الفصل التاسع

الحروب السايبريَّة

يُمثِّل العالَم الرقمي بيئة جديدة على العالَم الحقيقي في التعاطي مع المعلومات، وقد أصبح هذا العالم الرقمي فضاءً متكاملًا له معطيات يَتم من خلالها التفاعُل معه، وبعد أن تحوَّل إلى بيئة رسميَّة معتَمَدة، أصبح هذا العالَم الرقمي يُعرَف باسم **الفضاء السايبري** Cyberspace، ويُعرَّف هذا الفضاء بأنه البيئة الافتراضيَّة التي يَتم فيها تَبادُل المعلومات الرقميَّة عبر شبكات حاسوبيَّة، ويُمكِن تَصوُّر الفضاء السايبري كمجموعة ضخمة من شبكات الأنظمة الحاسوبيَّة المتَّصلة مع بعضها، ومثلما تَقَع حروب تقليديَّة في عالَم الواقع (كالتي تَحدُث في البر، والبحر، والجو، والفضاء) تَقَع حروب افتراضية في الفضاء السايبري تُسبِّب أذى وخسائر قد تُضاهي تلك الناتجة عن الحروب التقليديَّة، وتُدعَى **الحروب السايبريَّة** Cyberwars، والحرب السايبريَّة هي الهجمات الافتراضيَّة الموجَّهة من قِبَل منظَّمات أو دول لاختراق أو لتعطيل أو تخريب أنظمة أو شبكات حاسوبيَّة لمنظَّمات أو دول أخرى [27، 28]، ويُدعَى الهجوم الذي يَتم إطلاقه في الحرب السايبريَّة **الهجوم السايبري** Cyberattack.

تَحدُث الحروب السايبريَّة بشكل مفاجئ، وتُشَنُّ هجماتها في مواعيد سريَّة، ولأنَّ عنصر المفاجأة في وقوعها وعدم معرفة مُطلِقها والحجم الكبير لخسائرها تكون ذات

آثار بالغة، ويُماثِل بعضها تلك المرتَبِطة بأي عمل إرهابي، وتُدعَى الحرب السايبريَّة عندها **الإرهاب السايبري** Cyberterrorism.

ولقد كان الحديث عن الحروب السايبريَّة في الأوساط الدوليَّة الرسميَّة خافتًا، إلا أنه بعد اكتشافه والتَعرُّض لكثير من الهجمات السايبريَّة الموجَّهة عمدًا إلى دول بحدِّ ذاتها، أصبح الحديث عن تلك الحروب وعن ضرورة اكتساب مقدرات سايبريَّة علنيًّا.

وتَتَّجه كثير من بحوث أمن المعلومات الحديثة نحو التَعمُّق في مجال الحروب السايبريَّة من خلال دراسة دوافعها (أسبابها) وآلية خوضها، ومعرفة الأطراف المشارِكة فيها، ونتائج وقوعها، ولا شَكَّ أنَّ تطوير أي دراسة أو بحث يَتعلَّق بالحرب السايبريَّة سيزيد من إدراك المعطيات المرتَبِطة بها، وسيُمكِّن الطرف المَعني بها (سواء منظَّمة أو دولة) من تلافي آثارها السلبية أو التخفيف منها على الأقل، والتَصدِّي لها كلَّما وَقَعت.

1.9 دوافع الحروب السايبريَّة

لم تَنشأ الحروب السايبريَّة في الفضاء السايبري بلا سبب، فقد كانت هناك دوافع وأسباب عدَّة وجيهة وراء قيامها، ولم تَكُن هذه الحروب السايبريَّة لو لم تَحدُث ثورات تكنولوجيَّة عَمَّت أرجاء العالم، فالمعرفة والخبرة المتزايدة في النفاذ خفيةً إلى شبكات الحاسوب والأدوات البرمجيَّة التي طُوِّرت خصيصًا لاختراق تلك الشبكات أحدثت معطيات أو ممكنات قيام تلك الحروب، ولَعلَّ دوافع الحروب السايبريَّة مترابطة نسبيًّا، إلا أنَّ وراء كل دافع هدفًا أو غرضًا معيَّنًا جَعَل هذه الدوافع ذات صيغة شبه رسميَّة في عالم الفضاء السايبري، ودوافع الحروب السايبريَّة هي:

1. **حماية الفضاء السايبري العسكري.** تَنطلِق معظم دول العالم في التعامل مع الحروب السايبريَّة من حماية فضائها السايبري العسكري أولًا، الذي تَعدّه الواجهة الأماميَّة في التَصدِّي للهجمات السايبريَّة قبل خوض تلك الحروب، وعلى هذا الاعتبار أنشأَت بعض الدول هيئات سايبريَّة رسميَّة مهمَّتها الدفاع

عن المنشآت العسكريَّة المرتبطة بشبكات الحاسوب [30، 31]، ولَعلَّ السبب الرئيس وراء إنشاء هذه الهيئات هو الوعي بأنَّ الهجمات السايبريَّة قد أصبحت ذات تهديد أكبر على الأمن القومي لبلدٍ ما من التهديدات التقليديَّة.

في الحقيقة، لم تَكُن قرارات إنشاء الهيئات السايبريَّة الدفاعيَّة إلا مدخلًا لإنشاء هيئات سايبريَّة هجوميَّة متلازمة مهمَّتها شَنُّ الحروب السايبريَّة وإطلاق الهجمات الإلكترونيَّة القادرة على تعطيل المنشآت العسكريَّة التقليديَّة المرتَبِطة بالشبكات الحاسوبيَّة لبعض الدول، وعلى هذا الأساس تَبنَّت الهيئات السايبريَّة لمعظم الدول إستراتيجيَّتَي الدفاع السايبري والهجوم السايبري الأساسيتين في عملها، واعتَبَرت تلك الهيئات السايبريّة الرسميَّة أنَّ تطبيق الإستراتيجيَتين معًا ضروري للحفاظ على الأمن القومي، وبالأخص حماية التجهيزات العسكريَّة المرتبطة بالشبكات الحاسوبيَّة، على الرغم من نكرانها لتطبيق إستراتيجيَّة الهجوم السايبري، وقد تطوّر الأمر إلى أبعد من ذلك من خلال تَعاون بعض الدول معًا لتطوير سيناريوهات ردع هجمات سايبريَّة تُطلَق على نحوٍ تدريبي من أجل الاستعداد للتصدِّي للهجمات السايبريَّة الحقيقيّة، وخصّصت دول أخرى ميزانيات ماليَّة ضخمة لتطوير قدرات تلك الهيئات السايبريَّة على أداء عملها وتزويدها بالقوَّة المطلوبة في صراع الفضاء السايبري، وانطلاقًا من مبدأ مشارَكة المجتمع المدني في حماية الفضاء السايبري، شَجَّعت دول أخرى شركات محليَّة متخصَّصة في أمن المعلومات على المساهَمة في إغناء هذا القطاع وتطوير شركات جديدة للعمل فيه.

2. **تعطيل منشآت البنية التحتيَّة الحيويَّة.** مع ارتباط مرافِق البنية التحتيَّة الحيويَّة (مثل شبكات الطاقة الكهربائيَّة، وشبكات توزيع المياه، والمواصلات، والمؤسسات الماليَّة، والصحيَّة، والاتصالات، والدفاع، والمؤسسات الحكوميَّة بشكلٍ عام) بالشبكة الحاسوبيَّة، ازدادَت الهجمات السايبريَّة الموجَّهة لتعطيل تلك المرافِق، وقد تَعدَّى الأمر إلى وقوع تعطيل فَعَّال لمنشآت حسَّاسة ذات

أهميَّة قوميَّة [37، 33]، وردًّا على وقوع هذه الهجمات، أنشأَت بعض الدول هيئات سـايبريَّة مهمَّتها فقط حماية المرافِق الحيويَّة المرتَبِطة بشبكات الحاسوب، بل حتَّى إنَّ دولًا أخرى أسَّسَت هيئات سايبريَّة متخصِّصة في حماية الفضاء السايبري الحكومي والبنى التحتيَّة ومستقلَّة عن تلك الهيئات السايبريَّة المتخصِّصة في حماية الفضاء السايبري العسكري.

3. **النزعَة إلى التَفوُّق السايبري.** يَرغَب عدد من حكومات الدول إلى التفوُّق السايبري والحفاظ على هذا التفوُّق من خلال خَوض حروب سايبريَّة وإطلاق هجمات سايبريَّة حقيقيَّة، ولكنَّ الهدف الحقيقي لتلك الدول في السعي إلى التَفوُّق السايبري هو صَدُّ الهجمات السايبريَّة المستقبليَّة الموجَّهة إليها، وذلك عن طريق اكتشاف العيوب السايبريَّة للخصوم مسبقًا في أثناء إطلاق الهجمات السايبريَّة إليهم.
4. **مكافحة الإرهاب.** لا شَكَّ أنَّ الإرهاب العالمي بأنواعه ومصادره المختلفة أصبحَ يَستعمِل الفضاء السايبري لنشر مفاهيمه وعقيدته وإدارة تنظيماته، ومن ذلك تقوم الحكومات، كما يَسعى بعض (الهاكرز) كمجموعات مستقلَّة غير حكوميَّة متعدِّدة الجنسيات، للتَصدِّي للمنشورات والرسائل الإلكترونيَّة التي تَبثُّها التنظيمات الإرهابيَّة من خلال حَظْرها ومَنْعها من الانتشار كرَدٍّ فعل إيجابي في الوقوف ضد الإرهاب.
5. **اكتساب منافع شخصيَّة أو ماديَّة.** يَشنُّ بعض الأفراد أو المنظَّمات (التجارية أو الصناعيَّة) حربًا سايبريَّة ضد أفراد أو منظَّمات أخرى، وذلك للحصول على منافع شخصيَّة أو منافع ماديَّة، وتَتمثَّل معظم الهجمات السايبريَّة، التي تُطلَق من قِبَل الأفراد أو المنظَّمات، في نَشر برامج خبيثة أو زَرع برامج تَجسُّس في حواسيب الضحايا، وتُؤدِّي البرامج الخبيثة أو برامج التَجسُّس عملها من خلال آليَّة يَضعها الطرف (أو الأطراف) الذي أطلقها، بحيث تُحقِّق الهدف من وراء إطلاقها.

6. **إجراء بحوث علميَّة لتطوير حلول مستقبليَّة.** ليسَت جميع الهجمات السايبريَّة موجَّهة دائمًا ضدَّ أطراف معيَّنة لكسب المنافع الشخصيَّة أو الماديَّة، أو ضدَّ دول بعينها لإيذائها، إنَّما يُطلَق بعضها من قِبَل شركات متخصِّصة في أمن المعلومات وأمن الفضاء السايبري من أجل رسم سيناريوهات محدَّدة في كيفيَّة التَعاطي مع هذه التهديدات أو الهجمات، ووَضع الحلول التقنيَّة المناسبة لمواجهتها، ومن ثم تطبيق هذه الحلول في برمجياتها، ومن المُلاحَظ أنَّ هذه التهديدات السايبريَّة وحلول مواجهتها، المطوَّرة من قِبَل شركات أمن معلومات تجاريَّة، قد لا تُقارَن أبدًا مع تلك التهديدات والهجمات السايبريَّة المطوَّرة من قِبَل مجموعات متخصِّصة واحترافيَّة تَعمل مع حكومات دول كبرى.

2.9 أطراف الحروب السايبريَّة

لم يَعُد امتلاك تكنولوجيا المعلومات والعمل عليها صعبًا، ولم يَعُد الدخول إلى بعض شبكات الحاسوب (ومنها الشبكة الدوليَّة الإنترنت) إلا كفعل تحريك فأرة الحاسوب من مكانها؛ ولذلك لم يَعُد مستعصيًا على أي جهة – سواء أكانت فردًا، أم منظَّمة، أم مجموعة أفراد يُمثِّلون دولة ما بصفة رسميَّة – أن تخوض حربًا سايبريَّة في أي وقت كان ومن أي مكان، على أن يَتوافر الوصول إلى الشبكة الحاسوبيَّة والهدف وامتلاك الخبرات والبرمجيات المناسبة، فأدوات الحرب، وتحديدًا تلك التي يُشَنُّ بها هجوم، أصبحت برمجيات صغيرة تُوضَع في وسائط تخزين صغيرة.

وثَمَّة أطراف محدَّدة تَقود أي حرب سايبريَّة وتُوجِّهها، وعمومًا تَندرِج هذه الحروب السايبريَّة تحت ثلاثة مستويات هي: **الحروب السايبريَّة بين الأفراد** Individual cyberwar، **والحروب السايبريَّة بين المنظَّمات** Organizational cyberwar، **والحروب السايبريَّة بين الدول** International cyberwar، وثَمَّة حروب سايبريَّة أخرى تَحدُث بين أطراف من مستويات مختلفة.

1.2.6 (الحروب) السايبريَّة بين الأفراد

في حقيقة الأمر، لا توجد حرب سايبريَّة بين الأفراد، فعندما يشنّ فردٌ ما هجومًا سايبريًّا على فرد آخر يُسبِّب له أذى، عندها يُعدّ الطرف أو الفرد المستهدَف مجرَّد ضحيَّة، وتُدعَى هذه الحالةُ **الجريمةَ السايبريَّةَ** Cybercrime، والجريمة السايبريَّة هي الجريمة أو الهجوم أو الفعل المؤذي الذي يُستخدَم فيه الحاسوب للنفاذ إلى الشبكات الحاسوبيَّة لإلحاق الضرر بفرد أو بمجموعة من الأفراد، ويُدعَى الطرف أو الفرد الذي يَقترِف الجريمة السايبريَّة **المجرم السايبري** Cybercriminal، ومهما كان عدد أفراد الطرف المستهدَف في الجريمة السايبريَّة، فهم في النهاية مجرَّد ضحايا، وليسوا أطراف حرب حقيقيين.

أحيانًا يخرج الأذى أو الضرر الذي يُسبِّبه المجرم السايبري عن نطاق الفضاء السايبري ليدخل أحيانًا في نطاق الجريمة الحقيقيَّة، كجناية القتل العَمد، أو الاغتصاب، أو السرقة. وهذا دون شك عندما يُستعمَل الحاسوب (أو الشبكة الحاسوبيَّة) بوصفه وسيلة مؤقَّتة في إتمام الجريمة، كأنْ يُخزَّن دليلٌ ما على جريمة قتل في حاسوب.

ثَمَّة نوعان أساسيان من الجرائم السايبريَّة التي تُقترَف هما: **جرائم سايبريَّة نشيطة** Active cybercrimes و**جرائم سايبريَّة كامنة** Passive cybercrimes، والجرائم السايبريَّة النشيطة هي الجرائم السايبريَّة التي يَنجُم عنها إيذاء حواسيب الضحايا (الأفراد الآخرين من الحرب السايبريَّة المفتَرَضة) عن طريق نَشر البرامج الخبيثة، مثل الفيروسات والديدان وأحصنة طروادة وإطلاق هجمات الحرمان من الخدمة. أمّا الجرائم السايبريَّة الكامنة فهي الجرائم السايبريَّة التي تَتمثَّل في سرقة المعلومات الفرديَّة الخاصَّة، مثل كلمات السر لحسابات البريد الإلكتروني، ومواقع الشبكات الاجتماعيَّة، وأرقام التعاريف الشخصيَّة، وأرقام الحسابات المصرفيَّة، وتُقترَف الجرائم السايبريَّة الكامنة بشكلٍ كبير عن طريق استعمال برامج التَجسُّس. عمومًا تُعدّ

الجرائم السايبريَّة بنوعيها النشيط والكامن تهديدًا بشريًّا موجَّهًا نحو جميع الأطراف من جميع المستويات.

ولا يُمكِن الاستهانة بنتائج وقوع الجرائم السايبريَّة، فبعد انكشاف الضرر والأذى اللذين يُمكِن أن تُسبِّبهما الجرائم السايبريَّة، يشير أحد التقارير الدوليَّة إلى أنَّ تلك الجرائم تُكبِّد الاقتصاد العالمي ما يُقارِب 445 بليون دولار أمريكي سنويًّا بحسب تقديرات عام 2005م.

2.2.9 الحروب السايبريَّة بين المنظَّمات

تَمتلِك المنظَّمات (سواء أكانت تجاريَّة أم صناعيَّة) خصائص تجعلها أكثر احتمالًا لأن تَدخُل في حروب سايبريَّة بين بعضها مما هو الحال بين الأفراد كأطراف مستقلَّة، ولأنَّ المنظَّمة (مهما كان عملها) أساس بناء اقتصاد دولة، يُعدّ استهدافها من قِبَل أي منظَّمة منافِسة أخرى في الدولة نفسها أو في دولة أخرى حدثًا ممكنًا في معظم الأحيان [20، 21]. إنَّ المنظَّمة التي تُخصِّص ميزانيَّة ماليَّة كبيرة لوضع إستراتيجيَّة أمن معلومات خاصَّة بها تستطيع أن تَتصدَّى للهجمات السايبريَّة الموجَّهة من قِبَل أي منظَّمة أخرى (منافِسة أو غير منافِسة)، أو على الأقل تُخفّف من الآثار السلبيَّة للهجمات التي قد تتلقاها فعلًا.

تسعى الهجمات السايبريَّة بين المنظَّمات إلى تحقيق الهدفين الرئيسين الآتيين:

1. الحصول على معلومات الأعمال الخاصَّة للاستفادة منها في اكتساب منافع ماليَّة، ويَتم هذا عادةً عن طريق اختراق أنظمة حواسيب المنظَّمة المستهدَفة، أو زرع برامج تَجسُّس فيها، ومن ثم تحميل معلومات الأعمال الخاصَّة التي تحتوي على تفاصيل صناعة منتجات معيَّنة أو تصاميم مستقبليَّة أو صفقات تجاريَّة.

2. تخريب منشآت البنية التحتيَّة المتَّصلة بشبكات الحواسيب للمنظَّمة المستهدَفة وتكبيدها خسائر كبيرة، ويَتُم ذلك من خلال نشر فيروس أو دودة في أنظمة حواسيب المنظَّمة تُعطِّل عمل معدَّات البنية التحتيَّة أو تُدمِّرها، وتَشتدُّ الحروب السايبريَّة بين المنظَّمات عندما تَتطوَّر هذه المنظَّمات، وتصبح أكثر إنتاجًا وذات إيرادات ماليَّة كبيرة، وعلى هذا الأساس، تُحاوِل كل منظَّمة أن تَرفَع من مستوى حماية معلوماتها من خلال وضع ميزانية ماليَّة ضخمة لتخطيط ورسم المعايير التي تَضمَن تطبيق ممارسات جيدة في أمن المعلومات، وتوعية موظَّفيها المسؤولين عن تلك المعلومات بأهميَّة التقيُّد بالمعايير المرسومة للحفاظ على نجاح المنظَّمة ككل.

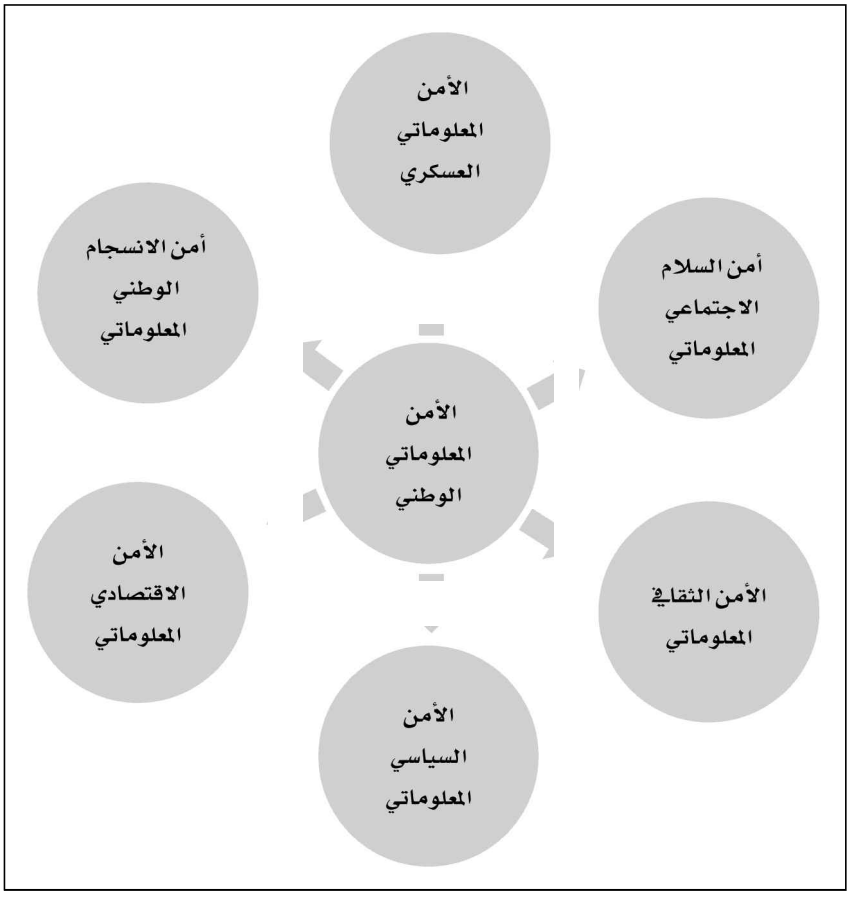
3.2.9 الحروب السايبريَّة بين الدول

إنَّ الحروب السايبريَّة التي تَحدُث بين الدول هي أوضح تجسيد لمفهوم (الحرب السايبريَّة)، فالحرب التقليديَّة عادةً ما تَقع بين دولتين أو أكثر، ولكن ليس ثَمَّة حرب تقليديَّة (بكل معنى الكلمة) تَحدُث بين أفراد أو بين منظَّمات. لذلك، وعلى نحوٍ مشابه للحروب التقليديَّة التي تَقع بين الدول، تَحدُث حروب سايبريَّة بينها، وفي بعض الأحيان، تَحدُث حروب سايبريَّة بين دول صديقة، إلا أنَّ الاعتراف بخوضها لا يُعلَن من قِبَل أي طرف منها، وقد يعود ذلك إلى أسباب دفاعيَّة تَتمثَّل مثلًا في اختبار أنظمة الحماية السايبريَّة للدولة التي شَنَّت الحرب ضدَّ دولة صديقة.

تشتمل الحروب السايبريَّة بين الدول التعرض إلى ستة أنواع من الأمن والأمان الوطني المعلوماتي، ويبيّن الشكل تمثيلًا مبسطًا لذلك.

الأمن المعلوماتي الوطني

(أمن المعلومات والاتصالات)



تَتشابه أهداف الحروب السايبريَّة بين الدول، من حيث المستهدفات المعلوماتية، مع أهداف الحروب السايبريَّة بين المنظَّمات، ولكن على نطاقٍ أوسع، وعلى العموم، ثَمَّة أيضًا ثلاثة أهداف رئيسة للحروب السايبريَّة بين الدول هي:

1. الحصول على المعلومات المصنَّفة سريَّة (مهما كان مستوى تصنيفها السرِّي) للدولة المستهدَفة، ويشمل ذلك المعلومات العسكرية، والأمنية، والاقتصادية، والاجتماعية، وغيرها.

2. تعطيل منشآت البنية التحتيَّة الحيويَّة للدولة المستهدَفة.
3. الحرب الإعلامية باستعمال الإعلام الجديد من خلال الفضاء السيبرياني.

تختلِف شدَّة الحروب السايبريَّة التي تحدُث بين الدول باختلاف المهارات العلميَّة للدولة المصدَر والدولة الهدف، والإمكانيات المتمثِّلة في المعدَّات والأدوات البرمجيَّة التي تَمتلِكها الدولة المصدَر، ويشهد العالم اشتداد قوَّة الحروب السايبريَّة بين الدول، وما قد يُصيب الدولة المستهدَفة هو تخريب منشآت بنيتها التحتيَّة الحيويَّة، هذا إن كانت هذه المنشآت متَّصلة بشبكات حاسوبيَّة، وقد يكون للحرب السايبريَّة أثر مادِّي في الدولة المستهدَفة، وهذا قَلَّما يَحدُث إلا في حالات محدَّدة.

4.2.9 الحروب السايبريَّة بين أطراف مختلفة المستويات

من الممكِن أن تَقَع حروب سايبريَّة بين أطراف من مستويات مختلفة، فقد يَحدُث أن يَشنَّ فرد أو مجموعة من الأفراد هجومًا سايبريًّا على منظَّمة ما بهدف الحصول على منافع شخصيَّة أو مكاسب ماليَّة، وقد يقوم فرد أو مجموعة من الأفراد بشَنِّ هجوم سايبري على مؤسسات دولة ما، ويَحدُث أيضًا أن تَخوض دولة ما حربًا سايبريَّة ضد مجموعة من الأفراد أو منظَّمة ما أو منظَّمات عدَّة، عمومًا عندما تَحدُث حروب سايبريَّة عدَّة معًا في الفضاء السايبري بين أطراف من مستويات مختلفة وعبر قارَّات العالم، يُمكِن أن نَدعو مجموعها **الحرب السايبريَّة العالميَّة** World cyberwar.

3.9 مقوِّمات الحروب السايبريَّة

إنَّ لكل حرب تقليديَّة في عالم الواقع معطياتها الخاصَّة، ولكن جميع الحروب التقليديَّة لديها عناصر تُؤسِّس لقيامها، وفي المقابل، تَمتلِك الحروب السايبريَّة مقوِّمات موحَّدة خاصَّة بها، ومقوِّمات الحروب السايبريَّة هي المكوِّنات أو العناصر (الماديَّة وغير الماديَّة) التي تُؤسِّس بمجموعها قيام تلك الحروب، ولكل حرب سايبريَّة معطياتها

الخاصَّة المتمثِّلة مثلًا في دوافع قيامها والنتائج المتوقَّعة من خوضها، ولكن مقوِّمات أي حرب سايبريَّة هي:

1. **البيئة** Environment.
2. **الطرف** Entity.
3. **الإستراتيجيَّة** Strategy.
4. **الأداة** Tool.

وعلى الرغم من أنَّ مقوِّمات أي حرب سايبريَّة موحَّدة، إلا أنَّ عواملها متغيِّرة، ويعني ذلك أنَّ الطرف أو الإستراتيجيَّة أو الأداة قد تَتغيَّر من حرب سايبريَّة إلى أخرى.

1.3.9 البيئة

تَتنوَّع البيئات الواقعيَّة التي تَحدُث بها الحروب التقليديَّة، فمن الممكِن تحديد بيئة أي حرب تقليديَّة بمجرَّد وقوعها، سواء في البر أو على البحر أو في الجو أو الفضاء، ولكن الحروب السايبريَّة لا تَقَع إلا في بيئة افتراضيَّة واحدة هي الفضاء السايبري، والفضاء السايبري، كما عُرِّف سابقًا، هو البيئة الافتراضيَّة التي يَتم فيها تَبادُل المعلومات الرقميَّة عبر شبكات حاسوبيَّة. يَصِف التعريف السابق الشكل العام للفضاء السايبري، ولكن من الناحية الفيزيائيَّة، الفضاء السايبري هو المجموع الأكبر لشبكات الحواسيب، التي تُعرَف باسم الإنترنت.

عندما تَقَع حرب تقليديَّة بين دولتين، تعرِف كلٌّ منهما حدودها (البريَّة، أو البحريَّة، أو الجويَّة) المرسومة التي لا تتجاوَزها إلا في حالة هجوم، وتُحافِظ على ثباتها في حالة دفاع، ولكن في بيئة الحروب السايبريَّة (التي هي الفضاء السايبري) لا توجد حدود بين أي طرف في أثناء قيامها، فالاستطلاع والتخطيط والهجوم (أو حتَّى الدفاع) في الفضاء السايبري يُمكِن أن تَتم جميعها من أي مكان في العالم وفي أي وقت، وهذه الحريَّة شبه المطلقة في التَحكُّم في شَنِّ حرب سايبريَّة وإدارتها من أي مكان في العالم

جَعلَت كل من لديه المعرفة والخبرة الكافيَتَين مع أدوات مناسبة قادرًا على خوضها، ومن أهم خصائص الحروب السايبريَّة شنُّ الهجمات فيها من قِبَل أطراف موجودين فيزيائيًّا عبر قارَّات العالم دون أن يَلتقوا أبدًا.

إنَّ الفضاء السايبري هو البيئة الوحيدة التي تَجري فيها أي حرب سايبريَّة؛ لذا فمن المهم أن يُدرِك الطرف (سواء أكان المصدَر أم الهدف) جميع خصائص الشبكة الحاسوبيَّة التي يعمل عليها، وأن يُحاوِل سَدَّ الثغرات المكتشَفة، ويُعالِج نقاط الضعف في هذه الشبكة إذا كان يُمثِّل الطرف الهدف، أو أن يَكتشِف ثغرات ونقاط ضعف الشبكة الحاسوبيَّة للطرف الهدف إذا كان يُمثِّل الطرف المصدَر. وأخيرًا، ينبغي للطرف المصدَر والطرف الهدف أن يَعُدّا الفضاء السايبري ساحة الحرب السايبريَّة التي من الواجب السيطرة عليها والتَحكُّم فيها على النحو الذي يُحقِّق الغاية.

2.3.9 الطرف

يُعدّ الطرف البشري (سواء أكان فردًا أم منظَّمةً أم دولةً) المقوِّم الأهم من مقوِّمات أي حرب سايبريَّة، فدون الطرف البشري لا يُمكِن أبدًا إشعال أي حرب سايبريَّة. والطرف البشري (واختصارًا الطرف فقط) هو المحرِّك الأساسي في الحرب السايبريَّة، إذْ لا يُمكِن أن تُوجَد إستراتيجيَّة في الحرب السايبريَّة (سواء أكانت هجومًا أم دفاعًا) دون أن يَرسُمها الطرف، ولا يُمكِن أن تَتحرَّك أدوات الحرب السايبريَّة وحدها، وتُؤدِّي دورها دون أن يَستثمرها الطرف، وكل ذلك دليلٌ على أنَّ مقوِّم الطرف هو أهم مقوِّمات أي حرب سايبريَّة.

على العموم، ثَمَّة طرفان أساسيان في أي حرب سايبريَّة، هما: **الطرف المصدَر** Source entity و**الطرف الهدف** Target entity، والطرف المصدَر هو الطرف البشري الذي يُؤدِّي دور المهاجم أو الذي يقوم بعملية الهجوم السايبري على الطرف الهدف في الحرب السايبريَّة. أمّا الطرف الهدف فهو الطرف المستهدَف الذي يَتلقَّى الهجوم

السايبري من الطرف المصدَر، الذي يُؤدِّي دور المدافِع أو الذي يقوم بعملية الدفاع في الحرب السايبريَّة، وقد يكون الطرف المصدَر فردًا أو منظَّمةً أو دولةً أو مجموعها، وقد يكون الطرف الهدف في الوقت نفسه فردًا أو منظَّمةً أو دولةً أو مجموعها.

يتَّصفُ كلٌّ من الطرف المصدَر والطرف الهدف بخصائص تُميِّزهما عن بعضهما، وهذه الخصائص تُمكِّنُ من التَعرُّف إلى كل طرفٍ فيما إذا كان طرفًا مصدَرًا أو طرفًا هدفًا، وخصائص الطرف المصدَر هي:

1. حيازة دافع للقيام بحرب سايبريَّة ضدَّ الطرف الهدف. لا بُدَّ أن يَمتلِك الطرف المصدَر دافعًا قويًّا ليُقرِّر القيام بهجوم سايبري على طرف معيَّن، ويحثُّ أحد الدوافع التي تَمَّ سردها سابقًا أي طرف على أن يَخوض حربًا سايبريَّة متى وُجِد هذا الدافع.
2. التَّمتُّع بمعرفة علميَّة ومهارة مكتَسَبة في المجال، وتجهيزات في الفضاء السايبري تَجعله يَتجرَّأ لشَنِّ هجوم سايبري على الطرف الهدف، وإذا لم تَتوافَر عوامل المعرفة العلميَّة والخبرة العمليَّة في خوض تجربة الحرب السايبريَّة لدى الطرف المصدَر، لن يستطيع عندها أن يَشنَّ هجومًا سايبريًّا على الطرف الهدف، أو أن يَخوض حربًا سايبريَّة ضدَّه، بل حتَّى من الممكِن أن يُصبِح الطرف المصدَر طرفًا هدفًا دون أن يدري إذا لم يَمتلِك المعرفة الكافية الخاصَّة بالحروب السايبريَّة.
3. السَّعي نحو معرفة نتائج الهجوم السايبري على الطرف الهدف، والاستطلاع حول نجاحه أو فشله. يَكتسِب الطرف المصدَر ثقة كبيرة في نفسه إذا عَلِم بنجاح هجومه على الطرف الهدف، وهذا الأمر سيُشجِّعه على شَنِّ هجمات سايبريَّة أخرى على الطرف الهدف نفسه وشَنِّ هجمات سايبريَّة على أطراف هدف أخرى أو خوض حرب سايبريَّة ضدَّها.

4. التَحـوُّل إلـى موقف الطرف الهدف تلقائيًّـا. بمجرَّد أن يَشـنَّ الطرف المصدَر هجومًا سـايبريًّا على الطرف الهدف سيَتحوَّل بدوره تلقائيًّا إلى طرف هدف، وسيَسـعى إلـى أن يَصدّ الهجمات السـايبريَّة التي قد تأتي مـن الطرف الهدف الآخـر الـذي بدوره قد تَحوَّل إلى طرف مصدَر، والأمـر برمَّته طبيعي جدًّا؛ لأنَّ مبدأ الحرب بشـكل عام يَعتمِد على أسـلوب الهجوم والدفاع في الوقت نفسه أو الصَدِّ والرَدِّ.

أمّا خصائص الطرف الهدف فهي:

1. حيـازة سـبب يَجعلـه فـي موقـف الطـرف الهـدف، كأن يكون قـد أطلـقَ هجومًا سـايبريًّا سـابقًا، وكان في موقف الطرف المصدَر، وبعدها وبدافع انتقامي من الطرف الآخر، أصبح في موقف الطرف الهدف. وهذا يُحتِّم الآن على الطرف الهـدف أن يَتوقَّـع في أي وقت تَلقِّي هجوم سـايبري، وأن يكون مسـتعدًّا لحماية بنيته السايبريَّة.
2. امتـلاك بنيـة سـايبريَّة ضعيفـة تَجعله عُرضةً لهجوم سـايبري. وهذا بلا شـك إن لم يَسـتطِع الطرف الهدف صَدّ الهجوم السـايبري والدفاع عن منشآته التي تَسـبَح في الفضاء السـايبري، فعندما لا يكون الطرف (سـواء أكان مصدَرًا أم هدفًا) محصَّنًا على نحوٍ جيد، سيُصبح عُرضةً لأي هجوم سايبري، سواء أكان بدافـع انتقامـي أم لا؛ لذا يَنبغي للطرف الهـدف أن يُعزِّز من دفاعاته الرقميَّة؛ لكي يكون جاهزًا في حال قام بالردِّ، ومستعدًّا في حال قام بالصدِّ.
3. الاسـتعداد للدفاع عن بنيته السـايبريَّة من هجمات سـايبريَّة مسـتقبليَّة أخرى بعد أن تَلقَّى الهجوم السايبري الأول من الطرف المصدَر، ومن ثمَّ التَحوُّل إلى أن يكون في موقف الطرف المصدَر، وهذا دون شك إنْ لم يكُن الطرف الهدف قد بادَر مسبقًا بهجوم سايبري على الطرف المصدَر.

إنَّ دراسة سلوك طرفَي الحرب السايبريَّة مهم جدًّا لمعرفة (أو على الأقل تَوقُّع) نتائجها، فالحرب السايبريَّة لا تقوم إلا بوجود نشاط سايبريّ بين طرفين، فلولا نشاط الطرفين المصدَر والهدف معًا لما كان هناك حرب سايبريَّة، فمن الممكِن أن يشنّ طرف واحد هجومًا سايبريًّا على طرف آخر لا يُحرِّك ساكنًا. عندها، لا يُؤسِّس هذا الهجوم السايبري حربًا سايبريَّة، وإنَّما يُسمّى (هجومًا سايبريًّا)، وفي المقابل، إذا كانت الهجمات السايبريَّة متبادَلة بين طرفين، عندها تكون قد وَقَعت حربٌ سايبريَّة.

3.3.9 الإستراتيجيَّة

يَعتمِد ربح الحروب التقليديَّة أو خسارتها على فعاليَّة الإستراتيجيَّة الموضوعة لخوض الحرب، سواء أكانت هذه الإستراتيجيَّة هجومًا أم دفاعًا، فعندما يَفوز طرف ما في حرب على طرف آخر، فإنَّ ذلك دليلٌ على أنَّ إستراتيجيَّة الحرب للطرف الفائز أكثر فعاليَّة من إستراتيجيَّة الحرب للطرف الخاسر (وهذا إنْ كان هو أيضًا يُطبِّق إستراتيجيَّة ما)، وفي الحرب التقليديَّة لا تحتاج بعض الدول إلا إلى إستراتيجيَّة لتُهاجِم بها طرفًا آخر فقط دون أن تَعوز إستراتيجيَّة أخرى للدفاع (وهذا عندما تكون الدولة متفوقة حربيًّا)، وبعض الدول الأخرى لا تحتاج إلا إلى إستراتيجيَّة لتدافع بها (على الأقل) عن نفسها من هجمات طرف آخر أو أطراف أخرى. أمّا في الفضاء السايبري فلا بُدَّ لكل طرف (سواء أكان فردًا، أم منظَّمة، أم دولة) أن يَمتلِك إستراتيجيَّتين معًا: واحدة للدفاع السايبري، وواحدة للهجوم السايبري؛ ليَخوض أي حرب سايبريَّة.

ثَمَّة إستراتيجيَّتان أساسيَّتان لخوض أي حرب سايبريَّة هما: **إستراتيجيَّة الدفاع السايبري** Cyber defense strategy **وإستراتيجيَّة الهجوم السايبري** Cyber offense strategy. وإستراتيجيَّة الهجوم السايبري هي الخطة المرسومة من قِبَل أي طرف، التي ينبغي أن يَضمَن تطبيقها شَنّ هجمات سايبريَّة ناجحة على الطرف الخصم، ولا بُدَّ أن يكون لدى كل طرف في الحرب السايبريَّة إستراتيجيَّتا الدفاع السايبري والهجوم

السايبري معًا، ويجب أن تكون الإستراتيجيَّتان مكمِّلتين لبعضهما، بمعنى أنه إذا طُبِّقَت إستراتيجيَّة الهجوم السايبري مثلًا، ينبغي أن تحتوي إستراتيجيَّة الدفاع السايبري على سيناريوهات لكل آليَّة هجوم؛ لكي تكون مستعدَّة للصَدِّ وحماية البنية السايبريَّة للطرف الذي وَضعهما، ولا تَختلِف إستراتيجيَّتا الدفاع السايبري والهجوم السايبري عن بعضهما من حيث السياسات العامة والأدوات، فكلتاهما تُطبَّقان في الفضاء السايبري نفسه ومن قِبَل الطرف نفسه.

ولا يُمكِن التَنبُّؤ بفوز طرف ما أو خسارته في أي حرب سايبريَّة، ولكن إذا اُعتمدت معايير محدَّدة في رسم إستراتيجيتَي الدفاع السايبري والهجوم السايبري وتطبيقهما، يُمكِن عندها توقع الفوز في الحروب السايبريَّة، وإذا لم تَضمَن معايير نجاح إستراتيجيَّة الهجوم السايبري نجاح أي هجوم سايبري، ينبغي على الأقل أن تَضمَن معايير نجاح إستراتيجيَّة الدفاع السايبري حماية البنية السايبريَّة.

معايير نجاح إستراتيجيَّة الدفاع السايبري هي:

1. أن تُراعي احتمال التَعرُّض لأقوى هجوم سايبري. عند رسم إستراتيجيَّة الدفاع السايبري، يجب على واضعيها أن يستعدوا لاحتمال مواجهة أكبر هجوم سايبري، وهذا السقف الأعلى من التشاؤم يَضمَن الحماية من الهجمات السايبريَّة الأقل حدَّة.
2. أن تكون قابلة للتعديل في حال لم يَنجَح تطبيقها في حماية البنية السايبريَّة كليًّا أو جزئيًّا. ينبغي أن تكون إستراتيجيَّة الدفاع السايبري مرنة قدر الإمكان للتعديل، خاصَّةً في أثناء وقوع الحرب السايبريَّة؛ لأنَّ تعديلها جزئيًّا قد يَقلِب الموازين، ويَتحوَّل الطرف الذي وَضعها من خاسر إلى فائز.
3. أن تحتوي على توقع سيناريوهات حصول هجمات سايبريَّة متعدِّدة الإمكانيَّات ومن أطراف مختلفة. إنَّ وضع إستراتيجيَّة دفاع سايبري، بحيث تكون موجَّهة للتعامل مع طرف معيَّن أو طرف ذي خصائص معيَّنة قد يؤدي إلى الفشل؛ لذا

يجب على إستراتيجيَّة الدفاع السايبري أن تُحاكي هجمات ذات قوى متفاوتة ومن أطراف مختلفة.

4. أن تكون بسيطة وواضحة قدر الإمكان منذ البداية وعند تطبيقها. إذا احتَوَت إستراتيجيَّة الدفاع السايبري على خطوات كثيرة وتفاصيل معقَّدة، فسوف يكون من الصعب على الأشخاص الموكَّلين بتطبيقها فهمها واستيعابها، عندما يقومون بدراستها، أمّا عند التطبيق العملي لهذه الإستراتيجيَّة في أثناء وقوع الحرب، فسوف يُعاني هؤلاء الأشخاص الموكَّلين بتطبيقها بطئًا في التنفيذ، وسوف يَتمتَّع الأشخاص الموكَّلون بتطبيق إستراتيجيَّة الدفاع السايبري بمرونة كافية إذا كانت هذه الإستراتيجيَّة سريعة التنفيذ.
5. أن يُرافِقها إستراتيجيَّة دفاع سايبري أخرى رديفة وبديلة لها في حال فَشِل تطبيق الإستراتيجيَّة الأساسيَّة؛ لذا يجب وضع إستراتيجيَّة دفاع سايبري بديلة وجاهزة للتطبيق فورًا إذا واجَه تطبيق الإستراتيجيَّة الأساسيَّة شللًا تامًّا.

أمّا معايير نجاح إستراتيجيَّة الهجوم السايبري فهي:

6. أن تكون مرسومة وفق أفضل الممارسات العالمية في وضع إستراتيجيَّات الهجوم السايبري. مما لا شك فيه، فإنه لا تُقارَن إستراتيجيَّات الهجوم السايبري للدول الماهرة في الحروب السايبريَّة مع تلك الموضوعة من قِبَل أفراد أو منظَّمات، حتَّى ولو امتَلكوا خبرة كبيرة في هذا المجال، مراقبة سلوك أي هجوم سايبري وتحليله من أي أطراف قويَّة في هذا المجال يُمكِّن من استخلاص بعض أو جميع خطوات إستراتيجيَّاتها في الهجوم السايبري، ومن ثم دراستها والاستفادة من دورها.
7. أن تَضم سيناريوهات متنوِّعة ومتعددة لهجمات سايبريَّة، بحيث إنْ لم تَنجَح إحداها تَنجَح الأخرى. إنَّ التَنوُّع في سيناريوهات الهجمات السايبريَّة ضروري لكي يَتحقَّق التأثير في أكبر قد مَمكِن من أنظمة شبكات حواسيب الطرف

الهدف، ومن المُمكِن عمليًّا أن يَفشَل تطبيق سيناريو ما لهجوم سايبري على طرفٍ، ويَنجَح على طرفٍ آخر، وهذا كلّه بسبب اختلاف مستويات حماية البنية السايبريَّة لدى كل طرف.

8. أن يتطلَّب تطبيقها استعمال أقل عدد مَمكِن من الأدوات. من الضروري التنويع في استعمال الأدوات البرمجيَّة اللازمة في الهجوم السايبري، ولكنَّ كثرة هذه الأدوات أو تعقيدها أو تطبيقها دفعةً واحدة قد يُؤدِّي إلى الخسارة في الحرب السايبريَّة، ومن ناحيةٍ ثانية، يُؤدِّي استعمال جميع الأدوات البرمجيَّة في هجوم سايبري واحد إلى كَشف جميع القدرات المتوافرة في هذا المجال، ومن ثم يؤدي إلى إضعاف قوَّة أي هجوم سايبري مستقبلي واحتمال الخسارة في الحرب السايبريَّة.

9. أن تُحدَّث على نحوٍ دوري. ينبغي أن تُواكِب إستراتيجيَّة الهجوم السايبري تَنوُّع الحروب السايبريَّة وتَطوُّرها على مستوى العالم، وأن تَتماشى مع تَطوُّر أسلحة الحروب السايبريَّة، وبالتحديد تلك الأدوات الخاصَّة بشَنِّ الهجوم السايبري، فإذا لم تُحدَّث إستراتيجيَّة الهجوم السايبري لأي طرف دوريًّا، فلن يُكتَب له النجاح بسبب تَطوُّر إستراتيجيَّات الدفاع السايبري للأطراف الأخرى وتحديثها.

والخلاصة، لا يُمكِن لأي طرف أن يفوز في حرب سايبريَّة إذا لم تَكُن إستراتيجيَّتا الدفاع السايبري والهجوم السايبري الخاصَّتان به ناجحتين، حتَّى ولو امتَلَك أدوات الحروب السايبريَّة، فالتخطيط الجيِّد لهاتين الإستراتيجيتين يُسهِم في الفوز، ولكنَّ لا يَضمَنه إلا إذا كانت آليات تطبيقهما ناجحةً أيضًا.

4.3.9 الأداة

لا يُمكِن إطلاق أي هجوم سايبري أو خوض حرب سايبريَّة دون امتلاك الأدوات اللازمة لذلك، وأدوات الحروب السايبريَّة بالمعنى التقني هي الأدوات البرمجيَّة التي يَتم العمل عليها في الفضاء السايبري، ويجري يوميًّا إنتاج أدوات برمجيَّة خاصَّة بالحروب السايبريَّة وتطويرها؛ لذا لا يُمكِن حَصر جميع تلك الأدوات البرمجيَّة في حديث واحد، وعمومًا ثَمَّة نوعان أساسيَّان من أدوات الحروب السايبريَّة، هما: **أدوات الدفاع السايبري** Cyber defense tools و**أدوات الهجوم السايبري** Cyber offense tools. من البدهي إدراك أنَّ أدوات الدفاع السايبري تَخصُّ الطرف الهدف، وأدوات الهجوم السايبري تَخصُّ الطرف المصدَر، ولكنَّ ذلك لا يعني أبدًا عدم امتلاك الطرف المصدَر أدوات الدفاع السايبري أيضًا، أو عدم امتلاك الطرف الهدف أدوات الهجوم السايبري؛ لذا فمن المنطقي أن يَمتلِك كلٌّ من الطرف المصدَر والطرف الهدف النوعين معًا.

تتألَّف أدوات الدفاع السايبري من **أدوات الحماية** Protection tools، و**أدوات الفحص** Scan tools، و**أدوات المراقبة** Monitoring tools. تَتولَّى أدوات الحماية مهمَّة الحفاظ على أمان شبكة الحواسيب المتَّصلة بالإنترنت وجميع الشبكات الحاسوبيَّة التي تَربُط منشآت البنية التحتيَّة الحيويَّة، وأمّا أدوات الفحص فتَتولَّى مهمَّة فحص أنظمة الحواسيب المرتَبِطة ببعضها والتأكُّد من عدم وجود ثغرات قد تُؤدِّي إلى اختراق تلك الأنظمة الحاسوبيَّة، وأمّا أدوات المراقبة فتَتولَّى مراقبة حركة مرور البيانات الداخلة والخارجة من الشبكة الحاسوبيَّة الداخليَّة وإليها؛ للتأكُّد من عدم وجود أنشطة مشبوهة أو غير طبيعيَّة، وإنَّ أدوات الدفاع السايبري الثلاثة السابقة هي الأساسات التي تُبنَى عليها أي آلية دفاع سايبري، وهي المفاصل التي تَرتكِز عليها إستراتيجيَّات الدفاع السايبري.

أمّا أدوات الهجوم السايبري فتتألَّف من **أدوات الاختراق** Hacking tools، و**أدوات التعطيل** Disruption tools، و**أدوات التَجسُّس** Spy tools. تقوم أدوات الاختراق بعملية اختراق أنظمة حواسيب الطرف المستهدَف، ويَتم ذلك من خلال البحث عن ثغرات في شبكة حواسيب الطرف الهدف، وأمّا أدوات التعطيل فهي البرامج الصغيرة التي تُرسَل إلى شبكة حواسيب الطرف الهدف لكي تُسبِّب تخريبًا وأذى في أنظمة الحواسيب المتَّصلة بتلك الشبكة وفي كل ما يَتَّصل بها أيضًا من منشآت البنية التحتيَّة، وأمّا أدوات التَجسُّس فهي أخطر الأدوات التي يَستعملها الطرف المصدَر، والتي تقوم بعملية تسجيل جميع أنشطة أو معلومات وبيانات الطرف الهدف خفيةً، ومن ثم إرسالها إلى الطرف المصدَر.

تَختلِف صفات أدوات الدفاع السايبري عن صفات أدوات الهجوم السايبري، فمن الضروري امتلاك جميع أدوات الدفاع السايبري وتطبيقها معًا لكي تُحمَى البنية السايبريَّة لأي طرف. أمّا أدوات الهجوم السايبري فيُمكِن استعمال أي مجموعة منها (أو جميعها) لإطلاق هجوم سايبري، فمن المُمكِن لإطلاق هجوم سايبري أن تُستعمَل مثلًا أدوات الاختراق وحدها دون استعمال أدوات التعطيل أو أدوات التَجسُّس، وكذلك الأمر مع أدوات التعطيل وأدوات التَجسُّس.

الملحق (1)

قائمة بمعايير (مواصفات دولية) وبأفضل الممارسات في إدارة أمن المعلومات وأمانها

يمكن الوصول لتفاصيلها من الإنترنت

Short list of 20 standards and good practices that are in use in the EU

Telecommunications market:

1 ISO/IEC 27001/2

2 ISO/IEC 24762:2008 Guidelines for ICT and disaster recovery services

3 ISO/IEC 27005 Information security risk management

4 ISO/IEC 27011 Information security management guidelines for telecommunications

5 BSI BS25999_1 Business Continuity

6 ITU_T X.1051 (02/2008)

7 ITU_T X.1056 (01/2009)

8 ITU_T X.800 (1991)

9 ITU_T X.805 (10/2003)

10 ISF Standard of Good Practice 2007

11 CobiT

12 ITIL Service Support

13 ITIL Security Management

14 IT_Grundschutz_Kataloge

15 KATAKRI

16 NIST SP 800_34

17 NIST SP 800_61

18 FIPS_200

19 UK NICC Minimum Standard ND1643

20 PCI DSS 1.2

Source: The European Union Agency for Network and Information Security (ENISA): Shortlisting network and information security standards and good practices.

الملحق (2)

مستويات سرية المعلومات في النظام الأمريكي

1. Core secrets أسرار عظمى

The highest level of classification. Information at this level is released only to select government individuals (Used by the NSA exclusively).

2. Top Secret سري للغاية

The highest security level outside of the NSA framework. "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe. It is believed that 1.4 million Americans have top secret clearances.

3. Secret سري

This is the second-highest classification. Information is classified Secret when its unauthorized disclosure would cause "serious damage" to national security. Most information that is classified is held at the secret sensitivity.

4. Confidential مؤتمن – خاص

This is the lowest classification level of information obtained by the government. It is defined as information that would "damage" national security if publicly disclosed, again, without the proper authorization.

5. Unclassified (غير سري) متاح

الملحق (3)

مواقع إلكترونية مفيدة في أمن المعلومات

http://www.infosyssec.org/infosysec/index.htm

http://www.certicom.com

http://www.counterpane.com

http://www.cs.purdue.edu/coast/

http://www.sans.org

http://www.icsa.net/

http://www.itpolicy.gsa.gov

http://www.bs.org/

http://www.rsa.com

http://www.telstra.com.au/info/security.html

https://www.cisecurity.org/

https://www.sans.org/security_training/by_location/all

https://www.pcisecuritystandards.org/

https://www.enisa.europa.eu/

http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref2048

http://www.pwc.com/gx/en/issues/cyber_security/information_security_survey.html

الاتحادات والمنظمات المتخصصة في أمن المعلومات

ISSA: (www.issa.org)

مؤسسة SANS : (www.sans.org)

الاتحاد العالمي لحماية الحاسوب (International Computer Security Association)

ICSA: (www.icsa.net)