارية للوائح، بما في ذلك حقوق الإنسان والمسؤوليات؛ يُعَدّ أمرًا أكثر أهمية.

وعندما يتعلق الأمر بالبعد التقني، فإن تركيا ضعيفة نسبيًّا في الاستجابة للحوادث السيبرانية، والسلامة والأمن السيبراني، وتحليل التهديدات السيبرانية، وإدارة الأزمات السيبرانية. ومن هنا، فهي بحاجة إلى تعزيز فرق الاستجابة الوطنية والقطاعية للحوادث الحاسوبية CIRT، وتطوير المزيد من التعليم الفني للمهنيين.

وفيما يتعلق بالإعداد التنظيمي، يجب على تركيا تحديد مؤسسة تنسيقية قوية ذات تفويض شامل ومسؤول مباشرة أمام الرئيس. هناك حاجة أيضًا إلى تسلسل هرمي واضح بين مؤسسات الأمن السيبراني. تحتاج تركيا بشدة إلى مؤسسة ذات نطاق وسلطة كافيين لتطوير وتنفيذ إستراتيجية مركزية للأمن السيبراني. إن وجود إستراتيجية وطنية أكثر شفافية للأمن السيبراني أمر لا بد منه. ونظرًا لأن الفضاء السيبراني يعتمد على الشفافية، فإن مشاركة المعلومات مع الجمهور وإدراج الجهات الفاعلة الخاصة في فرق الأمن السيبراني أمر لا غنى عنه. والحفاظ على سرية خطة العمل، كما هو الحال في وثائق الإستراتيجية الوطنية للأمن السيبراني NCSS لعام 2020، ليس حلًّا، ولكنه مصدر لانعدام الأمن. يجب الإعلان عن الهجمات السيبرانية الكبرى على البنى التحتية الحيوية أو مؤسسات الدولة لتطوير تدابير مضادة، وإلا، فإن تكرار حدوثها كما رأينا عدة مرات أمر لا مفر منه. لكن المفهوم الرئيس هنا هو التعاون وتبادل المعلومات. وتخلّف المؤسسات المشاركة في مشاركاتها في توفير الأمن السيبراني المعلومات سيؤدي إلى انعدام الأمن بكونه نتيجة طبيعية. ومن ثَمّ ينبغي أن تقترح الإستراتيجيات الجديدة آليات وحوافز جديدة لتقاسم المعلومات عبر المؤسسات العامة وبين القطاعين العام والخاص.

فيما يتعلق ببناء القدرات، يجب تطوير المزيد من الدورات التدريبية الرسمية وغير الرسمية، وتعليم الأمن السيبراني في المدارس الابتدائية والثانوية، وبرامج الأمن السيبراني في الجامعات. ينبغي تشجيع البحث والتطوير في مجال الأمن السيبراني ودعمه على جميع المستويات. يجب تعزيز ودعم مشاركة الجامعات والشركات الخاصة والمنظمات غير الحكومية في التدريب والحملات في مجال الأمن السيبراني. يجب أن تستفيد المؤسسات العامة من الخبرة على جميع المستويات من دون أي تمييز على أساس العرق أو الدين أو الجنس أو الآراء الفلسفية أو السياسية.

وختامًا، فيما يتعلق بتدابير التعاون، ينبغي إسباغ الطابع الرسمي على المزيد من الشراكات بين القطاعين العام والخاص والاتفاقات الثنائية والمتعددة الأطراف. والشراكة على المستويين الوطني والدولي بشفافية مطلقة هي مفتاح النجاح. جرى وضع نظريات وثائق الإستراتيجية الوطنية للأمن السيبراني NCSS الثلاث التي جرى تطويرها في العقد الماضي اعتمادًا على الحاجة إلى الكيانات العامة والخاصة للعمل معًا في مواجهة التهديدات. ولكن التعاون في الممارسة العملية كان ضعيفًا. فعلى سبيل المثال، لا يوجد ممثلون من جهات فاعلة غير حكومية، لا بين أعضاء مجلس الأمن السيبراني، ولا في المؤسسات التنظيمية والإشرافية التركية. وتفتقر فرق الاستجابة لطوارئ الحاسوب CIRT العامة والقطاعية أيضًا إلى مشاركة القطاع الخاص. وبغير الشراكة القوية بين القطاعين

العام والخاص التي تعزز مشاركة المعلومات وتسهل الاستجابات المنسقة للمخاطر والتهديدات- لا يمكن الحفاظ على النظام البيئي التركي آمنًا، فالتعاون بين القطاعين العام والخاص، وكذلك التعاون الدولي- أمر حتمي لضمان الأمن في الفضاء السيبراني، فالفضاء السيبراني مجال عالميّ فوضويّ يتطلب تعاونًا عالميًّا على كل المستويات بين جميع أصحاب المصلحة.

## الهوامش والمراجع


1. «إحصاءات الإنترنت الحية / Internet Live Stats»، 12 مارس 2022 https://www../internetlivestats.com

2. «إحصاءات الإنترنت الحية».

3. «خريطة التهديد السيبراني الحية»، Checkpoint، 12 مارس 2022: https://threatmap./checkpoint.com

4. ستيف مورغان، «جرائم الإنترنت تدمر ستة تريليونات دولار بحلول عام 2021»، مشروعات الأمن السيبراني، 14 مايو 2022:

https://cybersecurityventures.com/annual-cybercrime-report-2017/#:~:text=Cybersecurity%20Ventures%20predicts%20cybercrime%20damages,in%20size%2C%20sophistication%20and%20cost.

5. جوزيف س. ناي، «نهاية الفوضى السيبرانية؟ كيفية بناء نظام رقمي جديد»، الشؤون الخارجية، المجلد 101، العدد 1 (يناير / فبراير 2022)، 24 مارس 2022: (ص 3): https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy

6. ناي، «نهاية الفوضى السيبرانية؟».

7. ويليام ك. تيريل، «إستراتيجية الأمن السيبراني والسياسة والتنظيم في الولايات المتحدة: وضع ضعيف للتعامل مع بيئة الأمن بعد 11 سبتمبر؟»، دكتوراه غير منشورة. أطروحة، كلية قيادة الجيش الأمريكي وكلية الأركان العامة، (2012)، ص 7-8.

8. ويليام جيبسون، نيورومانسر، (نيويورك: خيال علمي، 1984)، 1 مايو 2022:

https://kupdf.net/download/william-gibson-neuromancer_59fbef8ce2b6f5126218562c_pdf.

9. فرانكلين د. كرامر، «القوة السيبرانية والأمن القومي»، (تحرير: فرانكلين د. كرامر، وستيوارت هـ. ستار، ولاري ك. وينتز)، القوة الإلكترونية والأمن القومي، (واشنطن العاصمة: Potomac Book، 2009)، 1 مايو 2022: (ص 4):

https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017210-115052-16-06-

10. هوغو لويسو، «العلوم الاجتماعية والدراسات على الإنترنت والفضاء السيبراني»، Chaire Cyber (2013)، 3 مايو 2022:

https://www.chaire-cyber.fr/IMG/pdf/r1_1_hugo_loiseau_territorialite_dans_le_cyberespace_3_draftv1.pdf.

11. أليساندرو فينامور، «تحليل وتوصيف وتصنيف حركة المرور على الإنترنت»، إيريس بوليتو (2012)، 3 مايو 2022:

https://iris.polito.it/handle/115832497191/.

12. دانيال ت. كويهل، «من الفضاء السيبراني إلى القوة السيبرانية: تحديد المشكلة»، (تحرير: كرامر وستار ووينتز)، القوة السيبرانية والأمن القومي، ص 27.

13. «نظرة عامة على ENISA للأمن السيبراني والمصطلحات ذات الصلة»، ENISA، (سبتمبر 2017)، 1 مايو 2022: (ص 6)

https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

14. ميليسا إ. هاثاواي وألكسندر كليمبورغ، «اعتبارات أولية: حول الأمن السيبراني الوطني»، (تحرير: ألكسندر كليمبورغ)، دليل إطار عمل الأمن السيبراني الوطني، (تالين: منشورات الناتو 1، CCD COE، 2012)، مايو 2022: (ص 8):

https://ccdcoe.org/uploads/201810//NCSFM_0.pdf

15. «الإستراتيجية الوطنية للأمن السيبراني وخطة العمل 2013-2016»، وزارة النقل والشؤون البحرية والاتصالات في الجمهورية التركية، (2016)، 1 مايو 2022: (ص 8):

1-cyber-security-strategy-and--0-https://www.btk.gov.tr/uploads/pages/2 5a3412df707ab.pdf-2014-action-plan-2013

16. «الإستراتيجية الوطنية للأمن السيبراني وخطة العمل 2013-2016»، ص 7.

17. «الإستراتيجية الوطنية للأمن السيبراني وخطة العمل 2020-2023»، وزارة النقل والشؤون البحرية والاتصالات في الجمهورية التركية، 2020، ص 10. استخدم الاتحاد الدولي للاتصالات التعريف نفسه في عام 2011. انظر: «دليل الأمن السيبراني الوطني للاتحاد الدولي للاتصالات»، الاتحاد الدولي للاتصالات (2011)، 1 مايو 2022: ص 5:

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

18. لاري د. ولش أوساف، «الفضاء السيبراني: المجال التشغيلي الخامس»، المؤسسة الدولية للتنمية IDA، 1 مايو 2022: (ص 3): https://apps.dtic.mil/sti/pdfs/AD1124078.pdf

19. نازلي شكري، السياسة السيبرانية في العلاقات الدولية، كامبردج: مطبعة معهد ماساتشوستس للتكنولوجيا (2012)، ص 234.

20. شكري، السياسة الإلكترونية في العلاقات الدولية، ص 236.

21. شكري، السياسة الإلكترونية في العلاقات الدولية، ص 236.

22. ناي، «نهاية الفوضى السيبرانية؟».

23. أوساف، الفضاء السيبراني، ص 2.

24. ناي، «نهاية الفوضى السيبرانية؟»، ص 3.

25. نذير آق يشيلمَن، السياسة السيبرانية والأمن السيبراني مع نهج متعدد التخصصات / Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik، (أنقرة، دار أوريون، 2018)، ص 107.

26. بول م. ناكاسوني ومايكل سولماير، «كيفية التنافس في الفضاء السيبراني: النهج الجديد للقيادة السيبرانية»، فورين أفيرز، المجلد 99، رقم 4 (25 أغسطس 2020)، 16 مايو 2022:

https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

27. ناكاسوني وسولماير، «كيفية التنافس في الفضاء الإلكتروني»، ص 2.

28. دان كريجن، ناديا دياكون - ثيبولت، وراندي بورس، «تعريف الأمن السيبراني»، مراجعة إدارة الابتكار التكنولوجي، (أكتوبر 2014)، 25 أبريل 2022: ص 13: https://www.timreview.ca/article/835

29. «تعريف الأمن السيبراني»، الاتحاد الدولي للاتصالات، 25 أبريل 2022:

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

30. «تعريف الأمن السيبراني».

31. « الوثائق الإستراتيجية الوطنية للأمن السيبراني NCSSD في تركيا 2016-2019»، ص 10.

32. «تعريف الأمن السيبراني».

33. مايكل فيل وإيان براون، «الأمن السيبراني»، مراجعة سياسة الإنترنت، المجلد 9، رقم 4 (2020)، 25 أبريل 2022: (ص 2):

https://policyreview.info/pdf/policyreview-20201533-4-.pdf

34. فيل وبراون، «الأمن السيبراني».

35. في هذه الورقة، تُستخدم العلاقات الدولية (IR) بأحرف كبيرة للإشارة إلى النظام الدولي، بينما تشير العلاقات الدولية في الحالة الصغيرة إلى العلاقات عبر الحدود بين الدول.

36. هيلاري أورمان، «دودة موريس: منظور لمدة خمسة عشر عامًا»، الأمن والخصوصية، (سبتمبر / أكتوبر 2003)، 3 مايو 2022: ص 35:

https://www.cs.umd.edu/class/fall2019/cmsc818O/papers/morris-worm.pdf

37. آق يشيلمَن، السياسة السيبرانية والأمن السيبراني مع نهج متعدد التخصصات، ص 59.

38. وليام ج. لين الثالث، «الدفاع عن مجال جديد: إستراتيجية البنتاغون السيبرانية»، فورين أفيرز، المجلد 89، رقم 5 (سبتمبر / أكتوبر 2010)، 4 مايو 2022: (ص 99): https://www.law.upenn.edu/live/files/6465-12-lynn-defending-a-new-

39. شيماكوف، «دودة موريس»، ص 1.

40. تيد أيزنبرغ، ديفيد غرايس، جوريس هارتمانيس، دون هولكومب، م. ستيوارت لين، وتوماس سانتورو، «لجنة كورنيل: حول موريس والدودة»، اتصالات جمعية الحواسيب، المجلد 2، رقم 6 (يونيو 1989)، 4 مايو 2022: ص 706:

https://www.cs.cornell.edu/courses/cs1110/2009sp/assignments/a1/p706-eisenberg.pdf

41. «الدودة هي برنامج يمكن تشغيله من تلقاء نفسه، ويمكنه نشر نسخة تعمل بكامل طاقتها على أجهزة أخرى. اسم مشتق من كلمة الدودة الشريطية، وهي كائن طفيلي يعيش داخل مضيف، ويستنزف موارده للحفاظ على نفسه. في المقابل، «الفيروس هو جزء من التعليمات البرمجية التي تضيف نفسها إلى برامج أخرى، بما في ذلك أنظمة التشغيل. لا يمكن تشغيله بشكل مستقل، فهو يتطلب تشغيل برنامج «المضيف» لتنشيطه. على هذا النحو، لديها نظير واضح للفيروسات البيولوجية، فهذه الفيروسات لا تُعَدّ على قيد الحياة بالمعنى المعتاد. لكنها تغزو الخلايا المضيفة وتخربها، وتحملها على إنتاج فيروسات جديدة «. انظر: يوجين هـ. سبافورد، «برنامج دودة الإنترنت: تحليل»، تقرير بوردو الفني CSD-TR-823، جامعة بوردو (1988)، 4 مايو 2022:/:https spaf.cerias.purdue.edu/tech-reps/823.pdf

42. أكشاي جاجو، «دراسة حول دودة موريس»، (2021)، 4 مايو 2022:

https://www.researchgate.net/publication/357046348_A_study_on_the_Morris_Worm

43. أورمان، «دودة موريس»، ص 35.

44. أورمان، «دودة موريس»، ص 40.

45. ليندا روزنكران، «الحكم على الهاكر المراهق (فتى المافيا)»، عالم الكومبيوتر (2001)، 4 مايو 2022:

https://www.computerworld.com/article/2583318/teen-hacker--mafiaboy--sentenced.html

46. ريبيكا هيرشر، «مقابلة فتى المافيا، المزحة المزعجة التي أوقف الإنترنت»، NPR، (فبراير 2015)، 4 مايو 2022:

https://www.npr.org/sections/alltechconsidered/2015384567322/07/02//meet-mafiaboy-the-bratty-kid-who-took-down-the-internet

47. تشارلز نيسون وأنيتا راماستري، «الجريمة السيبرانية»، سيبر هارفارد، (يونيو 2002)، 4 مايو 2022:https://cyber.harvard.edu/studygroup/cybercrime.html

48. سوزان هينيسي، «ردع الهجمات السيبرانية: كيفية تقليل الضعف»، فورين أفيرز، المجلد 96، رقم 6 (نوفمبر / ديسمبر 2017)، 4 مايو 2022، https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks. ص 41.

49. جون مولر، «التهديدات الرقمية للوهم الإلكتروني يمكن التحكم فيها وليست وجودية»، فورين أفيرز، المجلد. 101، رقم 2، (22 مارس 2022)، 4 مايو 2022، من https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion ص (1-2). لورانس ج. تروتمان، «هل الهجوم السيبراني هو بيرل هاربور الثاني؟» مجلة نورث كارولينا للقانون والتكنولوجيا، المجلد 18، العدد 2، (ديسمبر 2016)، 4 مايو 2022:https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1326&context=ncjolt. . ص 233.

50. جون مولر، معهد كاتو «الوهم السيبراني» (22 مارس 2022)، 4 مايو 2022:

https://www.cato.org/commentary/cyber-delusion

51. «تسهيل وجود فضاء سيبراني موثوق للجميع»، الاتحاد الدولي للاتصالات 4 ،ITU (2022) مايو 2022:

https://www.itu.int/itu-d/sites/cybersecurity/.

52. «دليل إستراتيجية الأمن السيبراني الوطني للاتحاد الدولي للاتصالات»، الاتحاد الدولي للاتصالات ITU، (سبتمبر 2011)، 4 مايو 2022: (ص 100): https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

53. «إرشادات إستراتيجية الأمن السيبراني الوطنية»، الناتو (2013)، 4 مايو 2022: (ص 6):

https://ccdcoe.org/uploads/201810//NCSS-Guidelines_2013.pdf

54. «المستودع الوطني لإستراتيجيات الأمن السيبراني» الاتحاد الدولي للاتصالات 4 ،ITU مايو 2022:

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

55. «الإستراتيجية الوطنية للأمن السيبراني وخطة العمل 2020-2023»، وزارة النقل والشؤون البحرية والاتصالات في جمهورية تركيا، ص. 10.

56. «مؤشر الأمن السيبراني العالمي 2020»، ص 6-7.

57. «مؤشر الأمن السيبراني العالمي 2018» الاتحاد الدولي للاتصالات، 7 مايو 2022: (ص 13):

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.012018--PDF-E.pdf.

58. مؤشر الأمن السيبراني العالمي 2020»، ص 25.

59. «وصف المؤشرات» NCSI، بزيارة الموقع https://ncsi.ega.ee/indicators/ في 7 مايو 2022. تستند جميع مؤشرات NCSI إلى (1)تطوير سياسة الأمن السيبراني (2) تحليل ومعلومات التهديدات السيبرانية (3)التعليم والتطوير المهني (4)الإسهام في الأمن السيبراني العالمي (5)حماية الخدمات الرقمية (6)حماية الخدمات الأساسية (7)تحديد الهوية الإلكترونية وخدمات الثقة (8)حماية البيانات الشخصية (9)الاستجابة للحوادث السيبرانية (10)إدارة الأزمات السيبرانية (11)محاربة الجريمة السيبرانية. (12)العمليات العسكرية السيبرانية.

60. يصنف مؤشر الأمن السيبراني الوطني، حالة 160 دولة من حيث الأمن السيبراني، E-estonia، تاريخ الزيارة، 7 مايو 2022:

https://e-estonia.com/the-national-cyber-security-index-ranks-160-countries-cyber-security-status/.

61. تركيا، NCSI، تاريخ الزيارة، 7 مايو 2022، https://ncsi.ega.ee/country/tr/

62. أكاديمية الحوكمة الإلكترونية، 7 مايو 2022: https://ncsi.ega.ee/

63. جوليا فو، عرفان هيماني، سايمون جونز، وينونا ديسومبر، دانيال كاسيدي، أنينا شوارزنباخ، «مؤشر القوة الإلكترونية الوطنية 2020»، (2020)، 7 مايو 2022: (ص 1): https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

64. جوليا فو، وآخرون، «مؤشر القوة الإلكترونية الوطنية 2020»، ص 10.

65. جوليا فو، وآخرون، «مؤشر القوة الإلكترونية الوطنية 2020»، ص 37.

66. جوليا فو، وآخرون، «مؤشر القوة الإلكترونية الوطنية 2020»، ص 10.

67. جوليا فو، وآخرون، «مؤشر القوة الإلكترونية الوطنية 2020»، ص 12-11.

68. باركلي بالارد، «يبدو أن الجرائم السيبرانية كلفت العالم أكثر من 1 تريليون دولار في عام 2020»، Techradar، (15 فبراير 2021)، 8 مايو 2022: https://www.techradar.com/news/cybercrime-cost-the-world-over-dollar1-trillion-in-2020

69. بن راسل، «الجريمة الإلكترونية تصل إلى أعلى من 6 تريليونات دولار في عام 2021، وفقًا لمشروعات الأمن السيبراني»، NBCDFW، (19 مايو 2020)، 8 مايو 2022:

https://www.nbcdfw.com/news/tech/cybercrime-to-top-6-trillion-in-2021-north-texas-security-firm-says/2636083/.

70. «مؤشر الأمن السيبراني العالمي 2018»، ص 3. «مؤشر الأمن السيبراني العالمي 2017»، ص 4.

71. «مؤشر الأمن السيبراني العالمي 2018».

72. يمكن العثور على جميع اللوائح القانونية ذات الصلة على صفحة الويب الخاصة بمؤسسة تكنولوجيا الاتصالات والمعلومات (Mevzuat ،(BTK، تاريخ الزيارة، 8 مايو 2022، https://www.btk.gov.tr/kanunlar

73. «مؤشر الأمن السيبراني العالمي 2020»، ص 128.

74. «تركيا»، مؤشر الأمن السيبراني الوطني NCSI (2020)، 8 مايو 2022: https://ncsi.ega.ee/ee/country/tr/

75. جوليا فو، وآخرون، «مؤشر القوة الإلكترونية الوطنية 2020»، ص 12.

76. «تركيا»، مؤشر الأمن السيبراني الوطني NCSI.

77. «مؤشر الأمن السيبراني العالمي 2018»، ص 3. «مؤشر الأمن السيبراني العالمي 2017»، ص 4. «مؤشر الأمن السيبراني العالمي 2020»، ص 6.

78. أمين داشكين، «إستراتيجية الأمن السيبراني التركية: البنية والتشريعات والتحديات»، مجلة الاستخبارات والأمن السيبراني، المجلد 2، العدد 1، (يونيو 2019)، ص 15-17.

79. داشكين، «إستراتيجية الأمن السيبراني التركية، ص 19.

80. داشكين، «إستراتيجية الأمن السيبراني التركية، ص 16.

81. «مؤشر الأمن السيبراني العالمي 2020»، ص 8. «مؤشر الأمن السيبراني العالمي 2017»، ص 4. «مؤشر الأمن السيبراني العالمي 2018»، ص 3.

82. «الإستراتيجية الوطنية للأمن السيبراني وخطة العمل 2020-2023، ص 6.

83. «الإستراتيجية الوطنية للأمن السيبراني وخطة العمل 2013-2014»، وزارة النقل والشؤون البحرية والاتصالات في الجمهورية التركية، (2013)، 8 مايو 2022: (ص 21-46):

https://www.btk.gov.tr/uploads/pages/21--0-cyber-security-strategy-and-action-plan-20135-2014-a3412df707ab.pdf

84. أنصار شكر وإحسان براق طولغا، «المنظمة الوطنية للأمن السيبراني: تركيا»، مركز التميز للدفاع الإلكتروني التعاوني التابع لحلف الناتو 8 ،(2018) CCDCOE مايو 2022: (ص 9):

https://ccdcoe.org/uploads/2018/10/CS_organisation_TUR_112018_FINAL.pdf

85. شكر وطولغا، «المنظمة الوطنية للأمن السيبراني»، ص 10-15.

86. حاقان شنتورك، ج. زعيم جيل، شرف صاري أوغلو، "المجلة الدولية لعلوم أمن المعلومات»، المجلد 1، رقم 4 (2012)، 8 مايو 2022: (ص 118): https://dergipark.org.tr/tr/pub/ijiss/issue/16066/167876

87. «إحصاءات الإنترنت الحية».

88. «خريطة التهديدات الإلكترونية الحية».

89. «مؤشر الأمن السيبراني العالمي 2020» ص 13. «مؤشر الأمن السيبراني العالمي 2017»، ص 4.

90. «مؤشر الأمن السيبراني العالمي 2018» ص 3. «مؤشر الأمن السيبراني العالمي 2017»، ص 4.

91. «مؤشر الأمن السيبراني العالمي 2018» ص 19. «مؤشر الأمن السيبراني العالمي 2017»، ص 4.

92. «مؤشر الأمن السيبراني العالمي 2018» ص 3. «مؤشر الأمن السيبراني العالمي 2017»، ص 4.

93. شنتورك وآخرون، «تحليل الأمن السيبراني في تركيا»، ص 120.