سياسات الاستخبارات والأمن السيبراني في تركيا

أرسين جاهموت أوغلو*

ملخص: يتناول هذا البحث سياسات الاستخبارات والأمن السيبراني في تركيا، وهو موضوع مهمّ؛ لأن تركيا تتبوّأ موقعًا بين الدول المتطورة أو الآخذة في التطور التي تتعرض لمثل هذا النوع من التهديدات. ومن المعروف مثلًا أن مسؤولي الأمن الأعضاء في تنظيم غولن الإرهابي تمكّنوا من الحصول على بعض برامج التجسس، وإلى جانب ذلك شهدنا مؤخرًا قيام تشكيلات الاستخبارات العالمية وبعض منظّمات الجريمة الإلكترونية المنظّمة بهجمات سيبرانية ضد الدولة التركية وبعض المسؤولين رفيعي المستوى، وعندما نأخذ بعين الاعتبار أن التهديدات التي واجهتها تركيا والهجمات التي استهدفت أمنها الوطني حصلت في الفترة الأخيرة من خلال الفضاء السيبراني؛ يمكن الإدراك بأنه يجب على وحدات الدولة ذات الصلة أن تقوم بعمل جادّ في هذا الصدد.

* باحث، تركيا

The Policies of Intelligence and Cybersecurity in Turkey

ERSİN ÇAHMUTOĞLU*

ABSTRACT The following article deals with the policies of intelligence and cybersecurity in Turkey, especially because Turkey occupies a position among developed, or developing, countries that are exposed to such threats. It is known, for example, that the security officials affiliated with the Gulenist terrorist organization managed to get some of the spyware programs. In addition, we have recently witnessed the formation of global intelligence and some cybercrime organizations that organized cyber attacks against the Turkish state as well as against some high-ranking officials. Therefore, it can be seen that relevant State units must take serious actions in this regard, especially when we take into consideration the threats Turkey has faced and the recent attacks on its national security through cyberspace.

* Researcher, Turkey

رؤية تركية
2019 - (8/2)
59 - 43

المدخل:

غـدت الاسـتخبارات التـي تُعَـدّ نشـاطًا رئيسًا مـن حيث تأمـين الأمن الوطنـي للدول؛ عمـلًا أساسـيًّا لا يمكن الاسـتغناء عنـه -في العلاقـات الدولية في حـالات السلم والحرب- في تحقيـق الأمـن القومـي للـدول، إلى جانب الأمـن الداخلي. فالتاريخ شـهد ولايزال يشـهد أعمالًا اسـتخباراتيةً تُجمَع فيها البيانات كافة في حالات السلم، لاسـتعمالها في حالات الحرب، والحصول على بيانات جديدة عبر الطرق التقليدية أو الحديثة.

يمكننـا القـول إن الحصول عـلى المعلومات الاسـتخباراتية في فترات السلم أسـهل منه في فـترات الحرب وأيـسر، والفعاليات الاسـتخباراتية تكون أكثر إنتاجيةً في أوسـاط الأمن التي تتوفر في الفترات التي تسود فيها العلاقات الطيبة. وهذه الفعاليات الاستخباراتية تُسَيَّر بأدوات تختلف تبعًا لاختلاف شروط العصر. ورغم أن الاستخبارات الإنسانية (HUMINT) التي تُعـدّ أمّ الفعاليـات الاسـتخباراتية، تحافظ على أهميتهـا منذ العصور القديمـة، فإن الإمكانات التكنولوجيـة، مثـل (OSINT، وCOMINT، وSIGINT، وCYBINT) ينتـشر استعمالها يومًا بعد يوم [1].

إضافة إلى هذه الفعاليات الحديثة، هناك إنتاجٌ لاسـتخباراتٍ إسـتراتيجيةٍ أخذت مفهومها للمـرة الأولى عـلى يد أ.د.شرمـان كَنْت، وسياسـاتٍ شـاملةٍ طويلـة المدى، ضـدّ التهديدات الخارجيـة الموجودة/ المحتَمَلـة التي تهـدّد الأمنِ القومي. وهـذه الطريقة التي تُعـدّ في الغالب اسـتخبارات خارجية منذ فترة الحرب الباردة، أُسِّـست في جهاز الاسـتخبارات المركزية (سي آي إيه) الأمريكية، باعتبارها وحدة يعمل فيها كَنْت أيضًا، واسـتعملت في أعمالِ اسـتخباراتيَّةٍ رفيعـة المسـتوى. يعتقد كَنْت أن الاسـتخبارات الإسـتراتيجية التي لا تزال تتبـوّأ مكانةً مهمّةً في أجهـزة الاسـتخبارات العالميـة، ذات صلة بالسياسـات الخارجية التي تتبناهـا الدول، ولا يمكـن الاسـتغناء عنها. وممّا يشـير إلى هذه الأهميـة هذه العبارة التي سـجّلها كَنْـت في كتابه، بعنـوان (الاسـتخبارات الإسـتراتيجية): "إن كانت السياسـة الخارجيـة درع الجمهورية، فإن الاستخبارات الإستراتيجية أداةٌ تستعمل هذه الدرع في الوقت والمكان المناسبين" [2].

ويمكـن القـول إن الـدول في وقتنـا الحـاضر تتنـاول مـن جديـدٍ الفعاليـات المتعلقـة بالاسـتخبارات الإسـتراتيجية، وتعمـل على تطبيقها بالجمع بينها بأسـاليب أكثـر تكنولوجية (على غرار الاستخبارات السيبرانية)[3]. وقد تغيّرت التهديدات تغيّرًا كبيرًا في أنواعها وأبعادها وآلياتها، إثر انتشـار الإنترنت في السنوات الأخيرة على وجه الخصوص، واتساع مجال الفضاء السيـبراني الـذي يوصف بأنـه "بُعْدُ الحرب الخامـس" [4]. بالمقابل تنتج الدول سياسـاتها في هذا الإطار من خلال تطوير إستراتيجيات أمنية قومية. وهذه السياسات يمكنها أن تكون هجومية (ofansif) بقدر ما تكون دفاعية (defansif).

يأتي ظهور برنامج ستوكسنت (Stuxnet) الذي عطّل مئات أجهزة الطرد المركزي التي تستخدمها إيران في نشاطاتها النووية، من بين أهم الأسباب الداعية إلى تقييم الأمن السيبراني على أنه مسألة تهم الأمن القومي. ورغم أن أنظمة تشغيل المنشآت النووية مغلقةٌ على الشبكات الخارجية، فإن هذا الفيروس تسرّب نتيجة ضعف داخلي. وممّا يشير إلى وجود صناعة للأسلحة السيبرانية في العالم، برنامج ستوكسنت هذا، الذي يعدّ نشاطًا تجسّسيًّا ناجحًا، وسلاحًا سيبرانيًّا، يهدف إلى الإضرار الفيزيائي أكثر من الحصول على البيانات، بحجمه الصغير، وقدرته على إخفاء ذاته، وإمكانية توجيهه، (وإصابته نظامًا معيّنًا دون غيره)، ومحتوياته المعقدة [5].

ومن الجدير بالذكر أن تركيا تتبوّأ موقعًا بين الدول المتطورة أو الآخذة في التطور التي تتعرض لمثل هذا النوع من التهديدات. ومن المعروف على سبيل المثال أن مسؤولي الأمن الأعضاء في تنظيم غولن الإرهابي، تمكنوا من الحصول على برنامج التجسس (RCS) الذي يملك نظام التحكّم عن بعد، إثر إبرام اتفاقية مع شركة هاكنغ تيم [6] Hacking Team، عام 2011، مقابل تسديد مبالغ تجاوزت مليون ليرة تركية [7]. إلى جانب ذلك، شاهدنا في الأيام الأخيرة الأخبار التي تشير إلى قيام تشكيلات الاستخبارات العالمية، وبعض منظمات الجريمة الإلكترونية المنظمة- بهجماتٍ سيبرانيةٍ ضد الدولة التركية، وبعض المسؤولين رفيعي المستوى. وعندما نأخذ بعين الاعتبار أن التهديدات التي واجهتها تركيا والهجمات التي استهدفت أمنها الوطني حصلت في الفترة الأخيرة عبر الفضاء السيبراني، يمكن الإدراك بأنه يجب على وحدات الدولة ذات الصلة أن تقوم بعمل جاد في هذا الصدد.

الأمن الوطني التركي في فترة ما قبل حكومة حزب العدالة والتنمية:

طـوّرت تركيـا، كما هو الحال في الدول الأخرى، سياسـات مختلفةً في مجـال أمنها الوطني، وقامت بمراجعتها بصورةٍ دوريةٍ. لكن الكثير من سياسـات الأمن الوطني التي وضعتها قيد التنفيـذ، بقيـت في مرحلة الحرب الباردة وبعدهـا، ضمن الخطوط التي رسـمها حلف الناتو، بحكـم موقعها في هذا الحلف. ولم تكن هذه السياسـات مثمرةً، وظلت غير كافية لتوفير الأمن الوطني، ولاسيّما في أيـام الانقلابـات والاضطرابـات السياسـية المختلفة التي شهدتها.

مسؤولـو الأمـن الأعضـاء فـي تنظيـم غولن الإرهابـي تمكنـوا مـن الحصول علـى برنامج التجسس (RCS) الذي يملك نظام التحكّم عن بعد إثـر إبرام اتفاقية مـع شركة هاكنغ تيم Hacking Team، عـام 2011، مقابل تسديد مبالغ تجاوزت مليون ليرة تركية

كما أن السياسـات الموجّهة ضدّ التهديدات الداخلية والخارجيـة في مجـال الاسـتخبارات التـي تشـكّل أحـد المجـالات الأساسـية في الأمـن الوطنـي، لم تكـن كافيةً من أجل تركيـا، ولم تستطع الحكومـات المختلفة انتهاج إسـتراتيجياتٍ ناجحـةٍ في مكافحـة التهديـدات التـي واجهتهـا بسبـب موقعهـا الجيوسـياسي. وبـدلًا من ذلك، سـاد الشـعور بالحاجـة إلى تكثيف الاسـتخبارات الداخليـة أكثـر من الحاجـة إلى تصور التهديـدات الخارجية، ولاسـيّما في فترة الانقلابـات والمراحـل التي شـهدت الاضطرابـات السياسـية، واعتُقِد أن المخاطـر نابعة من الداخل، بل وأن أغلبها نابعة من الفروقات الأيديولوجية والاعتقادات الدينية.

والسبـب في عـدم انتهاج سياسـةٍ ضدّ التهديـدات الخارجيـة لا يقتصر على الاعتقـاد بكفاية الدراسـات الاسـتخباراتية التي يجريها حلف الناتو، والتي تقوم على تصور التهديدات التي تطال أمنه الذاتي، بل يتعداه إلى النقص الحاصل في البنية التحتية والإستراتيجية، نتيجة العجز عن متابعة التقنيات المتطورة والتهديدات المتغيرة، والفشل في خلق الوعي حول إنشاء بنية مؤسساتية من أجل تشكيل استخبارات خارجية متطورة. ولا ننسى أن الأعمال الإرهابية المختلفة الأكثر ضررًا للأمن الوطني، مهّدت الطريق أمام تركيز تركيا على التهديدات الداخلية. فالهجمات الإرهابية التي نفّذها حزب العمال الكردسـتاني منذ سنوات طويلة أضرّت بالأمن الوطني، إلى جانب الأضرار الكبيرة التـي أحدثتهـا في المجالين الاقتصـادي والاجتماعي. وكذلك الضعف الأمنـي الذي ظهر بسبب التقصير الذي أحدثه التنافس الناتج عن غياب الثقة بين المؤسسات الأمنية أحيانًا، وسوء التنظيم فيما بينها أحيانًا أخرى؛ وهذا أدى إلى ظهور المنظمات الإرهابية.

حكومة حزب العدالة والتنمية وسياسة الأمن الوطني:

وضـع حـزب العدالـة والتنميـة الـذي وصـل إلى السلطة عـام 2002 حدًّا للمشـكلات التـي ورثها من الفترات التي سـبقته، مثل الأحداث غير القانونية التـي وُصِفت بـ(المُظلمة)،

والشبكات الإجرامية المنظَّمَة، وجرائم القتل المجهولة. كما أجرى ترتيبات قانونية في مختلف المجالات، مثل: التنصّت، ومراقبة الخدمات الاستخباراتية للدولة، وعرقلة الاستخبارات، إضافة إلى السياسات الأمنية، مثل: مكافحة تمويل الإرهاب والتهريب.

غيّرت حكومات حزب العدالة والتنمية نموذج الأمن الوطني التركي، وأقدمت على خطواتٍ مهمّةٍ في طريق تطوير سياسات مكافئة لسياسات الأمن الوطني التي يطبّقها الكثيرُ من الدول المتطورة، وذلك من خلال الخطوات التي اتّخذتها لاحقًا لتطوير مهمّات ومسؤوليات مجلس الأمن القومي (MGK) الذي يُعدّ مخطِّط سياسة الأمن القومي، وإعادة هيكلتها. بالمقابل، شهدت بعض الفترات اضطراباتٍ بسبب الانتشار المتزايد للإرهاب الدولي، والتهديدات الداخلية والخارجية التي تعرضت لها تركيا، ووقفت بعض الزمر الداخلية، مثل تنظيم غولن الإرهابي -الذي كشف عن حقيقته في أزمة جهاز الاستخبارات الوطنية (MİT) عام -2012 عقبةً أمام عملية التحول الديموقراطي، وخطوات التطور في البلاد. ودفعت هذه العقبات حكومة حزب العدالة والتنمية إلى تطوير سياساتها في الأمن الوطني، واتخاذ خطوات من شأنها تحقيق الأداء الأمثل للمؤسسات الأمنية في الدولة. ويأتي في مقدمة هذه الخطوات، تفعيلُ سياسات مكافحة الإرهاب، والتنسيق بين المؤسسات الأمنية، وبناء هيكل مؤسساتيّ لحماية النظام العام. وبناءً على ذلك، أُسِّست مستشارية الأمن والنظام العام (KDGM) في بنية وزارة الداخلية عام 2010، وبدأ هذا الهيكل المؤسساتي بتقديم إسهاماته في هذا الموضوع.

علاوةً على ذلك، أُعِدّت أمثلة عن السياسات الأمنية في النظام الدولي، والترويج لهذه الخطوات بواسطة المنشورات المختلفة. والأهمّ من هذا كله، هو إصدار كتاب بعنوان (الوثائق الإستراتيجية الخاصة بمكافحة الإرهاب الوطني والعالمي)[8]، الذي أُعِدّ بغية الإسهام في سياسات الحكومة في مكافحة الإرهاب. فكانت هذه الدراسة وسيلةً لتطوير إستراتيجية مكافحة الإرهاب تعادل إستراتيجيات الدول الغربية، مثل الولايات المتحدة الأمريكية وإنكلترا وبلجيكا وهولندا، والمنظمات الدولية، مثل الاتحاد الأوربي والأمم المتحدة.

وإلى جانب الإصلاحات التي يتطلبها النموذج الأمني المتغير في تركيا، والتي تحقّقت خلال حكم حزب العدالة والتنمية، حصلت تطورات إستراتيجية تتماشى مع احتياجات تركيا، نذكر من أهمها الإصلاحات التي طالت مجال الاستخبارات. فعلى الرغم من ارتباط مستشارية جهاز الأمن الوطني برئاسة الوزراء، باعتبارها المؤسسة الوحيدة المنتجة لاستخبارات الدولة، فإنها لم تتمكن في أغلب الأحيان من إقامة علاقات سليمة مع الحكومة حتى عام 2005. ووصلت العلاقات بين جهاز الاستخبارات والسلطات السياسية المستوى المطلوب، وتحقّق التنسيق في الفعاليات حول الأمن الوطني، إثر تعيين أمره طانر في منصب المستشار سنة 2005، وإحداث تغييرات تشريعية من خلال إصدار بنود إضافية[9].

وبذلك تبنى جهاز الاستخبارات الوطنية مهمّةً استباقيةً، وعزّز من قدراته العملياتية، وقطع شوطًا كبيرًا في إنتاج استخباراتٍ إستراتيجيةٍ. وفي أعقاب هذه المرحلة الجديدة التي يمكن تعريفها بمرحلة (إنتاج استخبارات مواكبة للعصر)، استمر تطوير هذا الجهاز بعد تولّي حاقان فيدان منصب المستشار سنة 2010، حتى أخذت الفعاليات الاستخباراتية تصبح أكثر فعالية يومًا بعد يوم.

والتطور المهمّ الآخر الذي شهده مجال الاستخبارات هو العمل على جمع استخبارات الأمن الوطني في حوض واحد. إذ جُمِع بين عمل الاستخبارات التقنية، وفعاليات الاستخبارات الأخرى تحت سقفٍ واحدٍ، من خلال نقل القيادة العامة للأنظمة الإلكترونية (GESKOM) إلى بنية جهاز الاستخباراتٍ الوطنية في شهر كانون الثاني/ يناير من عام 2012، وذلك لزيادة كفاءة إنتاج الاستخبارات[10]. وبعد الانتقال إلى بنية جهاز الاستخبارات الوطنية، تطورت البنية التحتية التقنية للوحدة التي تحمل اسم دائرة استخبارات الإشارة، وهذه خطوة مهمّة رغم كون هذا النظام لا يعادل في أعماله التقنية تلك الأعمال التقنية التي تنفذها الأنظمة في الدول المتقدمة مثل الولايات المتحدة وإنكلترا.

ووفّرت حكومة حزب العدالة والتنمية الحماية القانونية لتعزيز الاستخبارات الوطنية، والوقاية من التهديدات كافة. فبعد عملية 7 شباط/ فبراير عام 2012 التي تُسمَّى أيضًا المحاولة الانقلابية الأولى لتنظيم غولن الإرهابي- بدأت دراسات شاملة بتوجيهٍ من رجب طيب أردوغان رئيس الوزراء آنذاك. إذ أُصدِر بند إضافي ملحق في تاريخ 17 شباط/ فبراير عام 2012، ينصّ على وجوب طلب الإذن من رئيس الوزراء في أمر التحقيق الذي يَطال فعاليات الاستخبارات الوطنية وعناصرها[11]. فكان ذلك عائقًا أمام الضعف الذي قد يصيب جهاز الاستخبارات نتيجة التحقيقات المبنية على إشعارات كاذبة أو أدلة غير ملموسة، والحدّ من نقاط الضعف الأمنية المحتملة، ومن ثَمّ حفظ الأمن القومي.

وهناك خطوة مهمّة أخرى في مجال إصلاح الاستخبارات من خلال التشريعات التي عرفت باسم قانون جهاز الاستخبارات الوطنية، التي صدرت في شهر نيسان/ أبريل عام 2014. فمن خلال وضع التشريعات المذكورة قيد التنفيذ بموجب القانون رقم 6532، تم القيام بترتيبات قانونية ذات صلة بمجموعة واسعة من شؤون جهاز الاستخبارات، ومن ذلك هيكليتها المؤسساتية، وفعالياتها الداخلية والخارجية، والحقوق الفردية، والأعمال الإستراتيجية[12].

وفقًا لهذه المواد خُطِّط لتنفيذ أعمال مكثفة في مجالات، مثل الاستخبارات الخارجية، واستخبارات التقنيات (الأمن السيبراني)، واختبار أساليب الاستخبارات المعاصرة؛ لزيادة قدرة الاستخبارات الأمنية الوطنية ونوعيتها، وتطوير الأنشطة الاستخباراتية من خلال متابعة التطورات التكنولوجية. كما أُشِير إلى زيادة انتشار التمركز المناطقي للاستخبارات

الأمنية في أنحاء البلاد كافة، بهدف التعامل مع الاستخبارات الفورية بشكل أسرع وأكثر صحة[13]. والتجديد الآخر الذي جاءت به التشريعات رقم 6532، هو إدراج وحدة إعاقة الاستخبارات في عملية الإصلاح والتطوير. وبحسب التعبير الوارد في التشريعات ذات الصلة؛ لا مفرّ من أن تتّخذ الاستخبارات الأمنية الوطنية خطوات في هذا الاتجاه، لتطوير أساليب تنظيمات الاستخبارات الدولية في الجاسوسية الموجّهة ضدّ تركيا في الفترة الجديدة التي نحن فيها بوساطة الإمكانات التقنية والبيئة السيبرانية[14].

كما يتطلب الأمر تطوير ساحة عمل لوحدة الاستخبارات الخارجية المرتبطة بجهاز الاستخبارات الوطنية، والقيام بنشاط استخباراتي مكثف، إثر الاضطرابات التي شهدتها الفترة الأخيرة على الصعيدين الإقليمي والدولي، والمخاطر الأمنية التي تتعرض لها الحدود التركية؛ بسبب النشاطات الإرهابية. وبسبب العلاقة القائمة بين الاستخبارات والسياسة الخارجية، كان الهدف من التشريعات الأخيرة إسهام الاستخبارات الوطنية في إنتاج السياسة الخارجية وممارستها، لتكون عملية صنع القرار أكثر سرعة وسلامة[15].

وضع حزب العدالة والتنمية الذي وصل إلى السلطة عام 2002 حدًّا للمشكلات التي ورثها من الفترات التي سبقته مثل الأحداث غير القانونية التي وُصِفت بـ(المُظلمة) والشبكات الإجرامية المنظَّمة وجرائم القتل المجهولة كما أجرى ترتيبات قانونية في مختلف المجالات

وفيما يتعلق بزيادة مهامّ جهاز الاستخبارات الوطنية وصلاحياته، وتوسيع نطاق أنشطته، وتوسيع الحقوق والحريات الفردية، تناولت التشريعات ذات الصلة بشكل واضح ضرورة أخذ المعايير الدولية بعين الاعتبار. ورغم توسيع نطاق مهام جهاز الاستخباراتِ الوطنية ومسؤولياته، فإنه في الوقت نفسه خاضعٌ للرقابة والتفتيش من قبل لجنة الأمن والاستخبارات التي أُنشِئت في مجلس الشعب التركي الكبير عام 2014. تتألف هذه اللجنة من سبعة عشر عضوًا، يمثّلون الأحزاب السياسية الأربعة الموجودة في المجلس، وتعقد اجتماعاتها في أوقات محددة. وهذه هي المرة الأولى التي أُنشِئت فيها آلية رقابة على مستشارية جهاز الاستخبارات الوطنية منذ تأسيسها، وفُتِح المجال أمام رقابتها من قبل مجلس الشعب التركي الكبير باعتباره ممثل إرادة الشعب[16].

سياسة حكومات حزب العدالة والتنمية في الأمن السيبراني:

أعدّت دول عديدة بحوثًا كثيرة في مجال الأمن السيبراني الذي يشكل أحد الأركان الأساسية للأمن الوطني، وعززت سياساتها بقفزات محددة. وإلى جانب القيام بالدراسات الاستخباراتية المتطورة في هذا المجال باستخدام إمكانات الفضاء السيبري[17](cyberspace) ، طُوِّرت إستراتيجيات لمكافحة التهديدات السيبرانية الوطنية والدولية. وأصدرت الجمهورية التركية أيضًا، وللمرة الأولى، في فترة حكومة حزب العدالة والتنمية، القانون رقم 5809 في عام 2005

باسم قانون الاتصالات الإلكترونية، في إطار أمن الاتصالات الذي يشكل جزءًا من الأمن السيبراني [18]. وبعد هذا القانون الصادر في بنية مؤسسة العلوم والتكنولوجية والاتصالات، والذي يتضمن التشريعات القانونية الموجهة ضد جرائم المعلومات والاتصالات الخليوية؛ أصبحت تركيا على بيّنة من أهمية موضوع أمن الاتصالات على وجه الخصوص، والأمن السيبراني على وجه العموم.

وفي الفترة اللاحقة، أقدمت تركيا على اتّخاذ قرارات مهمّة في هذا المجال، ولاسيّما بعد ظهور تهديدات سيبرانية عالمية، (مثل الهجوم السيبراني الكبير الذي تعرضت له إستونيا في عام 2007). وبناءً على القرار الصادر من مجلس الأمن القومي الذي يجتمع مرة كل خمس سنوات، والذي يعدّ وثيقة سياسة الأمن القومي، في تاريخ 27 تشرين الأول/ أكتوبر 2010، قُرِّر اعتبار التهديدات المحتملة من الفضاء السيبراني "تهديدًا للأمن الوطني"، وإدراج هذا الموضوع في الأجندات اليومية للدولة[19]. وكان واضحًا من خلال التصريح الصحفي الذي يعقب الاجتماعات ذات الصلة أن الأمن السيبراني أصبح أحد الموضوعات الرئيسة لاجتماعات مجلس الأمن القومي بعد ذلك التاريخ.

بعد القرارات الصادرة من مجلس الأمن القومي، قامت الحكومة بدايةً بدراسات ذات صلة بالأمن السيبراني، وتحديد السياسات حول الاحتياطات الواجب اتّخاذها. وأُسِّست هيئة الأمن السيبراني بالقانون رقم 3842 الصادر من قبل مجلس الوزراء في تاريخ 11 حزيران/

يونيو 2012، من أجل تطوير البنية التحتية السيبرانية، وتعزيز الأمن السيبراني الوطني في تركيا[20].

وحُدِّدت السياسات اللازمة للأمن السيبراني، بالتعاون بين الوزارات والمؤسسات الأمنية في ضوء القرارات التي تصدرها هيئة الأمن السيبري التي بدأت تجتمع مرتين سنويًّا اعتبارًا من تأسيسها، وتوسّع مستوى تمثيل الأعضاء في هيئة الأمن السيبراني، حتى صار بالإمكان تنفيذ الأنشطة بشكل أكثر كفاءة. تتألف هيئة الأمن السيراني من رئيس هيئة التحقيق في الجرائم المالية (MASAK)، ورئيس مؤسسة العلوم والتكنولوجيا والاتصالات، ورئيس مؤسسة البحوث العلمية والتقنية التركية TÜBİTAK، ورئيس قيادة أركان الاستخبارات الإلكترونية وأنظمة المعلومات، ومستشارين في جهاز الاستخبارات الوطنية، ومستشارين في الأمن والنظام العام، ومستشارين في وزارة النقل والملاحة والاتصالات، والدفاع الوطني، ووزارتي الداخلية والخارجية[21] .

كما توسّعت صلاحيات هيئة الأمن السيبري ومسؤولياتها، من قبيل تحديد سياسات الأمن السيبراني الوطني وتنفيذها وتنسيقها، من خلال البنود والمواد المختلفة التي أُلحِقت بها جراء التغييرات التي تمّت عام 2014. وفقًا لذلك، وُسِّعت مهامها لتغطي حماية البنى التحتية المحورية، ومراكز التدخل السيبراني، وتطبيقات إنتاج الحلول الوطنية وتطويرها، وأعمال التوعية والتعليم ذات الصلة بالأمن السيبراني[22].

تشكّلُ قيادة الدفاع السيبراني التي أُسِّست في بنية القوات المسلحة التركية عام 2013 للحماية من الهجمات السيبرانية– آليةً دفاعيةً إضافيةً داعمةً لقوات حفظ النظام لمكافحة التهديدات السيبرانية، في سبيل دعم الأمن الوطني في تركيا. وفي العام ذاته بدأت الجهود للتطبيق في المجال التنفيذي. وبموجب القرار الصادر من هيئة الأمن السيبراني، كُلِّفت وزارة النقل والملاحة والاتصالات بمهمّة إعداد وتنسيق خطة العمل والسياسة والإستراتيجية ذات الصلة بتعزيز الأمن السيبراني الوطني. حيث أُعِدّت خطة عمل وطنية توازي السياسات التي تطبقها الدول المتطورة، ووُضِّحت السياسات التي ستطبقها الحكومة؛ وذلك لأول مرة خلال تسلّم بن علي يلدرم منصبه الوزاري عام 2013 .[23] والنقطة الأهمّ في خطة العمل هذه هي إنشاء المركز الوطني للتدخل في حوادث الأمن السيبراني (USOM) في بنية رئاسة الاتصالات اللاسلكية، بغية التدخل في مواجهة التهديدات السيبرانية التي تهاجم البنية التحتية للإنترنت في تركيا[24]. وأسفر الاجتماع الأول لهيئة الأمن السيبراني عن شروع المركز الوطني للتدخل في حوادث الأمن السيبري نشاطاته في بنية مؤسسة العلوم والتكنولوجيا والاتصالات في 23 أيار/ مايو 2013. والهدف الآخر من إنشاء هذا المركز، هو توفير الاتصال والتنسيق بين قوات حفظ النظام والقطاع الخاص والمنظمات الدولية.

عـلاوة على ذلـك، يُحلّل المركز الوطنـي للتدخل في حوادث الأمن السيـبراني تحليلًا فوريًّا التهديـدات السيبرانيـة العالميـة، كما هـو الحـال لـدى "US-CERT" (United States-Computer Emergency Readiness Team) في الولايـات المتحـدة الأمريكيـة، و"UK-CERT" (United Kingdom-Computer Emergency Response Team) في إنكلترا، ويتوقّع نقاط الضعف المحتملة، ويتّخذ الاحتياطات والتدابير اللازمة، ويحذّر الجميع مؤسساتٍ وأفرادًا في سياق (البلاغ الآمن). كما يعمل على استعمال أنظمة النت المؤسـساتية للإبلاغ المستمرّ عن نقاط الضعف اليومية،، مثل مواقع النت الضارّة، وتطبيقات الخليوي الكاذبة (Android ve iOS)، وامتدادات فيشينغ أتّاك [25] (Phishing attack) المزيفة في البريد الإلكتروني، والثغرات الأمنية الحرجة في أنظمة النقل والاتصالات [26].

بـدأ المركـز الوطني للتدخل في حـوادث الأمن السيبراني USOM بالإسـهام الحقيقي في الأمـن السيـبراني الوطني في تركيا، بعـد أن دخل حيّز التنفيذ، وصان البنيـة التحتية السيبرانية مـن عدد كبـير من التهديـدات. وبفضل هذا المركز، كـان تأثير هجوم برمجة الفديـة العالمي [27] WannaCry الذي بدأ في تاريخ 12 أيار/ مايو 2017 على تركيا قليلًا بالمقارنة مع الدول الأخـرى [28] ؛ لأنه اسـتطاع أن يتنبّـأ بالأضرار التي يسببها التهديد المذكـور على نظام الويندوز المفتـوح، فأبلـغ الشركـات والمؤسـسات التـي من المحتمـل أن تكـون هي الهدف، عـبر نظام الإنترنت، وحال دون وقوع الأضرار الناجمة عن هذا التهديد.

وأُنشِـئَت كذلك فِرَق التدخل في حوادث الأمن السيبراني [29] (SOME) في بنية مؤسـسة العلـوم والتكنولوجيـا والاتصـالات، لتعمـل بالتنسيق مـع USOM. والهدف مـن الوحدة المنقسمـة إلى قسمين: فِرَق التدخل في حوادث الأمن السيبراني القطاعي والآخر المؤسـساتي- هـو توفير الإمكانية والقابلية لدى مؤسـسات الدولة أو القطاع الخـاص لحماية نفسها في حال تعرّضهـا لتهديد سـيبراني فـوري. ويجري إعـداد دليل توجيهي لحمايـة وتنظيم البنيـة التحتية السيبرانية من قبل فرق التدخل في حوادث الأمن السيبري [30] .

كما أُعِدّت خطة عمل الأمن السيبراني من قبل هيئة الأمن السيبراني عام 2013، وحُدِّثت تحـت عنوان (خطة عمل اسـتراتيجية الأمـن السيـبراني 2016-2019)، ونشرها في الجريدة الرسمية بتاريخ 19 تموز/ يوليو 2016 . [31] وشملت هذه الأعمال تقديم التقييمات في مجالات واسـعة، مثل: مجـالات التغطيـة المتقدّمة للفضـاء السيـبراني، والتهديدات اليوميـة والدائمة، والمصطلحـات الخاصة بالأمن السيبراني، والبنى التحتية المحورية والجوهرية، والهجمات التي تركـز على الهـدف، وأمن المعلومـات، والتجسس السيبراني، وأعمال البحـث والتطوير -AR GE وإنتاج الحلول، ودورات التوعية الوطنية [32].

لقـد شـهدت تركيا تطورًا مهمًّا في مجـال الأمن السيبراني في إطار التعـاون الدولي. فدخلت في عضوية مركز التكامل في الدفاع السيبراني في إسـتونيا (CCDCOE) في 3 تشرين الثاني/

نوفمبر 2015، وحصلت على إمكانية المشاركة المباشرة في أعمال المركز. ويُعتقد أن زيارة رئيس الجمهورية رجب طيب أردوغان إلى مقر CCDCOE خلال زيارته إلى إستونيا في 23 تشرين الأول/ أكتوبر عام 2014، كان لها أثر كبير في العضوية المذكورة [33].

أُسِّس مركز التكامل في الدفاع السيبراني (CCDCOE) في مدينة تالين في إستونيا في بنية حلف الناتو، ويقدّمُ -إلى جانب التنسيق الأمني السيبراني في حلف الناتو والدول الأعضاء فيه- خدمات التدريب للدول الأعضاء، وإجراء تطبيقات في مجال الأمن السيبراني بشكل دوريٍّ كل عام، وإنتاج إستراتيجيات موجهة للتهديدات السيبرانية اليومية. ومن أهم إنجازات المركز، نشره كُتيِّبًا بعنوان (تالين)، الذي أُعِدّ وفقًا للقواعد القانونية التي ستُتَّبَع في حال تعرض الدول لهجوم سيبراني، رغم أنه لا يحمل صبغة رسمية [34].

تشكّل قيادة الدفاع السيبراني التي أُسِّست في بنية القوات المسلحة التركية عام 2013 للحماية من الهجمات السيبرانية- آليةً دفاعيةً إضافيةً داعمةً لقوات حفظ النظام لمكافحة التهديدات السيبرانية في سبيل دعم الأمن الوطني في تركيا

وعقدت اللجنة التنفيذية للصناعات الدفاعية اجتماعًا في مستشارية الصناعات الدفاعية (SSM)، برئاسة رئيس الوزراء بن علي يلدرم في 29 تشرين الأول/ أكتوبر 2016، واتّخذت قرارات في الأمن السيبراني، والأعمال المتعلقة بسياسات الصناعة الدفاعية الوطنية[35]. وفي إطار البرنامج المسمّى ببرنامج مركز تحليل الجريمة السيبرانية SİSAMER، تقرَّر إحداث مركز عمليات الدفاع السيبراني في بنية القوات المسلحة التركية إلى جانب منح الصلاحيات لمستشارية الصناعات الدفاعية. وينتظر من المركز المذكور الذي أُنشِئَت بنيته التحتية التكنولوجية بإشراف مؤسسة الهندسة والتقنية الدفاعية (STM)، أن يتصدّى للهجمات التي تستهدف الأمن السيبري الوطني لحظة وقوعها.

وفي شهر تشرين الثاني/ نوفمبر من نفس العام، أصدر رئيس الجمهورية تعليماته إلى هيئة الرقابة العامة (DDK) بإجراء بحث في تطبيقات الأمن السيبراني في العالم، وبيان نواقص تركيا في هذا الموضوع، وتقديم الحلول لتدارك تلك النواقص. فكان من الضروري قيام المؤسسات والمنظمات الموجودة في الخارج والجامعات بالالتقاء مع المؤسسات الخاصة التي تعمل في مجال الأمن السيبراني بعد تحديد الوضع القائم لتركيا، ثم بيان المقترحات اللازمة[36]. وقد تمّ تناول موضوع الأمن السيبراني في الأعمال السابقة لهيئة الرقابة العامة (DDK). ففي التقرير رقم 2013/ 3 في تاريخ 21 تشرين الثاني/ نوفمبر 2013 المعدّ في هذا الإطار، قُدِّمت مقترحات واسعة النطاق، ومنها البنى التحتية المحورية، والبيانات الحساسة، وتجارب أمن المؤسسات العامة، والتوعية في أمن المعلومات العامة. ويؤكد الجزء الأخير من التقرير المذكور أن المؤسسات العامة في عموم تركيا تشهد مشكلات أمنية مهمّة ناجمة عن البنية التحتية المحورية

والضعف الفردي الخطير. ويتوقف التقرير عند أهمية تنظيم تدريبات تهدف إلى رفع مستوى الوعي والخبرة لدى الأفراد[37]. وهناك عمل آخر أُعِدَّ في الفترة القريبة الماضية، يعرض أهمية توفير الأمن السيبراني العام. حيث وُقِّع على التعميم المنشور في الصحف الرسمية في تاريخ 3 كانون الأول/ ديسمبر 2016 حول ضمّ الهيئات والمؤسسات العامة إلى الشبكة الافتراضية العامة[38] (Kamunet)؛ من قبل رئيس الوزراء بن علي يلدرم، وإبلاغه المؤسسات المعنية[39]. وهكذا تحقّق الاتصال بين المؤسسات العامة ضمن شبكة أكثر أمنًا، وبدأ العمل على توفير شبكة اصطناعية أكثر أمنًا في وجه الهجمات السيبرانية، تكون الاتصالات المعنية وتبادل البيانات فيها محجوبة عن النت.

أُسِّس مركز التكامل في الدفاع السيبراني (CCDCOE) في مدينة تالين في إستونيا في بنية حلف الناتو ويقدّمُ -إلى جانب التنسيق الأمني السيبراني في حلف الناتو والدول الأعضاء فيه- خدمات التدريب للدول الأعضاء وإجراء تطبيقات في مجال الأمن السيبراني بشكلٍ دوريٍّ كل عام

وقد تحدّث بن علي يلدرم في المؤتمر الوطني المعلوماتي الذي نظمته الجمعية المعلوماتية التركية (TBD) في تاريخ 8 كانون الأول/ ديسمبر 2016 حول الشبكة الافتراضية العامة، فذكر أن السياسة التي تطبّقها الحكومة فيما يخصّ الأمن السيبراني سُتراجع في الفترة القادمة. وفي هذا السياق، قَيّمَ الأمن السيبراني الوطني الحالي، وطرحَ أفكاره حول تعزيزه في المستقبل قائلًا: "غدت مسألة الأمن السيبراني اليوم مسألة أمن الوطن، وعلينا أن نقطع أشواطًا في هذا المجال، ونخطو خطوات نحو الحلول المحلية والوطنية بحلول عام 2017"[40].

وجاءت التوضيحات المفصّلة حول برنامج الشبكة الافتراضية العامة في التقرير (الريبورتاج) الذي قدّمه وزير النقل والملاحة والاتصالات أحمد أصلان إلى صحيفة ميلّيَّت، حيث بيّن أن الهدف من المشروع هو وضع حركة البيانات والاتصالات بين المؤسسات العامة في ظروف آمنة، وأشار إلى أنه من المخطّط ضمّ جميع المؤسسات في هذا الإطار حتى نهاية عام 2017. كما ذكر أصلان أن أحد أهم أهداف المشروع هو تطوير خوادم الشبكة الخاصة للشبكة الافتراضية العامة KamuNet من خلال جهاز التشفير الوطني أو مفاتيح التشفير[41].

بعد خطة عمل الدفاع السيبراني الأولى التي أعدّتها تركيا عام 2013، بدأت تُقدِم على خطوات حقيقية، فاتّخذت الاحتياطات الشاملة لمواجهة التهديدات السيبرانية الوطنية والدولية، حتى أصبحت دولة أكثر أمنًا في مجال الفضاء السيبراني الوطني مقارنة بالفترات الماضية. وطوّرت تركيا آليات الدفاع السيبراني من خلال إنشاء كيانات، مثل المركز الوطني للتدخل في حوادث الأمن السيبري (USOM)، وفرق التدخل في حوادث الأمن السيبري (SOME). ولو أخذنا بالحسبان أن تركيا كانت من بين الدول الضعيفة في مجال الدفاع السيبراني حتى عام 2013، لأمكننا التخمين بأنها ستكون في وضع أفضل في الفترة الجديدة[42].

الخاتمة:

ينبغي أن تواكب الجهود المبذولة لضمان الأمن الوطني التغيراتِ المستمرةَ التي تشهدها التهديدات الداخلية والخارجية. فاتساع نطاق الفضاء السيبراني، جرّاء تطور التكنولوجيا، وانتشار النشاطات الإرهابية في هذا المجال، يمهّدان الطريق أمام ولادة الإرهاب السيبراني. فنرى منظمات إرهابية مثل داعش تستعمل عناصرها في المجال السيبراني من أجل إطلاق دعايات منظمة، وشنّ هجوم على أهدافها المختارة من الدول أو المنظمات الدولية [43].

كما أن ضعف الوعي بالمجالات التي يمكن للإرهاب أن يمتد إليها، يشكل اليوم نقاط ضعف أمنية. فهجوم ستوكسنت Stuxnet في إيران حدث نتيجة ضعف الموظّف، وهذه الحقيقة يمكنها أن تكون بمثابة درس مهمٍّ في موضوع ضعف وعي الأفراد والمجتمعات بالأمن السيبراني وأمن البيانات الحساسة [44]. والهجمات التي شهدتها الفترات اللاحقة، مثل رد أكتوبر Red October وفلام Flame ودوكو Duqu بصفتها مثالاً على (التهديدات المستمرة المتطورة)- تُعدّ من مشكلات الأمن السيبراني المهمّة [45] .

انطلاقًا من هذه النقطة، ومع الأخذ بعين الاعتبار هذه الأنواع من التهديدات، يُنْتَظَر من إستراتيجية الأمن الوطني التي ستُنشَأ في الفترة القادمة أن تكون أكثر شمولية. ففي هذا السياق، جاء المسؤولون في حكومة حزب العدالة والتنمية على ذكر إعادة هيكلة الاستخبارات، ولاسيّما بعد محاولة 15 تموز 2016 الانقلابية، وبدأت الإجراءات المطلوبة في المؤسسات ذات الصلة[46]. والاحتمال قائم للتركيز أكثر على الأعمال الكريبتولوجية عقب حلِّ جهاز الاستخبارات الوطنية برامجَ الاتصال التي اعتمدها تنظيم غولن الإرهابي، مثل برنامجي بايلوك ByLock وإيغلا Eagle، وتأسيس رئاسة الاستخبارات الخارجية الموجودة في بنية جهاز الاستخبارات الوطنية، باعتبارها مؤسسة منفصلة، مثل (سي آي أي، وام 16)، واقتصار مسؤولية جهاز الاستخبارات الوطنية على الاستخبارات الداخلية فقط.

ويُتَوَقَّعُ في الوقت ذاته أن يُؤسَّس مجلس استخبارات تابع لرئاسة الجمهورية، تمامًا مثل مديرية الاستخبارات الوطنية بالولايات المتحدة الأمريكية، وأن يعمل جهاز الاستخبارات الوطنية وأجهزة الاستخبارات الأخرى، تحت تنسيق هذا المجلس الذي يعمل عمل (السقف). ومع تشكيل حوض يضمّ الاستخبارات الأمنية الوطنية، ستُتَّخَذ القرارات في الإستراتيجيات الأمنية بصورة أكثر فاعلية. ومن الممكن أن تغدو مستشارية الأمن والنظام العام (KDGM) التي لا تقوم بوظيفة عملية بحسب التشريعات الحالية؛ واحدةً من المؤسسات الفاعلة في إنتاج الاستخبارات الإستراتيجية، إثر دخول حزمتها الإصلاحية الاستخباراتية الجديدة حيّز التنفيذ، وأن تكتسب قدرات عملية مثل (الأمن السيبراني) بالمعنى الفني، بمقتضى جملة من الترتيبات القانونية.

وسيكون إنشاء بنية مؤسساتية تعادل أجهزةً مثل NSA[47] و GCHQ[48] وCSE[49] مهمّةً في مجال الاستخبارات الحديثة. وهذا النوع من الأجهزة الموجودة لدى الدول المتقدّمة خاصّةً تقوم ببحوث مميّزة في مختلف المجالات، مثل الاتصالات والكريبتولوجيا واستخبارات الإشارة، والأمن السيبراني: (أمن المعلومات، أمن البيانات الحساسة، أمن البنى التحتية الحرجة). وقد خطا GCHQ خطوةً نموذجيةً في هذا الاتجاه، فأنشأ في الأشهر الماضية وحدة بنية تحتية أسماها المركز الوطني للأمن السيبراني (NCSC)، الذي يُجري بحوثًا في أمن المعلومات والبيانات الحساسة[50]. فتم بذلك إعداد أرضية عمل أكثر فاعلية في مجال الأمن السيبراني الذي يشهد تغييرًا كبيرًا في تهديداته وساحات انتشاره.

كما يتمّ في هذه المؤسسات إحداث برامج توعية في الأمن السيبراني. فمن المعروف أن أكبر التهديدات السيبرانية التي تتعرض لها تركيا نابعة من مشكلة الوعي وغياب التوعية في هذا المجال[51] . ومن ثَمّ ينبغي سدّ هذه الثغرة، والتوعية في إطار أمن المعلومات في تركيا، ولاسيّما في أعمال المؤسسات الحساسة (بغضّ النظر عن التسلسل الهرمي). وتجدر الإشارة إلى أن الحصول على البيانات الحساسة للمؤسسات تتمّ بطريقة هجمات سيبرانية مختلفة تُدعَى (الهندسة الاجتماعية) [52]، تستهدف المؤسسات المغلقة على الشبكة الخارجية [53].

إضافة إلى الاهتمام بمثل هذا النوع من التهديدات، ينبغي الاهتمام الجاد بالبنية التحتية للنت، والبنى التحتية الحساسة، مثل: أنظمة الماء، والكهرباء، والغاز، والمدن الذكية، والمصارف، والمشافي. كما ينبغي أخذ الاحتياطات اللازمة قبل فوات الأوان من أجل أمن ما يسمى إنترنت الأشياء[54] (Internet of Things) ، وأمن الأنظمة الذكية التي يُتَوَقّع أنها ستصل إلى أربعة أضعاف عدد سكان العالم الحالي بحلول عام 2020. و يأتي في مقدمة الخطوات الكبرى التي ينبغي اتخاذها في هذا المجال- توطين الإنتاج وأعمال البحث والتطوير المتقدمة. وتجدر الإشارة هنا إلى الأعمال التي قامت بها الدولة في الفترة الأخيرة في هذا المجال، ولاسيّما في مجال الصناعة الدفاعية.

ومن المعروف أيضًا أن قضية الأمن الوطني من أهمّ القضايا التي تتّخذ مكانًا لها بين إستراتيجيات الجمهورية التركية الطويلة الأمد. ومتابعة البحوث، والأساليب الأمنية الحديثة، وخلق الوعي بالتهديدات المتغيرة، ومن ثَمّ تحديد سياسات مهمّة جدًّا أكثر فعالية من أجل تحقيق أهداف حكومة حزب العدالة والتنمية لعامي 2023 و2071.

الهوامش والمصادر :

1. OSINT: Open Source Intelligence, COMINT: Communication Intelligence, IMINT: Imagery Intelligence, SIGINT: Signal Intelligence, CYBINT: Cyber Intelligence.
2. شرمان كَنْت، الاستخبارات الإستراتيجية، (المترجم: كمال أق قايا)، مطبعة أندوستري، أنقرة 1968، ص6.

3. تتم استخبارات الأمن القومي للدول عن طريق الفضاء السيبراني للفعاليات الاستخباراتية التي تسيّرها المؤسسات الخاصة بغية الحصول على الضرائب التجارية. كما يُستعمَل مفهوم الاستخبارات السيبرانية من أجل المعلومات التي تتضمن تقييمات ومقترحات حول التهديدات السيبرانية المحتملة.
4. غوكهان بيرقدار، "الاستخبارات السيبرانية: مطلب جديد من متطلبات البعد الخامس للحرب"، مجلة الإستراتيجيات الأمنية، الإصدار 10، العدد 20، ص120 - 147.
5. شيدا توركاي، "حقوق الحرب السيبرانية ومعضلة التطبيق"، مجموعة كلية الحقوق في جامعة إسطنبول، الإصدار 71، العدد 1، 2013، ص1177-1228.
6. هاكيكنغ تيم Hacking Team شركة للبرمجيات، مقرها إيطاليا، يَعدّها المتخصصون شركةً تنتج برمجياتٍ لأهداف الاستخبارات السيبرانية تمامًا مثل Gamma Group، وAmesys، وTrovicor.
7. "أتلاي جان ثعلب باي لوك"، جريدة صباح، 12 تشرين الثاني/ نوفمبر 2016.
8. مستشارية الأمن والنظام العام، الوثائق الإستراتيجية الخاصة بمكافحة الإرهاب الوطني والعالمي، منشورات KDGM، أنقرة 2013.
9. انظر: قانون جهاز الاستخبارات الوطنية وخدمات استخبارات الدولة رقم 2937، (البند الإضافي: 5397 من المادة الثالثة - 03. 07. 2005).
10. "القانون رقم 6532..."، جهاز الاستخبارات الوطنية، https://www.mit.gov.tr، (تاريخ زيارة الموقع: 11 آذار/ مارس 2017).
11. انظر: القانون رقم 2937، المادة 26 - (التعديل: المادة 1/ -6278 17. 02. 2012).
12. "قانون جديد خاص بجهاز الاستخبارات الوطنية"، ملّيّت، 17 نيسان 2014.
13. انظر: القانون رقم 6532، "مقاومة الاستخبارات والاستخبارات الخارجية"، (الملحق: المادة 1/ 6532 - 17. 04. 2014).
14. انظر: القانون رقم 2937، المادة 6 - (البند الأول المعدّل: المادة 3/ -6532 17. 04. 2014).
15. "القانون رقم 6532..."، جهاز الاستخبارات الوطنية، https://www.mit.gov.tr، (تاريخ زيارة الموقع: 16 شباط/ فبراير 2017).
16. "حول لجنة الأمن والاستخبارات"، مجلس الشعب التركي الكبير، https://komisyon.tbmm.gov.tr، (تاريخ زيارة الموقع: 18 شباط/ فبراير 2017).
17. الفضاء السيبراني (cyberspace) هو الاسم الذي يطلق على الوسط الذي تجتمع فيه جميع شبكات وأنظمة المعلوماتية حول العالم وتتفاعل فيما بينها. وفي العمليات الحربية العسكرية يُستعمَل مفهوم الفضاء السيبراني بأنّه البعد الخامس بعد البعد البري والبحري والجوي والفضائي.
18. "قانون الاتصالات الإلكترونية"، الصحيفة الرسمية، https://www.resmigazete.gov.tr، (تاريخ زيارة الموقع: 14 شباط/ فبراير 2017).
19. "الاجتماع الذي عقد بتاريخ 27 تشرين الأول/ أكتوبر 2010"، الأمانة العامة لمجلس الأمن القومي، https://www.mgk.gov.tr، (تاريخ زيارة الموقع: 18 شباط/ فبراير 2017).
20. "هيئة الأمن السيبراني"، مؤسسة العلوم والتكنولوجيا والاتصالات، https://www.btk.gov.tr، (تاريخ زيارة الموقع: 18 شباط/ فبراير 2017).
21. "هيئة الأمن السيبراني"، مؤسسة العلوم والتكنولوجيا والاتصالات، https://www.btk.gov.tr، (تاريخ زيارة الموقع: 21 أيلول/ سبتمبر 2017).
22. "قانون رقم 6518 بتاريخ 06. 02. 2014"، الصحيفة الرسمية، https://www.resmigazete.gov.tr، (تاريخ زيارة الموقع: 28 آذار/ مارس 2017).
23. "إستراتيجية الأمن السيبراني الوطني وخطة عمل 2013 - 2014"، مؤسسة العلوم والتكنولوجيا والإتصالات، https://www.btk.gov.tr، (تاريخ زيارة الموقع: 16 نيسان/ أبريل 2017).
24. أُغلِقت مؤسسة العلوم والتكنولوجيا والاتصالات في 15 تموز 2016 بموجب القرار الذي اتخذه مجلس رئاسة الوزراء بعد انقلاب 15 تموز الذي نفّذه تنظيم غولن الإرهابي، وضُمَّ مركز التدخل في حوادث الأمن السيبراني (USOM) إلى مؤسسة العلوم والتكنولوجيا والاتصالات.
25. فيشينغ أتّاك Phishing attack: نوع من الهجمات السيبرانية، يأتي بمعنى هجوم التصيّد. فالفيروس

الذي يتسرّب إلى النظام المستهدف بواسطة ملفات أو امتدادات مزيفة عبر البريد الإلكتروني يشفّر البيانات ويطلب الفدية أو يعمل في النظام باعتباره برمجة جاسوسية.

26. مركز التدخل في حوادث الأمن السيبراني (USOM)، https://www.usom.gov.tr، (تاريخ زيارة الموقع: 22 أيار/ مايو 2017).

27. برمجة الفدية هذه (ransomware) المعروفة بأسماء من قبيل WannaCry أو WanaCrypt0r أو WanCry، والتي تأثرت منها حوالي 150 دولة حول العالم، تشفّر الأنظمة التي تطالها، وتطلب فدية تتراوح بين 300 إلى 600 دولار لفك الشيفرة. هذا النوع من الفيروسات التي تشكل تهديدًا سيبرانيًّا عالميًّا، تظهر بأسماء مختلفة، وتستمر في كونها تهديدًا أمنيًّا. من أجل معلومات أوفى، انظر: "Large-Scale Petya Ransomware Attack in Progress, Hits Europe Hard", Trend Micro ، 27 حزيران/ يونيو 2017، (تاريخ زيارة الموقع: 21 أيلول/ سبتمبر 2017): https://blog.trendmicro.com/trendlabs-security-intelligence/large-scale-ransomware-attack-progress-hits-europe-hard/?_ga=2.83339794.566050990.150744935074.1502645555-2645555.

28. "مؤسسة العلوم والتكنولوجيا والاتصالات: مركز التدخل في حوادث الأمن السيبراني اكتشف العجز وعمل على الوقاية من الأضرار"، مؤسسة العلوم والتكنولوجيا والاتصالات، BTK، https://www.btk.gov.tr، (تاريخ زيارة الموقع: 17 أيار/ مايو 2017).

29. "مركز التدخل في حوادث الأمن السيبراني وفرق التدخل في الحوادث السيبرانية المؤسساتية"، مؤسسة العلوم والتكنولوجيا والاتصالات، BTK، https://www.btk.gov.tr، (تاريخ زيارة الموقع: 18 شباط/ فبراير 2017).

30. وزارة النقل والملاحة والاتصالات- المديرية العامة للاتصالات، فِرَق التدخل في الحوادث السيبرانية المؤسساتية: تأسيسها ودليل إدارتها، أنقرة، تموز/ يوليو 2014.

31. "إستراتيجية الأمن السيبراني الوطني خلال الأعوام 2016 - 2019"، وزارة النقل والملاحة والاتصالات، https://www.udhb.gov.tr، (تاريخ زيارة الموقع: 17 شباط/ فبراير 2017).

32. "إستراتيجية الأمن السيبراني الوطني خلال الأعوام 2016 - 2019".

33. "زيارة أردوغان المحورية من أجل الأمن السيبراني"، نشرة سيبرانية، https://siberbulten.com، (تاريخ زيارة الموقع: 13 آذار/ مارس 2017).

34. Tallinn Paper: The Law of Cyber Targeting, CCDCOE, https://ccdcoe.org/multimedia/tallinn-paper-law-cyber-targeting.html, (accessed date: 11 February 2017); In order to get its Turkish version which have been translated by National Security Council, look at: National Security Council. https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakk-nda-tallinn-el-kitab-(uluslararas-siber-guevenlik-hukuku#, (accessed date: 17 February 2017

35. "البيان الصحفي لاجتماع اللجنة التنفيذية للصناعات الدفاعية"، مستشارية الصناعات الدفاعية، SSM، https://www.ssm.gov.tr، (تاريخ زيارة الموقع: 19 شباط/ فبراير 2017).

36. "رئيس الجمهورية أردوغان أصدر تعليماته"، خبر 7، https://www.haber7.com.tr، (تاريخ زيارة الموقع: 14 أيار/ مايو 2017).

37. "تقييم الأوضاع المحلية والدولية المتعلقة بحماية البيانات الشخصية، وأعمال الرقابة التي أُنجِزت في إطار الأمن المعلوماتي وحماية البيانات الشخصية"، الموقع الرسمي لرئاسة الجمهورية التركية/ هيئة الرقابة العامة، https://www.tccb.gov.tr، (تاريخ زيارة الموقع: 11 أيار/ مايو 2017).

38. "Kamunet(الشبكة الافتراضية العامة)"، وزارة النقل والملاحة والاتصالات، (تاريخ زيارة الموقع: 2 نيسان/ أبريل 2017): https://www.udhb.gov.tr/doc/siberg/KamuNetweb.pdf.

39. "ضم المؤسسات والهيئات العامة إلى Kamunet"، صحيفة رسمية، https://www.resmigazete.gov.tr، (تاريخ زيارة الموقع: 16 شباط/ فبراير 2017).

40. "حزب العدالة والتنمية"، تويتر، 8 كانون الأول/ ديسمبر 2016، https://www.twitter.com/

Akparti، (تاريخ زيارة الموقع: 11 نيسان/ أبريل 2017).

41. "درع افتراضي حول المؤسسات العامة"، ملِّيَّت، 12 حزيران/ يونيو 2017.

42. حاقان حكيم، وأوغوزهان باشي بيوك، "الجرائم السيبرانية وإستراتيجيات تركيا في مجال الأمن السيبراني"، مجلة الأمن الوطني والإرهاب، الإصدار 4، العدد 2، 2013، ص135-158.

43. James Scott ve Drew Spaniel, "The Anatomy of Cyber Jihad", Institute for Critical Infrastructure Technology (ICIT), https://icitech.org/icit-brief-the-anatomy-of-cyber-jihad-cyberspace-is-thenew-great-equalizer, (accessed date: 15 May 2017).

44. لو أخذنا بعين الاعتبار أن الفيروس Stuxnet ينتقل إلى النظام عن طريق (فلاشة)، لأمكننا القول إن هذا الوضع ناجم عن ضعف الموظف.

45. مراد أقين، وشرف صاري أوغلو، "التهديدات المستمرة المتطورة"، كتاب التبليغات الخاصة بالمؤتمر الدولي التاسع للكريبتولوجيا والأمن المعلوماتي، (مجلة الأمن المعلوماتي، تشرين الأول/ أكتوبر 2016)، ص79 - 87.

46. "إشارة من أجل هيكلة الاستخبارات"، وطن، 2 آب/ أغسطس 2016.

47. وكالة الأمن الوطني (National Security Agency): أُسِّست عام 1952 في الولايات المتحدة الأمريكية.

48. مقر الاتصالات الحكومية (Government Communications Headquarters): أُسِّس عام 1946 في المملكة المتحدة، ويعمل في الغالب في مجال الاستخبارات الإلكترونية.

49. هيئة أمن الاتصالات (Communications Security Establishment): أُسِّست عام 1946 في كندا.

"Britain to Enter New Era of Online Opportunity", NCSC, https://www.ncsc.gov.uk, (accessed date: 18 February 2017).

50. "تقرير حول وضع التهديدات السيبرانية للفترة تشرين الأول/ أكتوبر- كانون الأول/ ديسمبر 2016"، STM، (تاريخ زيارة الموقع: 22 كانون الثاني/ يناير 2017):

51. https://www.stm.com.tr/documents/file/Pdf/Siber %20Tehdit %20Durum %20Raporu %20Ekim- %20Aral %C4 %B1k %202016.pdf

52. هجمات الهندسة الاجتماعية طريقة للحصول على المعلومات المهمّة وغير المهمّة عبر التواصل مع أشخاص في وحدات الاتصالات المؤسساتية، وانتهاز الضعف الشخصي.

53. حاقان يشار، "التهديدات الموجهة للأمن السيبراني المؤسساتي والتدابير الوقائية منها"، مجلة العلوم والتكنولوجيا/ جامعة دوزجه، الإصدار 3، العدد 2، 2015، ص 488 - 507.

54. إنترنت الأشياء (Internet of Things): اسم يطلق على كافة الأشياء القادرة على أخذ المعلومات وتوجيهها، والتواصل مع الماكينات أو الأشخاص.