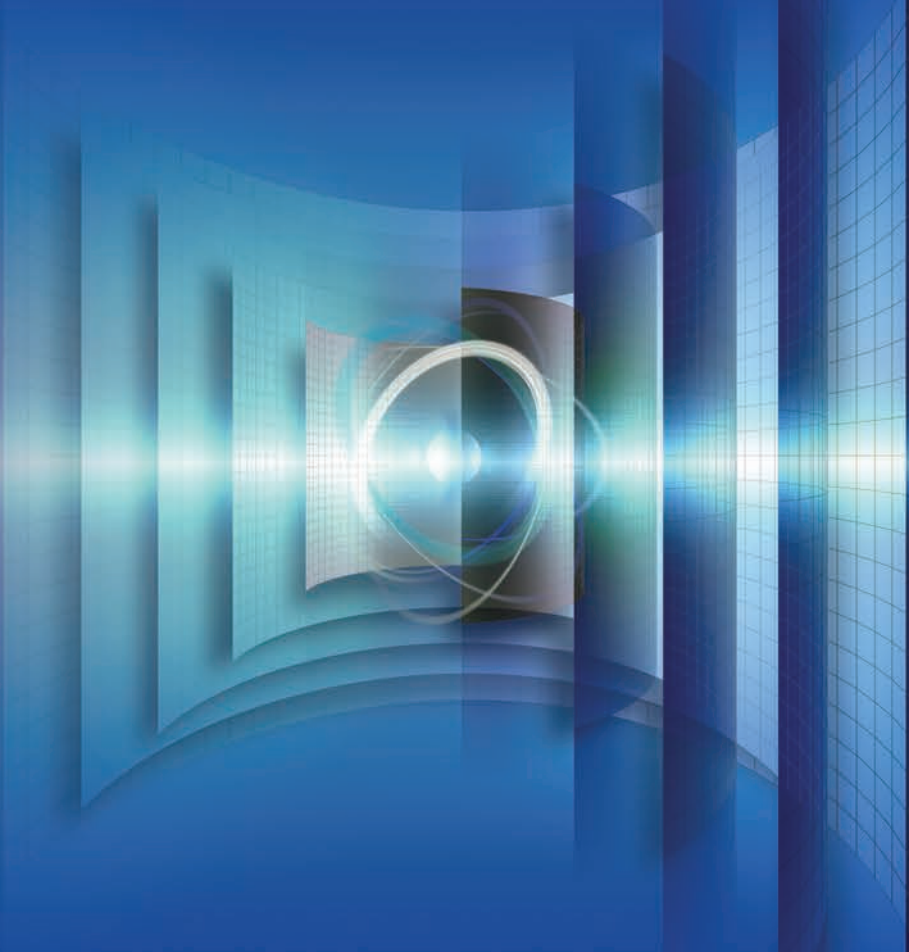


دليل التنفيذ

الأمن الحاسوبي  
لأغراض الأمن النووي



## سلسلة الأمن النووي الصادرة عن الوكالة

تعالج سلسلة الأمن النووي الصادرة عن الوكالة قضايا الأمن النووي المتعلقة بمنع وكشف الأفعال الإجرامية أو المتعمدة غير المأذون بها المنظوية على مواد نووية أو مواد مشعة أخرى أو ما يرتبط بذلك من مرافق أو أنشطة، أو المستهدفة لها، والتصدي لتلك الأفعال. وتتسق هذه المنشورات مع الصكوك الدولية المتعلقة بالأمن النووي، وتكملها، مثل اتفاقية الحماية المادية للمواد النووية وتعديلها، والاتفاقية الدولية لقمع أعمال الإرهاب النووي، وقراري مجلس الأمن التابع للأمم المتحدة رقم 1373 و1540، ومدونة قواعد السلوك بشأن أمان المصادر المشعة وأمنها.

### فئات سلسلة الأمن النووي الصادرة عن الوكالة

تصدر منشورات سلسلة الأمن النووي الصادرة عن الوكالة في الفئات التالية:

- **أساسيات الأمن النووي** التي تحدد هدف نظام أمن نووي لدولة ما والعناصر الأساسية لنظام من ذلك القبيل. وتوفر الأساس لتوصيات الأمن النووي.
- **توصيات الأمن النووي** التي تحدد التدابير التي ينبغي أن تتخذها الدول من أجل تحقيق وتعهّد نظام أمن نووي وطني فعال يتّسق مع أساسيات الأمن النووي.
- **أدلة التنفيذ** التي تقدّم إرشادات عن الوسائل التي يمكن للدول أن تنفذ من خلالها التدابير المحددة في توصيات الأمن النووي. وبهذا، تركز على كيفية العمل بالتوصيات المتعلقة بمجالات واسعة للأمن النووي.
- **الإرشادات التقنية** تقدّم إرشادات عن مواضيع تقنية محدّدة لاستكمال الإرشادات المحددة في أدلة التنفيذ. وهي تركز على تفاصيل كيفية تنفيذ التدابير الضرورية.

### الصياغة والاستعراض

يشارك في إعداد منشورات سلسلة الأمن النووي واستعراضها أمانة الوكالة، وخبراء من الدول الأعضاء (الذين يساعدون الأمانة في صياغة المنشورات) ولجنة إرشادات الأمن النووي، التي تستعرض وتعتمد مسودة المنشورات. وعند الاقتضاء، تُعقد أيضاً اجتماعات تقنية مفتوحة العضوية خلال عملية الصياغة من أجل إتاحة الفرصة للأخصائيين من الدول الأعضاء والمنظمات الدولية المعنية لاستعراض ومناقشة مسودة النص. وإضافة إلى ذلك، ولضمان مستوى رفيع من الاستعراض وتوافق الآراء على الصعيد الدولي، تعرض الأمانة مسودات النصوص على جميع الدول الأعضاء لفترة 120 يوماً لكي تستعرضها استعراضاً رسمياً.

وتُعدّ الأمانة لكل منشور الخطوات التالية، التي توافق عليها لجنة إرشادات الأمن النووي على مراحل متتالية ضمن عملية الإعداد والاستعراض:

- عرضاً وخطة عمل يصفان المنشور المتوخى الجديد أو المنقّح، وغرضه المستهدف ونطاقه ومحتواه؛
- مسودة منشور لعرضها على الدول الأعضاء للتعليق عليها خلال فترة 120 يوماً الاستشارية؛
- صيغة نهائية لمسودة المنشور مع مراعاة تعليقات الدول الأعضاء.

وثرّاعى في عملية صياغة واستعراض المنشورات في سلسلة الأمن النووي الصادرة عن الوكالة اعتبارات السرية، ويسلم فيها بأن الأمن النووي يتصل اتصالاً متلازماً بشواغل الأمن الوطني العامة والمحددة.

وأحد الاعتبارات المستند إليها هو أن معايير أمان الوكالة وأنشطتها الرقابية ذات الصلة ينبغي أن توضع في الاعتبار في المضمون التقني للمنشورات. وعلى وجه التحديد، تقوم اللجان المعنية بمعايير الأمان ذات الصلة ولجنة إرشادات الأمن النووي باستعراض منشورات سلسلة الأمن النووي التي تعالج المجالات التي يوجد فيها ترابط مع الأمان المعروفة بوثائق الترابط - في كل مرحلة من المراحل المحددة أعلاه.

الأمن الحاسوبي لأغراض الأمن النووي

الدول الأعضاء في الوكالة الدولية للطاقة الذرية

|                           |                             |                               |                            |
|---------------------------|-----------------------------|-------------------------------|----------------------------|
| الاتحاد الروسي            | بوروندي                     | سري لانكا                     | لاتفيا                     |
| إثيوبيا                   | البوسنة والهرسك             | السلفادور                     | لبنان                      |
| أذربيجان                  | بولندا                      | سلوفاكيا                      | لختنشتاين                  |
| الأرجنتين                 | بوليفيا، دولة -             | سلوفينيا                      | لكسمبورغ                   |
| الأردن                    | المتعددة القوميات           | سنغافورة                      | ليبيا                      |
| أرمينيا                   | بيرو                        | السنغال                       | ليبيريا                    |
| إريتريا                   | بيلاروس                     | السودان                       | ليتوانيا                   |
| إسبانيا                   | تايلند                      | السويد                        | ليسوتو                     |
| أستراليا                  | تركمانستان                  | سويسرا                        | مالطة                      |
| إستونيا                   | تركيا                       | سيراليون                      | مالي                       |
| إسرائيل                   | ترينيداد وتوباغو            | سيشيل                         | ماليزيا                    |
| إسواتيني                  | تشاد                        | شيلي                          | مدغشقر                     |
| أفغانستان                 | توغو                        | صربيا                         | مصر                        |
| إكوادور                   | تونس                        | الصين                         | المغرب                     |
| ألبانيا                   | تونغا                       | طاجيكستان                     | مقدونيا الشمالية           |
| ألمانيا                   | جامايكا                     | العراق                        | المكسيك                    |
| الإمارات العربية المتحدة  | الجبيل الأسود               | عُمان                         | ملاوي                      |
| أنغيغوا وبربودا           | الجزائر                     | غابون                         | المملكة العربية السعودية   |
| إندونيسيا                 | جزر البهاما                 | غانا                          | المملكة المتحدة لبريطانيا  |
| أنغولا                    | جزر القمر                   | غرينادا                       | العظمى وأيرلندا الشمالية   |
| أوروغواي                  | جزر مارشال                  | غواتيمالا                     | منغوليا                    |
| أوزبكستان                 | جمهورية أفريقيا الوسطى      | غيانا                         | موريتانيا                  |
| أوغندا                    | الجمهورية التشيكية          | فانواتو                       | موريشيوس                   |
| أوكرانيا                  | الجمهورية الدومينيكية       | فرنسا                         | موزامبيق                   |
| إيران (جمهورية-الإسلامية) | الجمهورية العربية السورية   | الفلبين                       | موناكو                     |
| آيرلندا                   | جمهورية الكونغو الديمقراطية | فنزويلا (جمهورية-البوليفارية) | ميانمار                    |
| آيسلندا                   | جمهورية تنزانيا المتحدة     | فنلندا                        | ناميبيا                    |
| إيطاليا                   | جمهورية كوريا               | فيجي                          | النرويج                    |
| بابوا غينيا الجديدة       | جمهورية لاو                 | فيت نام                       | النمسا                     |
| باراغواي                  | الديمقراطية الشعبية         | قبرص                          | نيبال                      |
| باكستان                   | جمهورية مولدوفا             | قطر                           | النيجر                     |
| بالاو                     | جنوب أفريقيا                | قيرغيزستان                    | نيجيريا                    |
| البحرين                   | جورجيا                      | كازاخستان                     | نيكاراغوا                  |
| البرازيل                  | جيبوتي                      | الكاميرون                     | نيوزيلندا                  |
| بربادوس                   | الدانمرك                    | الكرسي الرسولي                | هايتي                      |
| البرتغال                  | دومينيكا                    | كرواتيا                       | الهند                      |
| بروناي دار السلام         | رواندا                      | كمبوديا                       | هندوراس                    |
| بلجيكا                    | رومانيا                     | كندا                          | هونغاري                    |
| بلغاريا                   | زامبيا                      | كوبا                          | هولندا                     |
| بليز                      | زمبابوي                     | كوستاريكا                     | الولايات المتحدة الأمريكية |
| بنغلاديش                  | ساموا                       | كولومبيا                      | اليابان                    |
| بنما                      | سان مارينو                  | الكونغو                       | اليمن                      |
| بنن                       | سانت فنسنت وجزر غرينادين    | الكويت                        | اليونان                    |
| بوتسوانا                  | سانت كيتس ونيفس             | كينيا                         |                            |
| بوركينافاسو               | سانت لوسيا                  |                               |                            |

وافق المؤتمر المعني بالنظام الأساسي للوكالة الدولية للطاقة الذرية الذي عُقد في المقرّ الرئيسي للأمم المتحدة في نيويورك، في 23 تشرين الأول/أكتوبر 1956، على النظام الأساسي للوكالة الذي بدأ نفاذه في 29 تموز/يوليه 1957. ويقع المقرّ الرئيسي للوكالة في فينينا. ويتمثل هدف الوكالة الرئيسي في "تعزيز وتوسيع مساهمة الطاقة الذرية في السلام والصحة والازدهار في العالم أجمع".

العدد 42-G من سلسلة الأمن النووي الصادرة عن الوكالة

# الأمن الحاسوبي لأغراض الأمن النووي

دليل التنفيذ

الوكالة الدولية للطاقة الذرية

فيينا، 2022

## ملاحظة بشأن حقوق النشر

جميع منشورات الوكالة العلمية والتقنية محمية بموجب أحكام الاتفاقية العالمية لحقوق النشر بشأن الملكية الفكرية بصيغتها المعتمدة في عام 1952 (برن) والمنقحة في عام 1972 (باريس). وقد تم تمديد حق النشر منذ ذلك الحين بواسطة المنظمة العالمية للملكية الفكرية (جنيف) ليشمل الملكية الفكرية الإلكترونية والفعالية. ويجب الحصول على إذن باستخدام النصوص الواردة في منشورات الوكالة بشكل مطبوع أو إلكتروني، استخداماً كلياً أو جزئياً؛ ويخضع هذا الإذن عادة لاتفاقيات حقوق النشر والإنتاج الأدبي. ويُرحَّب بأية اقتراحات تخص الاستنساخ والترجمة لأغراض غير تجارية، وسيُنظَر فيها على أساس كل حالة على حدة. وينبغي توجيه أية استفسارات إلى قسم النشر التابع للوكالة (IAEA Publishing Section) على العنوان التالي:

Marketing and Sales Unit, Publishing Section  
International Atomic Energy Agency  
Vienna International Centre  
PO Box 100  
1400 Vienna, Austria  
fax: +43 1 26007 22529  
tel.: +43 1 2600 22417  
email: sales.publications@iaea.org  
<https://www.iaea.org/publications/ar/almanshurat>

حقوق النشر محفوظة للوكالة الدولية للطاقة الذرية، 2022

طُبِعَ من قِبَل الوكالة الدولية للطاقة الذرية في النمسا

نوفمبر 2022

STI/PUB/1918

ISBN 978-92-0-639421-2 (نسخة ورقية) | 978-92-0-639221-8 (PDF) | 978-92-0-639321-5 (epub)

ISSN 2520-6923

## تصدير بقلم رافائيل ماريانو غروسي

### المدير العام

توفّر سلسلة الأمن النووي الصادرة عن الوكالة إرشادات خاصة بتوافق الآراء الدولي بشأن جميع جوانب الأمن النووي من أجل دعم الدول الأعضاء في عملها الهادف إلى الوفاء بمسؤولياتها في مجال الأمن النووي. وتضع الوكالة هذه الإرشادات وتتعهدها كجزء من دورها المركزي المتمثل في توفير الدعم والتنسيق على الصعيد الدولي فيما يتعلّق بالأمن النووي.

وأطلقت سلسلة الأمن النووي الصادرة عن الوكالة في عام 2006 وتقوم الوكالة بتحديثها تحديثاً مستمراً بالتعاون مع خبراء من الدول الأعضاء. وبصفتي المدير العام، ألتزم بكفالة أن تحافظ الوكالة على هذه المجموعة المتكاملة والشاملة والمتسقة من المنشورات الجيدة النوعية من إرشادات الأمن النووي المحدثة والميسورة الاستخدام والملائمة للغرض، وأن تعمل على تحسينها. وينبغي أن يتيح التطبيق الصحيح لهذه الإرشادات في استخدام العلم والتكنولوجيا النوويين مستوى عالياً من الأمن النووي وأن يوفر الثقة اللازمة للسماح بالاستخدام المستمر للتكنولوجيا النووية لصالح الجميع. والأمن النووي مسؤولية وطنية. وتكمل سلسلة الأمن النووي الصادرة عن الوكالة الصكوك القانونية الدولية المتعلقة بالأمن النووي، وهي بمثابة مرجع عالمي لمساعدة الأطراف على الوفاء بالتزاماتها. ومع أن إرشادات الأمن النووي ليست قانوناً ملزماً للدول الأعضاء، فإنها تُطبّق على نطاق واسع. وقد أصبحت نقطة مرجعية وقاسماً مشتركاً لا غنىَ عنهما بالنسبة للغالبية العظمى من الدول الأعضاء التي اعتمدت هذه الإرشادات لاستخدامها في اللوائح الوطنية لتعزيز الأمن النووي في توليد القوى النووية، ومفاعلات البحوث، ومرافق دورة الوقود، وكذلك في التطبيقات النووية في مجالات الطب، والصناعة، والزراعة، والبحوث.

وتستند الإرشادات الواردة في سلسلة الأمن النووي الصادرة عن الوكالة إلى الخبرة العملية للدول الأعضاء فيها، ويتّصل إليها من خلال توافق الآراء الدولي. وتتسم مشاركة أعضاء لجنة إرشادات الأمن النووي وآخرين بأهمية خاصة، وأنا ممتن لجميع أولئك الذين يساهمون بمعرفتهم وخبراتهم في هذا المسعى. وتستخدم الوكالة أيضاً الإرشادات في سلسلة الأمن النووي الصادرة عن الوكالة عندما تقوم بمساعدة الدول الأعضاء من خلال بعثاتها الاستعراضية وخدماتها الاستشارية.

ويساعد ذلك الدول الأعضاء في تطبيق هذه الإرشادات ويتيح تقاسم الخبرات والرؤى والقيّمة. وخلال التنقيح الدوري للإرشادات، تؤخذ في الحسبان التعقيبات الواردة من هذه البعثات والخدمات، والدروس المستخلصة من الأحداث والخبرات في استخدام إرشادات الأمن النووي وتطبيقها.

وأعتقد أن الإرشادات المقدمة في سلسلة الأمن النووي الصادرة عن الوكالة وتطبيقها يساهمان إسهاما قيما في ضمان مستوى عال من الأمن النووي في استخدام التكنولوجيا النووية. وأحث جميع الدول الأعضاء على تعزيز هذه الإرشادات وتطبيقها، وعلى العمل مع الوكالة من أجل المحافظة على جودتها، في الحاضر وفي المستقبل.

### ملحوظة تحريرية

الإرشادات الواردة في سلسلة الأمن النووي الصادرة عن الوكالة هي إرشادات غير مُلزمة للدول، ولكن يجوز أن تَستخدِم الدول الإرشادات لكي تساعد على الوفاء بالتزاماتها بمقتضى الصكوك القانونية الدولية وعلى الاضطلاع بمسؤولياتها المتصلة بالأمن النووي داخل الدولة. وتهدف الإرشادات المعبّر عنها بجملة تبدأ بالفعل "ينبغي" إلى عرض الممارسات الدولية الجيدة والإشارة إلى إجماع دولي بأنّ من الضروري أن تتخذ الدول الإجراءات الموصى بها أو ما يعادل ذلك من تدابير بديلة.

ويجب أن تُفهم المصطلحات ذات الصلة بالأمن حسب تعريفها الوارد في المنشور الذي ترد فيه، أو في الإرشادات الأعلى درجة التي يدعمها المنشور. وفي غير ذلك من الحالات، فإنّ الكلمات تُستخدَم بمعانيها المتعارف عليها.

ويُعتَبَر التذييل جزءًا لا يتجزأ من المنشور. ويكون للمواد الواردة في أي تذييل نفس صفة المتن. وتُستخدَم المرفقات لتوفير معلومات أو تفسيرات إضافية. ولا تُعتَبَر المرفقات أجزاءً لا تتجزأ من النص الرئيسي.

وعلى الرغم من توخي قدر كبير من الحرص للحفاظ على دقة المعلومات الواردة في هذا المنشور، لا تتحمل الوكالة ولا دولها الأعضاء أي مسؤولية عن العواقب التي قد تنشأ عن استخدام تلك المعلومات.

واستخدام تسميات معيّنة لبلدان أو أقاليم لا يعني ضمناً إصدار أي حكم من جانب الناشر، أي الوكالة، بشأن الوضع القانوني لهذه البلدان أو الأقاليم أو سلطاتها ومؤسساتها أو تعيين حدودها.

وذكر أسماء شركات أو منتجات معيّنة (سواء مع الإشارة إلى أنها مسجّلة أو دون تلك الإشارة) لا يعني ضمناً وجود أي نية لانتهاك حقوق الملكية، كما لا ينبغي أن يُفسّر على أنه تأييد أو توصية من جانب الوكالة.

## المحتويات

|    |                                                                                |
|----|--------------------------------------------------------------------------------|
| 1  | 1 - مقدّمة .....                                                               |
| 1  | الخلفية (1-1 — 9-1) .....                                                      |
| 3  | الغرض من المنشور (10-1 — 11-1) .....                                           |
| 3  | النطاق (12-1 — 14-1) .....                                                     |
| 4  | هيكل الدليل (15-1 — 16-1) .....                                                |
| 5  | 2- المفاهيم والسياق .....                                                      |
| 5  | أهم المصطلحات (1-2 — 9-2) .....                                                |
| 8  | تحديد الأصول الرقمية الحساسة (10-2 — 20-2) .....                               |
| 12 | الهجوم السيبراني (21-2 — 23-2) .....                                           |
| 13 | الأمن الحاسوبي في مختلف مجالات الأمن النووي (24-2 — 30-2) .....                |
| 14 | التحديات وجوانب الضعف ونظم الأمن الحاسوبي (31-2 — 52-2) .....                  |
| 21 | الكفاءات والقدرات في مجال الأمن الحاسوبي (53-2) .....                          |
| 22 | 3- الأدوار والمسؤوليات المنوطة بالدولة (1-3) .....                             |
| 22 | الاعتبارات التشريعية والرقابية (2-3 — 9-3) .....                               |
| 24 | السلطة المختصة بالأمن الحاسوبي في إطار منظومة الأمن النووي (10-3 — 16-3) ..... |
| 25 | أوجه الترابط مع المجالات الأخرى (17-3 — 38-3) .....                            |
|    | 4- الأدوار والمسؤوليات المنوطة بالسلطات المختصة والجهات المشغلة                |
| 30 | (1-4 — 9-4) .....                                                              |
| 32 | العمل مع البائعين والمتعاقدين والموردين (10-4 — 11-4) .....                    |
| 32 | السلطة المختصة بالأمن الحاسوبي (12-4 — 26-4) .....                             |
| 35 | الهيئة الرقابية (27-4 — 32-4) .....                                            |

37 5- وضع استراتيجية الأمن الحاسوبي ..... 37

37 استراتيجية الأمن الحاسوبي في إطار منظومة الأمن النووي (1-5 — 4-5) ..... 37  
38 تقييم التهديدات السيبرانية لمنظومة الأمن النووي (5-5 — 15-5) ..... 38  
40 تعيين سلطة مختصة بتقييم التهديدات السيبرانية (16-5 — 18-5) ..... 40  
41 تقييم الأثر المترتب على اختلال تشغيل الأصول الرقمية الحساسة (19-5 — 25-5) ..... 41  
43 طريقة تقييم المخاطر لتحديد تدابير الأمن الحاسوبي (26-5 — 29-5) ..... 43

44 6- تنفيذ استراتيجية الأمن الحاسوبي (1-6 — 3-6) ..... 44

45 إسناد المسؤوليات المتعلقة بالأمن الحاسوبي (4-6 — 7-6) ..... 45  
45 العلاقات بين السلطات المختصة والجهات المشغلة (8-6 — 13-6) ..... 45  
47 الكفاءات والقدرات في مجال الأمن الحاسوبي (14-6 — 19-6) ..... 47  
48 التصدي لحوادث الأمن الحاسوبي (20-6 — 24-6) ..... 48  
49 التمارين (25-6 — 26-6) ..... 49  
49 الأنشطة التوكيدية (27-6 — 33-6) ..... 49  
51 التعاون والمساعدة على الصعيد الدولي (34-6) ..... 51

51 7- وضع برنامج للأمن الحاسوبي (1-7 — 4-7) ..... 51

52 محتويات برنامج الأمن الحاسوبي (5-7 — 9-7) ..... 52  
55 تقييم المخاطر على مستوى المنظمة الواحدة (10-7 — 16-7) ..... 55  
56 تدابير الأمن الحاسوبي (17-7 — 18-7) ..... 56  
57 اتباع نهج متدرج في تحديد تدابير الأمن الحاسوبي (19-7 — 21-7) ..... 57  
58 تصميم تدابير الأمن الحاسوبي (22-7 — 23-7) ..... 58  
58 الدفاع في العمق في سياق تدابير الأمن الحاسوبي (24-7) ..... 58  
58 إدارة شؤون البائعين والمتعاقدين والموردين (25-7 — 32-7) ..... 58

60 8- المحافظة على استدامة الأمن الحاسوبي (1-8 — 4-8) ..... 60

61 ثقافة الأمن (5-8 — 7-8) ..... 61  
61 التدريب (8-8 — 20-8) ..... 61

|     |                                                                   |
|-----|-------------------------------------------------------------------|
| 63  | ..... خطط الطوارئ والتصدي (21-8 — 27-8)                           |
| 64  | ..... أنشطة توكيد الأمن الحاسوبي (28-8 — 30-8)                    |
|     | التذييل: اعتبارات متعلقة بالترابط مع الأمان النووي لأغراض الأمن   |
| 66  | ..... الحاسوبي في المرافق                                         |
| 70  | ..... المراجع                                                     |
|     | المرفق الأول: إرشادات في شكل توصيات مقترحة بشأن الأمن الحاسوبي    |
| 72  | ..... لأغراض منظومة الأمن النووي الوطنية                          |
| 79  | ..... أنماط التهديدات السيبرانية                                  |
| 93  | ..... المرفق الثاني: إسناد المسؤوليات المتعلقة بالأمن الحاسوبي    |
|     | المرفق الرابع: مثال لإطار الكفاءات ومستويات القدرات في مجال الأمن |
| 96  | ..... الحاسوبي                                                    |
| 100 | ..... مسرد المصطلحات                                              |



## 1- مقدمة

### الخلفية

1-1- تؤدي النظم الحاسوبية دوراً أساسياً في جميع الجوانب التي ينطوي عليها التشغيل المأمون والأمن للمرافق والأنشطة المرتبطة باستخدام المواد النووية والمواد المشعة الأخرى وبخزن تلك المواد ونقلها، بما في ذلك المحافظة على الحماية المادية، كما تؤدي دوراً أساسياً في التدابير المتخذة للكشف عن المواد الخارجة عن التحكم الرقابي والتعامل معها. ولذلك فإن جميع هذه النظم الحاسوبية تتطلب الحماية الأمنية في مواجهة الأعمال الإجرامية أو المتعمدة غير المأذون بها. ومع تطور التكنولوجيا، من المتوقع أن يتزايد استخدام النظم الحاسوبية في جميع جوانب العمليات التشغيلية، بما في ذلك في سياقي الأمن النووي والأمان النووي.

2-1- وتشدد أساسيات الأمن النووي [1] على الأهمية التي يحظى بها أمن المعلومات، بما يشمل الأمن الحاسوبي، ضمن إطار منظومة الأمن النووي، وعلى الحاجة إلى تنفيذ أنشطة توكيدية لتحديد ومعالجة المسائل والعوامل التي يمكن أن تؤثر في القدرة على توفير مستوى ملائم من الأمن النووي، بما في ذلك الأمن الحاسوبي.

3-1- ويشكل أمن المعلومات الحساسة أحد مكونات العنصر 3 من العناصر الأساسية لمنظومة الأمن النووي الوطنية. وينص المرجع [1] على ما يلي: "ينبغي أن ينص الإطار التشريعي والرقابي والتدابير الإدارية ذات الصلة لتنظيم منظومة الأمن النووي... على وضع لوائح ومتطلبات لحماية سرية المعلومات الحساسة وحماية أصول المعلومات الحساسة". وتنطوي المحافظة على أمن المعلومات الحساسة وأصول المعلومات الحساسة على حماية سرية تلك المعلومات والأصول وسلامتها وتوافرها. وينص تعديل اتفاقية الحماية المادية للمواد النووية [2] أيضاً على حماية سرية المعلومات تحت عنوان المبدأ الأساسي لام.

4-1- وتنص الفقرة 4 10 من الوثيقة المعنونة "توصيات الأمن النووي بشأن الحماية المادية للمواد النووية والمرافق النووية" (الوثيقة [3] [INFCIRC/225/Revision 5]) على ما يلي:

"وينبغي [توفير الحماية للنظم الحاسوبية] المستخدمة في الحماية المادية والأمان النووي وفي حصر المواد النووية ومراقبتها [في مواجهة الأعمال التي تستهدف الإخلال

بها (مثل الهجوم السيبراني أو التلاعب أو التزوير) بما يتوافق مع [تقييم التهديدات] أو [وصف التهديدات المحتاط لها في التصميم]."

5-1- كما تشدد توصيات الأمن النووي بشأن المواد المشعة والمرافق ذات الصلة [4] وبسبب المواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي [5] على الحاجة لمنع الوصول غير المأذون به إلى المعلومات الحساسة وحمايتها من الإخلال بها. وترد في المرفق الأول إرشادات في شكل توصيات استكمالاً للتوصيات الواردة في المراجع [3-5] إلى حين تنقيح هذه المنشورات في المستقبل.

6-1- وعند معالجة المعلومات الحساسة ونقلها وتخزينها في شكل رقمي باستخدام النظم الحاسوبية، يلزم توفير الحماية الكافية لسرية تلك المعلومات وسلامتها وتوافرها، من خلال تنفيذ تدابير الأمن الحاسوبي الكفيلة بذلك طوال دورة عمر هذه الأصول الرقمية. ويشمل الأمن الحاسوبي التدابير اللازمة لمنع وقوع الهجمات السيبرانية، والكشف عنها والتصدي لها إذا وقعت، بما في ذلك إعادة النظم الحاسوبية المتضررة للعمل.

7-1- وقد وجدت الجهات التي تشكّل تهديدات للأمن النووي في الهجمات السيبرانية وسيلة لاستهداف النظم الحاسوبية من أجل تنفيذ أو تيسير الأعمال الشريرة، سواء بطريقة مباشرة أو عن طريق الجمع بينها وبين وسائل أكثر تقليدية مثل الوصول المادي والأطراف الداخلية. ويمكن لهذه الأعمال أن تؤدي إلى تعريض المواد النووية والمواد المشعة الأخرى للسحب دون إذن أو التخريب، وهو ما يمكن أن تترتب عليه عواقب إشعاعية غير مقبولة. ويمكن استغلال الهجمات السيبرانية أيضاً لتيسير ارتكاب أعمال إجرامية أو أعمال متعمدة أخرى غير مأذون بها، مثل تهريب المواد النووية أو مواد مشعة أخرى لإخراجها من التحكم الرقابي.

8-1- ومن ثم فبغية التصدي لتهديدات الأمن النووي المحتملة بكامل نطاقها، يلزم أن تشمل منظومة الأمن النووي على وسائل للتصدي للجهات التي تشكّل تهديدات والتي لديها بالفعل المهارات اللازمة لاستهداف النظم الحاسوبية بهجمات سيبرانية أو يمكن أن تكتسب تلك المهارات. وبالإضافة إلى ذلك، فإذا كانت الجهات التي تشكّل تهديدات للأمن النووي لا تتمتع بالمهارات اللازمة بنفسها، يمكنها أن تحمل أفراداً آخرين ممن لديهم هذه المهارات على مساعدتها (على سبيل المثال عن طريق دفع مقابل مالي لهم أو إكراههم على ذلك).

9-1- وتمثل المحافظة على الأمن الحاسوبي بفعالية في المرافق التي تتعامل مع المواد النووية أو مواد مشعة أخرى، وفي الأنشطة ذات الصلة مثل النقل، تحدياً كبيراً، بالنظر إلى ضخامة التهديدات وسرعة تطورها. وتضم منظومة الأمن النووي الخاصة بالدولة العديد من العناصر الأساسية التي تعتمد على نظم حاسوبية أو تُنفَّذ بدعم من نظم حاسوبية، ومن ثم يتوقف تنفيذها على الأمن الحاسوبي الفعال.

## الغرض من المنشور

10-1- الغرض من هذا المنشور هو تقديم إرشادات بشأن إرساء وتنفيذ الأمن الحاسوبي باعتباره مكوناً أصيلاً من مكونات الأمن النووي.

11-1- وهذا الدليل التنفيذي موجّه لواقعي السياسات، والسلطات المختصة، والجهات المشغلة والشاحنة والناقلة وغيرها من الجهات المكلفة بمسؤوليات متعلقة بالأمن والأمان النوويين.

## النطاق

12-1- تنطبق الإرشادات الواردة في هذا المنشور على الجوانب المتصلة بالأمن النووي وبالترابط بينه وبين الأمان النووي وسائر عناصر منظومة الأمن النووي في الدولة، مثل الحماية المادية للمواد النووية والمرافق النووية، وأمن المواد المشعة والمرافق والأنشطة المرتبطة بها، والكشف عن الأحداث المتصلة بالأمن النووي والتصدي لها. ويشمل نطاق هذا المنشور النظم الحاسوبية التي يمكن أن يؤدي الإخلال بها إلى التأثير سلباً في الأمن النووي أو الأمان النووي.

13-1- ويتناول هذا المنشور الأمن الحاسوبي من حيث جوانبه العامة المنطبقة على جميع مجالات الأمن النووي، بما في ذلك الجوانب المتعلقة بالمواد النووية والمرافق النووية، والمواد المشعة الأخرى والمرافق المرتبطة بها، والمواد النووية والمرافق المشعة الأخرى الخارجة عن التحكم الرقابي. ويمكن الاطلاع على إرشادات أكثر تفصيلاً بشأن الأمن الحاسوبي في السياق المحدد لأمن المرافق النووية، بما في ذلك أمثلة تركز على الجوانب التقنية في تنفيذ تدابير الأمن الحاسوبي وإدارة مخاطر الأمن الحاسوبي،

في عديدين من سلسلة الأمن النووي الصادرة عن الوكالة هما العدد T-33، المعنون Computer Security of Instrumentation and Control Systems at Nuclear Facilities ("الأمن الحاسوبي لنظم الأجهزة والتحكم في المرافق النووية") [6]، والعدد T-17 (الصيغة المنقحة، Rev. 1) المعنون Computer Security Techniques for Nuclear Facilities ("تقنيات الأمن الحاسوبي لأغراض المرافق النووية") [7].

14-1- ويحيل هذا المنشور إلى ما يرد في أساسيات الأمن النووي [1] وفي توصيات الأمن النووي [3-5] من الإرشادات المتعلقة بأمن المعلومات، لكنه لا يقدم إرشادات مفصلة بشأن هذا الموضوع العام. ويقدم العدد G-23 من سلسلة الأمن النووي الصادرة عن الوكالة، المعنون "أمن المعلومات النووية"، إرشادات بشأن أمن المعلومات النووية وتحديد المعلومات الحساسة وأصول المعلومات الحساسة وضمان أمنها.

## هيكल الدليل

15-1- عقب هذه المقدمة، يعرض القسم 2 المصطلحات والمفاهيم الرئيسية. ويبيّن القسم 3 الأدوار والمسؤوليات المنوطة بالدولة فيما يتعلق بالأمن الحاسوبي ضمن منظومة الأمن النووي، في حين يبيّن القسم 4 الأدوار والمسؤوليات المنوطة بالكيانات المعنية. ويصف القسم 5 الأنشطة التي تضطلع بها الدولة عند وضع استراتيجية للأمن الحاسوبي لأغراض الأمن النووي، في حين يصف القسم 6 أنشطة تنفيذ هذه الاستراتيجية. ويصف القسم 7 العناصر والتدابير التي يتألف منها برنامج الأمن الحاسوبي<sup>1</sup>. ويصف القسم 8 الأنشطة اللازمة للمحافظة على استدامة الأمن الحاسوبي. ويعرض التذييل اعتبارات تقنية مهمة تتعلق بأوجه الترابط مع الأمان النووي.

16-1- ويقدم المرفق الأول إرشادات في شكل توصيات مقترحة بشأن الأمن الحاسوبي لأغراض منظومة الأمن النووي الوطنية، بما يتوافق مع الإرشادات التنفيذية الواردة في هذا المنشور. ودعماً للإرشادات الواردة في هذا المنشور، تقدم المرفقات من الثاني إلى الرابع أمثلة للتدابير التنفيذية الممكنة. ويقدم المرفق الثاني لمحة عامة عن أنماط التهديدات السيبرانية. ويقدم المرفق الثالث أمثلة للطريقة المتبعة في إسناد

---

<sup>1</sup> قد تطلق بعض المنظمات على برنامج الأمن الحاسوبي اسم "خطة الأمن الحاسوبي".

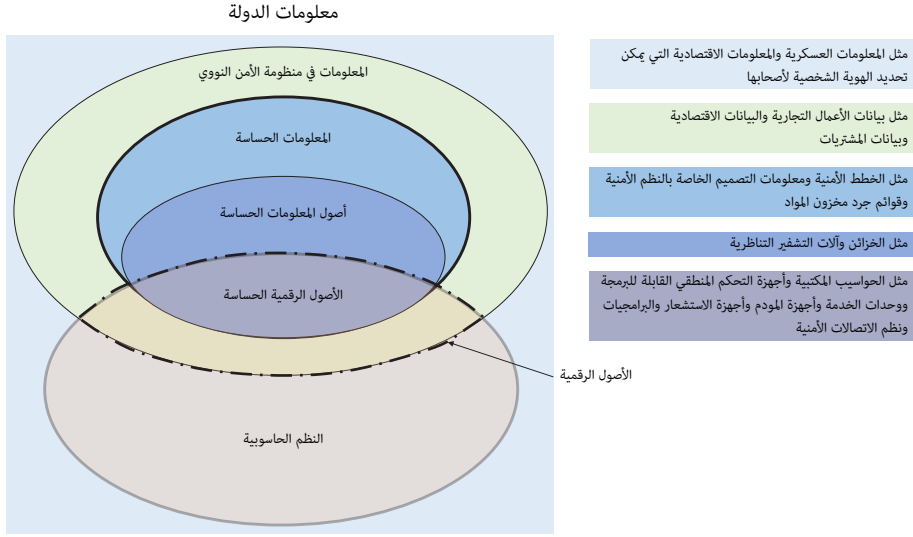
المسؤوليات المتعلقة بالأمن الحاسوبي في منظومة الأمن النووي، ويقدم المرفق الرابع توضيحاً لإطار كفاءات الأمن الحاسوبي.

## 2- المفاهيم والسياق

### أهم المصطلحات

1-2- ينطوي العمل الذي تقوم به المنظمات داخل الدولة على أنشطة تتعلق بأنواع عديدة من المعلومات، بما في ذلك إيجاد هذه المعلومات ومعالجتها والتعامل معها وتخزينها. ومن بين هذه المعلومات، هناك بعض الأنواع التي قد تُعتبر حساسة بما فيه الكفاية بحيث تتطلب مستوى معيناً من الحماية، مثل الأسرار العسكرية أو المعلومات الشخصية الخاصة بالمواطنين. وقد تسنّ الدولة قوانين وطنية لتنظيم أمن المعلومات تنصّ فيها على تعريف أنواع المعلومات وتصنيفها وتحدد متطلبات الحماية المحددة اللازمة لها، بما في ذلك فيما يخص البيانات الموجودة في شكل رقمي والنظم الحاسوبية المرتبطة بها. وفي هذه الحالة، تخضع المعلومات الموجودة في منظومة الأمن النووي الخاصة بالدولة لهذه المتطلبات، وقد تتطلب توفير الحماية لأنواع أخرى من المعلومات، أو توفير حماية إضافية للأنواع المحددة من المعلومات التي يمكن أن يؤدي الإخلال بأمنها إلى مساعدة خصم على تنفيذ عمل شرير ضد أحد المرافق أو الأنشطة أو ارتكاب عمل إجرامي أو عمل آخر متعمد غير مأذون به باستخدام مواد نووية أو مواد مشعة أخرى. وتُعرّف المعلومات الحساسة بأنها المعلومات الموجودة في أي شكل من الأشكال، بما في ذلك البرامج الحاسوبية، والتي يمكن أن يؤدي إفشاؤها أو تعديلها أو تبديلها أو إتلافها دون إذن أو الحرمان من استخدامها إلى الإخلال بالأمن النووي [1]. ويوضّح الشكل 1 مفاهيم أصول المعلومات الحساسة والنظم الحاسوبية والأصول الرقمية الحساسة والعلاقات فيما بينها. ويرد وصف هذه المفاهيم بمزيد من التفصيل أدناه.

2-2- وتُعرّف أصول المعلومات الحساسة [1] بأنها أي معدات أو مكونات تُستخدم لتخزين المعلومات الحساسة أو معالجتها أو التحكم فيها أو إرسالها. ويمكن أن تكون المعلومات الحساسة موجودة في شكل رقمي أو في أي شكل آخر.



الشكل 1-1- المعلومات والنظم الحاسوبية في الدولة وفي منظومة الأمن النووي

3-2- والنظم الحاسوبية هي التكنولوجيات التي تُنتج المعلومات الرقمية أو تتيح الوصول إليها أو تعالجها أو ترسلها أو تخزنها، أو التي تؤدي خدمات تنطوي على هذه المعلومات أو تقدم خدمات من هذا القبيل أو تتحكم فيها. ويمكن أن تشمل هذه النظم: الحواسيب المكتبية والنقالة واللوحية وغيرها من الحواسيب الشخصية، والهواتف الذكية، والحواسيب الكبيرة، ووحدات الخدمة، والأجهزة الرقمية وأجهزة التحكم الرقمي، والطابعات، وأجهزة الشبكات، والمكونات والأجهزة المدمجة. ويمكن لهذه النظم أن تشمل أيضاً الخدمات الافتراضية مثل الحوسبة السحابية أو الأجهزة الافتراضية. وقد توجد هذه النظم في شكل مكون واحد أو في شكل مجموعة من الأصول الرقمية.

4-2- وتؤدي النظم الحاسوبية العديد من الوظائف في أي دولة. وقد تشمل منظومة الأمن النووي على نظم حاسوبية تؤدي وظائف بالغة الأهمية على مستوى الأعمال والاتصالات دون أن تكون حساسة من منظور الأمن النووي ومن ثم لا تدخل في نطاق الإرشادات الواردة في هذا المنشور.

5-2- ويلزم توفير الحماية لأصول المعلومات الحساسة لمنع الإخلال بأمن المعلومات الحساسة التي تخزنها تلك الأصول أو تتحكم فيها أو ترسلها. وتختلف النهج المتبعة في توفير الحماية باختلاف نوع الأصل المعني وشكل المعلومات ذات الصلة. ويتناول المرجع

[8] في المقام الأول حماية المعلومات المكتوبة في شكل ورقي وغيرها من المعلومات الموجودة في شكل "مادي". والأصول الرقمية هي نظم حاسوبية (أو جزء من نظم حاسوبية) مرتبطة بمنظومة الأمن النووي الخاصة بالدولة أو تشكّل جزءاً منها. ويُستخدم تعبير "الأصول الرقمية الحساسة" للإشارة إلى أصول المعلومات الحساسة المؤلفة من نظم حاسوبية (أو التي تشكل أجزاءً من نظم حاسوبية). وتتطلب حماية الأصول الرقمية الحساسة اتخاذ تدابير للأمن الحاسوبي.

6-2- وهناك أصول رقمية حساسة تدعم النظم التي تؤدي وظائف متعلقة بالأمان النووي وبالأمن النووي وبحصر المواد النووية ومراقبتها، أو التي تخزن وتعالج المعلومات الحساسة المتصلة بهذه الوظائف. وقد تكون الأصول الرقمية الحساسة، ومن ثم الوظائف الأساسية التي تؤديها، معرضة للهجمات السيبرانية، ويمكن أن يستهدف الخصوم تلك الأصول بالتحديد. وفي حال وقوع هجوم من هذا القبيل والإخلال بأمن الأصول الرقمية الحساسة، فإن ذلك يمكن أن يؤدي إلى آثار سلبية تمس بالأمن والأمان النوويين. ويمكن للإخلال بأمن الأصول الرقمية الحساسة أن يسهم أو يتسبب فيما يلي، على سبيل المثال:

- (أ) تنفيذ عمل تخريبي يؤدي إلى عواقب إشعاعية غير مقبولة أو عواقب إشعاعية مرتفعة في حال إلحاق الضرر بمناطق حيوية؛
- (ب) سحب مواد نووية أو مواد مشعة أخرى دون إذن؛
- (ج) الانتقاص من القدرة على منع الأحداث المتصلة بالأمن النووي والكشف عنها والتصدي لها؛
- (د) فقدان معلومات حساسة أو تعديلها أو الحرمان من الوصول إليها.

7-2- وبحسب الحال، قد تلزم معاملة البرمجيات إما على أنها معلومات أو باعتبارها تشكّل جزءاً أصيلاً من النظام الحاسوبي المحتوي عليها، أو وفقاً للتصنيفين معاً. وعلى سبيل المثال، ففي مرحلة التصميم الأولي، قد تتخذ البرمجيات شكل تعبير عام عن خوارزمية معالجة، ومن ثم تكون المعاملة المثلى لها باعتبارها معلومات. أما حين تتخذ البرمجيات شكلها التشغيلي (أي القابل للتنفيذ)، فإنّها تشكّل جزءاً من النظام الحاسوبي الذي ترتبط به والذي لا يؤدي وظائفه من دونها، وتستهدف معظم الهجمات السيبرانية استغلال جوانب الضعف في تلك البرمجيات.

8-2- والأمن الحاسوبي هو جانب محدد من أمن المعلومات يتعلق بحماية النظم الحاسوبية مما قد يخل بها. ويشمل ذلك جميع الأنظمة والشبكات المترابطة المؤلفة

من تلك النظم. ولا يُستخدم مصطلحاً "أمن تكنولوجيا المعلومات" و"الأمن السيبراني" في هذا المنشور، لاعتبارهما مرادفين لمصطلح "الأمن الحاسوبي" في هذا السياق. والأمن الحاسوبي هو أحد فروع أمن المعلومات، كما هو مذكور في المرجع [8]. وعادة ما يشترك أمن المعلومات والأمن الحاسوبي في المقاصد والمنهجية والمصطلحات.

9-2- وبالنظر إلى الترابط بين الشبكات الحاسوبية وتدفق المعلومات فيما بينها، يلزم أيضاً اتخاذ تدابير للأمن الحاسوبي لحماية الأصول الرقمية الحساسة من التهديدات المنظوية على استغلال أصول رقمية أخرى ونظم حاسوبية أخرى. ومن ثم فإنّ اتباع نهج متعدد الطبقات يقوم على تطبيق تدابير أمنية متدرجة على جميع الأصول الرقمية يكفل الدفاع في العمق في مواجهة الهجمات السيبرانية.

### تحديد الأصول الرقمية الحساسة

10-2- ينبغي أن تتّبع الجهات المالكة للنظم الحاسوبية و/أو التي تصمّم هذه النظم عملية منهجية لتحديد الوظائف التي تؤديها أصول رقمية واللازمة للأمن والأمان النوويين، وأي أصول رقمية حساسة مرتبطة بهذه الوظائف، والتأثير المحتمل في الأمن والأمان النوويين في حالة الإخلال بأمن أي أصول رقمية حساسة. وعند الاضطلاع بهذه العملية، ينبغي للجهات المعنية أن تراعي أنّه قد توجد نظم حاسوبية لا تحتوي بذاتها على أصول رقمية حساسة، ومع ذلك ففي حال الإخلال بأمنها أو إصابتها ببرامجيات خبيثة<sup>2</sup> يمكن أن تؤثر في الأصول الرقمية الحساسة الموجودة في نظم أخرى.

11-2- ويهدف الأمن الحاسوبي إلى المحافظة على سرية المعلومات الحساسة الموجودة في الأصول الرقمية الحساسة وسرية الأصول الرقمية الحساسة نفسها، وعلى سلامة تلك المعلومات والأصول وتوافرها. وتدعم الأصول الرقمية الحساسة والمعلومات الحساسة الموجودة فيها التشغيل الصحيح للوظائف التي تقوم عليها منظومة الأمن النووي. وينبغي إيلاء الاعتبار الواجب للاحتياجات اللازمة لحماية كلّ سمة من هذه السمات، بناءً على الوظائف التي يؤديها كلّ أصل من الأصول الرقمية الحساسة وعلى المعلومات الحساسة التي يحتويها ذلك الأصل.

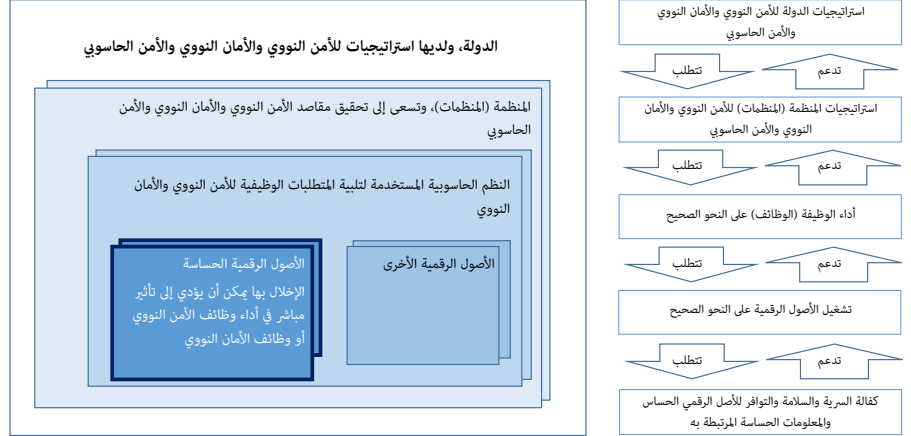
---

<sup>2</sup> البرامجيات الخبيثة (Malware) هي أي شكل من الشفرات الحاسوبية المصممة عمداً لتنفيذ عمل شرير. ويمكن أن يشمل ذلك تيسير سرقة المعلومات الحساسة أو الإخلال بتصميم نظام حاسوبي أو الإخلال بوظيفة يؤديها نظام حاسوبي.

12-2- وينبغي أن تكون الخطوة الأولى في العملية المنهجية المذكورة هي تحديد الوظائف التي توفّر دعماً مباشراً بجانب واحد أو أكثر من جوانب الأمن النووي (مثل الحماية المادية، وحصر المواد النووية ومراقبتها، وإدارة المعلومات الحساسة) والأمان النووي. وبعد ذلك ينبغي تحديد ما يدعم هذه الوظائف من النظم الحاسوبية والأصول الرقمية المكوّنة لها.

13-2- وينبغي بعد ذلك إجراء تحليل أولي للعواقب يتناول آثار الإخلال بأمن الأصول الرقمية الموجودة داخل هذه النظم، لتحديد الأصول التي يمكن أن يؤدي الإخلال بها بفعل هجوم سيبراني إلى التأثير في الوظائف المطلوبة من النظام ومن ثم التأثير سلباً في الأمن النووي. وبناءً على نتائج التحليل، تُصنّف الأصول الرقمية التي يمكن أن يؤدي الإخلال بها إلى آثار سلبية باعتبارها أصولاً رقمية حساسة. ويوضح الشكل 2 هذا المفهوم. وينبغي إجراء هذا التحليل الأولي دون أن تؤخذ في الحسبان تدابير الأمن الحاسوبي القائمة، للوقوف على التأثير الذي سيترتب "في أسوأ الحالات" إذا ما تعرضت الأصول الرقمية للإخلال بها.

14-2- وينبغي أن تشمل العملية المذكورة أيضاً تقييم نظم الدعم أو المعدات غير المرتبطة مباشرة بوظائف الأمن والأمان النوويين، للوقوف على ما إذا كان تعرّض هذه النظم أو المعدات لهجوم سيبراني يمكن أن يؤدي إلى تأثير مباشر أو غير مباشر في وظائف الأمن والأمان النوويين. وينبغي أن يخضع للتقييم أي أصل رقمي يمكن توصيله مؤقتاً بأصل رقمي حساس، بحيث يمكن تصنيفه أصلاً رقمياً حساساً بدوره. ومن أمثلة ذلك حواسيب الصيانة ومعدات الاختبار الرقمية.



الشكل 2- رسم تخطيطي مفاهيمي يبين أصلاً رقمياً حساساً ضمن نظام حاسوبي لدى إحدى المنظمات.

15-2- ويمكن للمنظمات أن تختار من بين عدد من الاستراتيجيات المختلفة لإدارة الأصول الرقمية الحساسة. ويمكنها تصنيف الأصول الرقمية الحساسة إلى فئات - على سبيل المثال، بناءً على انتمائها لنفس النظام أو بناءً على تشابه طبيعتها - وإخضاع جميع الأصول الرقمية الحساسة المصنفة ضمن فئة معينة للإدارة سويًا. وبذلك يمكن معاملة نظام حاسوبي يؤدي وظيفة مهمة على أنه أصل رقمي حساس واحد، أو باعتباره مؤلفاً من مجموعة من الأصول الرقمية الحساسة. ومن شأن هذا التصنيف أن يساعد على ضمان توفير مستويات مماثلة من الحماية للأصول الرقمية الحساسة المتشابهة من حيث العواقب التي يُحتمل أن تترتب على الإخلال بها. وبعد تحديد الأصول الرقمية الحساسة وتصنيفها وفقاً للعواقب المحتملة في حال الإخلال بها، يمكن تطبيق نهج متدرج بمراعاة مبدأ الدفاع في العمق.

16-2- وينبغي تحديد متطلبات السرية والسلامة والتوافر فيما يخص كل أصل رقمي حساس من خلال تقييم مساهمة ذلك الأصل في الأمن والأمان النوويين والعواقب التي يُحتمل أن تترتب على اختلال تشغيله بعد تعرّضه لهجوم سيبراني. وقد يستوجب تحديد تلك المتطلبات الاستناد إلى تقدير خبير متخصص، مع الاسترشاد بالمبادئ والعمليات التحليلية ذات الصلة.

17-2- وإلى حين تقييم النظام الحاسوبي لتحديد تصنيفه باعتباره أصلاً رقمياً حساساً (أو نظاماً مشتملاً على أصل رقمي حساس) من عدمه، ينبغي معاملته على أنه نظام "غير مصنف". وعادة ما ينبغي أن تكون تدابير الأمن الحاسوبي المطبقة على الأصول غير المصنفة شديدة الصرامة توجيهاً للحذر، لأن الآثار التي يُحتمل أن تترتب على تعرّض هذه الأصول لهجوم سيبراني ليست معروفة. وينبغي النظر في حظر أو تقييد استخدام هذا النوع من الأصول في منظومة الأمن النووي. وعلى سبيل المثال، يمكن حظر استخدام الأجهزة الشخصية الخاصة بالموظفين، مثل الهواتف النقالة والحواسيب اللوحية، داخل المرافق النووية؛ كما يمكن حظر توصيل الحواسيب المملوكة لأطراف ثالثة بأي نظام في مرفق نووي إلى حين خضوعها لتقييم كامل. ومن الجوانب الأساسية في تصميم نظام آمن التحديد السليم لما يشكل أصلاً رقمياً حساساً، ولنطاق ذلك الأصل وحدوده والوصلات التي تربطه بغيره، وللمستويات المقبولة للاعتماد على أصول رقمية أخرى، مما يستلزم الاستناد إلى تقدير الخبراء مع الاسترشاد بمبادئ الأمن الحاسوبي وهندسة النظم. وعلى سبيل المثال، فمن خلال تعديل تصميم النظام ككل بما يتيح نقل إمكانية أداء وظائف معينة فيما بين الأصول الرقمية الحساسة وغيرها من الأصول الرقمية، قد يكون من الممكن تبسيط تعريف الأصول الرقمية الحساسة ومن ثم تبسيط تدابير الأمن الحاسوبي ذات الصلة.

18-2- وينبغي توخي الحرص بصفة خاصة في حال استخدام أصول رقمية حساسة قائمة على الخدمات الافتراضية والتعاقدية، مثل خدمات الحوسبة السحابية، لأن هذه الخدمات تتضمن عناصر لا تخضع للتحكم المباشر من قبل الجهة المالكة للبيانات. وعلى سبيل المثال، فالأصول الرقمية الحساسة المؤلفة من تطبيقات أو خدمات قائمة على الحوسبة السحابية تعتمد على برامجيات وأجهزة خاضعة لتحكم الجهة المشغلة للخدمة السحابية ( مثل خدمة التخزين السحابية). وفي تلك الحالات، ينبغي وضع شروط تعاقدية صارمة بشأن المسائل من قبيل التحكم في الوصول والتوافر وفصل البيانات وإتلاف البيانات وواجهة الاتصال والبرامجيات والأجهزة والعمليات الإدارية، وذلك لضمان توفير الحماية الكافية للتطبيقات المعنية في مواجهة الوصول غير المأذون به والتلاعب. ولا يؤدي إسناد توفير الأصول الرقمية الحساسة إلى منظمة أخرى (أي التعاقد مع جهة خارجية) إلى إعفاء الجهة المالكة أو المشغلة للعملية ذات الصلة من المسؤولية عن حماية تلك الأصول الرقمية الحساسة.

19-2- وقد تشمل الأصول الرقمية الحساسة مكونات في نظم تكنولوجيا المعلومات ونظم التكنولوجيا التشغيلية. وسوف تتوقف تدابير الأمن الحاسوبي المناسبة لهذه المكونات على نوع النظام المحتوي عليها ووظيفته. ومع ذلك، فكثيراً ما توجد وصلات تربط بين نظم تكنولوجيا المعلومات ونظم التكنولوجيا التشغيلية، ولذلك ينبغي لتدابير الأمن الحاسوبي المطبقة على فرادى النظم أن تأخذ في الاعتبار أي وصلات بينية من هذا القبيل.

20-2- وبغية توفير توكيد بأن الأصول الرقمية الحساسة تستوفي المتطلبات المتخصصة الموضوعية لها، تُطبَّق عمليات عادة ما يُشار إليها باسم "نماذج دورة الحياة". وتقدم نماذج دورة الحياة وصفاً للأنشطة المنفّذة لاستحداث الأصول الرقمية الحساسة وتشغيلها وصيانتها وسحبها، والعلاقات التي تربط بين هذه الأنشطة. وينبغي أن تؤخذ احتياجات الأمن الحاسوبي في الحسبان في جميع مراحل دورة حياة الأصل الرقمي الحساس. وقد تكون لفرادى المرافق والوظائف والنظم والمكونات والأصول الرقمية الحساسة وغيرها من الأصول الرقمية الحساسة دورات حياة تخصُّ كلاً منها على حدة لكنها تتفاعل بعضها مع بعض. ويمكن استخدام دورة الحياة الافتراضية لتطوير النظم، التي توضع لنظم الأجهزة والتحكم عند إنشائها، كأساس لدورة حياة النظم الحاسوبية، بما فيها الأصول الرقمية الحساسة، على أن يُنظر فيها في سياق الفترة العمرية للمرفق.

## الهجوم السيبراني

21-2- يُقصد بمصطلح "الهجوم السيبراني" أو "الهجمة السيبرانية" عمل شرير يُنفَّذ بنية سرقة بند مستهدف محدد أو تعديله أو منع الوصول إليه أو إتلافه، من خلال الوصول غير المأذون به إلى نظام حاسوبي حساس أو تنفيذ إجراءات داخل هذا النظام. وتستهدف الهجمات السيبرانية سمة واحدة أو أكثر من سمات الأمن الحاسوبي، أي السرية والسلامة والتوافر،<sup>3</sup> فيما يخص معلومات حساسة موجودة في أصل رقمي حساس أو الأصل الرقمي الحساس نفسه، ويمكن استخدامها لتنفيذ أو تيسير ارتكاب عمل شرير ضد أحد المرافق أو الأنشطة أو ارتكاب عمل إجرامي أو عمل آخر متعمد غير مأذون به باستخدام مواد نووية أو مواد مشعة أخرى. وهناك مفهوم آخر وثيق الصلة بمفهوم الهجوم السيبراني، ألا وهو مفهوم "الهجوم غير الموجّه"، والذي ينطوي على إدخال شفرات خبيثة غير موجّهة لهدف بعينه إلى النظم أو الشبكات الحاسوبية دون تعمّد ذلك. ويمكن لهذا النوع من الهجمات أيضاً أن يؤثّر سلباً في الأمن النووي.

22-2- ويمكن تنفيذ الهجوم السيبراني عن طريق الوصول المادي المباشر إلى المعلومات أو أصول المعلومات، أو عن طريق الوصول الإلكتروني، أو باستخدام مزيج من الطريقتين، ويمكن أن ينفَّذ الخصم الهجوم مباشرة أو أن ينفَّذه (أو يساعد الخصم على تنفيذه) طرفاً داخلي، عن علم منه أو دون علم، تحت تأثير الخصم. وينبغي معاملة الهجمات السيبرانية فور الكشف عنها على أنّها أحداث متصلة بالأمن الحاسوبي.

23-2- ويمكن لحادثات الأمن الحاسوبي الناتجة عن هجمات سيبرانية أن تؤدي إلى أحداث أخرى متصلة بالأمن الحاسوبي ثم في نهاية المطاف إلى أحداث متصلة بالأمن النووي، سواء مباشرة أو في سياق سلسلة من الأنشطة الشريرة، بما قد يشمل تنفيذ هجمات سيبرانية أخرى أو الوصول المادي غير المأذون به أو استغلال عناصر داخلية، أو تنفيذ توليفة من الأعمال في إطار هجوم مختلط.

---

<sup>3</sup> من المفترض أنّ هناك سمات أخرى، مثل التحقق من المصادقية وعدم القابلية للتصل، تدخل حمايتها في نطاق حماية السرية والسلامة والتوافر.

## الأمن الحاسوبي في مختلف مجالات الأمن النووي

24-2- تعالج منظومة الأمن النووي المجالات الثلاثة المشمولة بالمراجع [3-5]، ويدعم الأمن الحاسوبي تحقيق مقاصد الأمن النووي في كل مجال من هذه المجالات. ويرد في الأقسام التالية وصف موجز للدور الذي يؤديه الأمن الحاسوبي في كل من هذه المجالات.

### المواد النووية والمرافق النووية

25-2- تعتمد الحماية المادية للمواد النووية والمرافق النووية على التدابير الأمنية لتحقيق ما يلي [3]:

(أ) الحماية من السحب دون إذن؛

العثور على المواد النووية المفقودة واستعادتها؛

الحماية من عمليات التخريب؛

التخفيف من آثار التخريب أو تقليلها إلى أدنى حد.

26-2- وتدعم النظم الحاسوبية في المرافق النووية وظائف متعلقة بالتحكم في العمليات، والأمان النووي، والأمن النووي، وحصر المواد النووية ومراقبتها. وتُستخدم في أداء كل وظيفة من هذه الوظائف أصول رقمية حساسة يمكن أن تُستهدف في سياق هجوم قائم بذاته أو بالاقتران مع هجوم مادي (أي هجوم مختلط). وتحتاج هذه النظم الحاسوبية للحماية من الهجمات السيبرانية عن طريق الأمن الحاسوبي.

### المواد المشعة والمرافق ذات الصلة

27-2- تُستخدم المواد المشعة حول العالم في طائفة متنوعة من الأغراض، بما في ذلك أغراض عديدة لا تنطوي على استخدام مواد نووية. ويتزايد استخدام النظم الحاسوبية في هذه القطاعات لأغراض الأمان والأمن وفي العمليات التشغيلية. ويلزم وضع تدابير أمنية، بما في ذلك تدابير للأمن الحاسوبي، لمنع الوصول غير المأذون به للمواد المشعة أو الاستحواذ عليها لاستخدامها في عمل شرير، وكذلك لمنع تخريب هذه المواد والمرافق المتصلة بها.

28-2- وعادة ما يحتوي السجل الوطني للمصادر المشعة أو للمواد المشعة على معلومات حساسة تتطلب الحماية الأمنية، وينبغي تجسيد ذلك في الإطار التشريعي والرقابي. والأمن الحاسوبي مطلوب في هذا المجال من أجل حماية السرية والسلامة والتوافر فيما يخص المعلومات الحساسة وأصول المعلومات الحساسة، بما فيها الأصول الرقمية الحساسة؛ على سبيل المثال لدعم سرية وسلامة سجلات المصادر وتوافر البيانات اللازمة للتصدي للحادثات.

### المواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي

29-2- المواد الخارجة عن التحكم الرقابي هي مواد نووية أو مواد مشعة أخرى موجودة بكمية تستلزم خضوعها للتحكم الرقابي لكنها ليست قيد التحكم، إما لأن ضوابط التحكم المرتبطة بها قد تعطلت لسبب ما أو لأنها لم تكن خاضعة لأي ضوابط من الأصل. ويتحقق أمن المواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي من خلال تنسيق العمل الذي تضطلع به السلطات المختصة من أجل تنفيذ الوظائف المسندة إليها والمتمثلة في منع وقوع الأحداث المتصلة بالأمن النووي والكشف عنها والتصدي لها إذا وقعت. وهذه الوظائف تؤديها في العديد من الحالات نظم مؤلفة من أصول رقمية حساسة أو مدعومة بأصول رقمية حساسة.

30-2- ويتطلب هذا المجال تطبيق تدابير للأمن الحاسوبي لأغراض منها، على سبيل المثال، توفير الحماية لسرية المعلومات الحساسة، وسلامة نظم الكشف، وسرية نظم نقل البيانات وسلامتها وتوافرها، وتوافر التدابير اللازمة لدعم التصدي، مثل قدرات الاتصالات والتحليل الجنائي النووي.

### التحديات وجوانب الضعف ونظم الأمن الحاسوبي

#### التحديات

31-2- الطرف الذي يشكّل تهديداً للأمن النووي هو طرف لديه الدافع والنية لارتكاب عمل شرير ويتمتع بالقدرة على ذلك، وقد يكون شخصاً واحداً أو مجموعة من الأشخاص. والخصم هو أي فرد ينفذ عملاً شريراً أو يشرع في ذلك.

2-32- ويُعدُّ فهم التهديدات والمخاطر المرتبطة بالتعرُّض لهجوم سيبراني محتمل عنصراً أساسياً في وضع تدابير فعالة للأمن الحاسوبي في سياق الأمن النووي. ويشمل ذلك فهم الأطراف التي تشكّل تهديدات للأمن النووي من حيث دوافعها ونواياها وقدراتها والتكتيكات التي تستعملها في التخطيط لهجوم سيبراني وتنفيذه. - ويقدم المرفق الثاني أمثلة توضح الخصائص العامة لبعض الأطراف التي تشكّل تهديدات للأمن النووي والتي يمكن أن تعتمد إلى تنفيذ هجمات سيبرانية.

### جوانب الضعف

2-33- يُقصد بجوانب الضعف في نظام حاسوبي أو شبكة حاسوبية الخصائص التشغيلية التي تجعل النظام عرضة للاستغلال أو لتهديد معين. ويمكن لهذه الخصائص أن تكون ذات طبيعة إدارية أو مادية أو تقنية. وقد يستغل الخصم جوانب الضعف بما يمكنه من الوصول غير المأذون به لأصل رقمي حساس أو التحكم في ذلك الأصل. وقد تتفاوت العواقب المرتبطة باستغلال أحد جوانب الضعف في أصل رقمي حساس من الضالة إلى الجسامة رهناً بما ينطوي عليه ذلك الاستغلال من إمكانية التأثير سلباً في تشغيل الأصل الرقمي الحساس وأدائه لوظيفته.

2-34- وما فتئ مستوى التعقيد الذي تتسم به النظم الحاسوبية يتزايد باستمرار، سواءً من حيث الأجهزة أو البرمجيات، وكذلك عدد النظم الحاسوبية المستعملة والترابط فيما بينها. ويزيد هذا التعقيد من صعوبة تكوين فهم كامل للنظم، ومن ثم المحافظة على الخبرات اللازمة لإدارة شؤون الأمن. ومن الممكن أن يكون عدد جوانب الضعف في النظام مرتبطاً بمستوى التعقيد الذي يتسم به، ولذلك ينبغي ألا تبلغ النظم من التعقيد إلا القدر اللازم لأداء الوظائف المتوخاة منها.

2-35- وتستند الهجمات السيبرانية الناجمة في العديد من الحالات إلى استغلال جوانب ضعفاً مكتشفة حديثاً. وعلى سبيل المثال، فهناك حالات تقع فيها "هجمات فورية" يستغل فيها الخصم نقطة ضعف لم تكن معروفة للجهة المدافعة قبل الهجوم. وبالإضافة إلى ذلك، فالتطور السريع الذي تشهده التكنولوجيات الحاسوبية الجديدة يفسح المجال لتغيّر طبيعة جوانب الضعف، حيث تظل فئات بأسرها من جوانب الضعف الجديدة غير ظاهرة حتى اعتماد هذه التكنولوجيات الجديدة وبدء تشغيلها.

36-2- وبالنظر إلى مستوى التعقيد الذي تتسم به بعض النظم الحاسوبية وإمكانية وجود جوانب ضعف خفية فيها، فقد لا تكون تدابير الأمن الحاسوبي المتاحة كافية لخفض المخاطر وصولاً إلى مستوى مقبول يسمح باستخدام هذه النظم في تطبيقات محددة في مجالي الأمن والأمان النوويين. وفي الحالات التي لا تكون فيها التدابير قادرة على خفض المخاطر إلى مستوى مقبول، ينبغي النظر في اتباع نهج بديلة (مثل الأخذ بتصميم مختلف أو تغيير توزيع الوظائف).

### اتباع نهج متدرج والأخذ بمبدأ الدفاع في العمق في مجال الأمن الحاسوبي

37-2- يمكن أن تكون تدابير الأمن الحاسوبي ذات طبيعة تقنية أو مادية أو إدارية، أو أن تجمع بين توليفة من هذه العناصر. وينبغي اختيار توليفة تدابير المراقبة باتباع نهج متدرج يقوم على العلم بالمخاطر وعلى مبدأ الدفاع في العمق لتحقيق مستوى ملائم من الأمن الحاسوبي. ويمكن اختيار مجموعة تدابير الأمن الحاسوبي المحددة التي يجري تنفيذها على أساس مزيج من التدابير المنصوص عليها في الإرشادات العامة أو في المتطلبات التي وضعتها الدولة والتدابير التي تحددها الجهة المشغلة من خلال عملية خاصة بها قائمة على العلم بالمخاطر.

38-2- ومستويات الأمن الحاسوبي هي وسيلة لتحديد المتطلبات الأمنية المناسبة من حيث النطاق ودرجة الصرامة على النحو اللازم لتوفير الحماية لمختلف الأصول الرقمية الحساسة. ومن ثم فإن كل مستوى من المستويات الأمنية المتدرجة سيتطلب تنفيذ مجموعة مختلفة من تدابير الحماية لاستيفاء المتطلبات الأمنية لذلك المستوى. وتُطبق متطلبات أكثر صرامة فيما يخص الأصول الرقمية الأكثر حساسية. ويوضح الشكل 3 هذا المبدأ.

39-2- ومن الأساليب العملية لتطبيق النهج المتدرج لجميع النظم الحاسوبية والأصول الرقمية الحساسة المرتبطة بها ضمن نطاقات أمنية حاسوبية، بحيث تُطبق تدابير الأمن الحاسوبي بطريقة متدرجة على كل نطاق بحسب متطلبات الحماية المناسبة له (أي المستوى الأمني المنطبق عليه). وبعد ذلك تحدّد مستويات الأمن الحاسوبي الملائمة لكل نطاق بناءً على الأثر المحتمل للهجمات السيبرانية في الوظائف والنظم والأصول الرقمية الحساسة المشمولة بذلك النطاق.



الشكل-3- توضيح اتباع نهج متدرج باستخدام مفهوم مستويات الأمن الحاسوبي.

2-40- واستخدام مستويات الأمن الحاسوبي، على النحو المبيّن في الشكل 3، هو نهج متدرج ينطوي على تحديد متطلبات الأمن الحاسوبي بما يتناسب مع العواقب التي يُحتمل أن تترتب على هجوم سيبراني ناجح. ويمكن الاسترشاد بالاعتبارات التالية في تطبيق هذه الطريقة:

- (أ) يُطبّق مستوى أعلى من متطلبات الحماية فيما يخص الأصول الرقمية الحساسة التي يمكن أن يؤدي الإخلال بها إلى أضرار العواقب، بما في ذلك الأحداث الكبرى المتصلة بالأمن النووي.
- (ب) يُطبّق مستوى أدنى من متطلبات الحماية فيما يخص النظم الحاسوبية التي تؤدي وظائف متصلة بالأمن النووي ولكنها لا تُعتبر أصولاً رقمية حساسة.
- (ج) تُطبّق متطلبات عامة على جميع المستويات الأمنية والنظم الحاسوبية التي تؤدي وظائف متصلة بالأمن النووي، ويمكن معالجة هذه المتطلبات باستخدام نفس تدابير الأمن الحاسوبي المعمول بها فيما يخص النظم الحاسوبية المستعملة في المجالات الأخرى.

2-41- ومن الضروري أيضاً تطبيق تدابير للأمن الحاسوبي فيما يخص النظم الحاسوبية التي لا تُعتبر أصولاً رقمية حساسة. وبالنظر إلى الترابط فيما بين الشبكات الحاسوبية وتدفق المعلومات بين الحواسيب، فإن توفير الدفاع في العمق ضد الهجمات السيبرانية يستوجب اتباع نهج متعدد الطبقات يقوم على متطلبات متدرجة للأمن الحاسوبي فيما يخص جميع النظم الحاسوبية. وفي المثال المذكور أعلاه، من المرجح أن النظم

الحاسوبية في النطاقات المحدد لها متطلبات أمنية من المستوى 4 والمستوى 5 لن تُصنّف على أنّها أصول رقمية حساسة، بيد أنّ هذه النطاقات تخضع لتدابير حماية حتى يمكن توفير عدة طبقات من الدفاع في العمق في مواجهة التسلل إلى الأصول الرقمية الحساسة في النطاقات ذات المستويات الأعلى والإخلال بها.

42-2- وينطوي الدفاع في العمق لأغراض الأمن الحاسوبي على وضع طبقات دفاعية متعددة من تدابير الأمن الحاسوبي التي يلزم أن تتعطل أو يتم تجاوزها حتي يمكن لأي هجوم سيبراني أن يمضي قدماً ليوثر سلباً في أصل رقمي حساس. ويكون توفير الدفاع في العمق عن طريق تطبيق توليفة مناسبة من تدابير الأمن الحاسوبي المتقاطعة التي يكمل بعضها بعضاً. ولا يتحقق الدفاع في العمق فقط من خلال تعدّد الطبقات الدفاعية، وإنما يتطلب أيضاً تنفيذ تدابير الأمن الحاسوبي الكفيلة بمنع تعرّض الأصول الرقمية الحساسة للهجوم، وبالكشف عن الهجمات إذا وقعت والحماية منها والتصدي لها والتخفيف من آثارها وتيسير التعافي منها. وعلى سبيل المثال، ففي حال تعطل وظيفة المنع (مثلاً فيما يخص مخالفة السياسة التي تحظر استخدام وسائط تخزين نقالة) أو تجاوز آليات الحماية (مثلاً عن طريق فيروس جديد لا تتعرف عليه تلك الآليات باعتباره هجوماً سيبرانياً)، ستظلّ هناك آليات قائمة للكشف عن أي تغيير غير مأذون به في الأصل الرقمي الحساس والتصدي له.

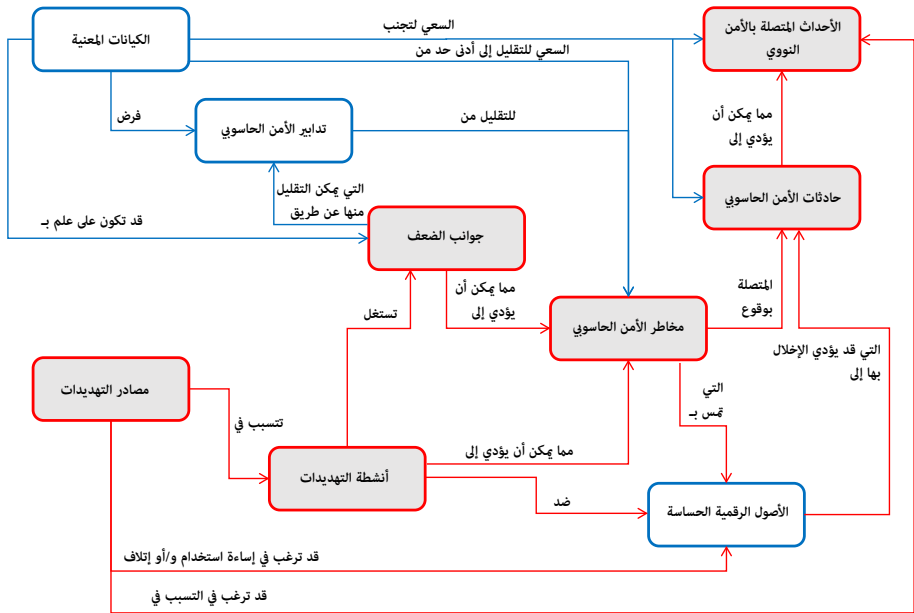
43-2- وحتى يكون الدفاع في العمق فعالاً، ينبغي أيضاً أن يكون مصمماً بحيث لا يؤدي أي عطل واحد يصيب أحد تدابير الأمن الحاسوبي المتعددة الطبقات إلى إبطال أو تعطيل أكثر من طبقة واحدة. وعلى سبيل المثال، يمكن أن يؤدي استغلال نقطة ضعف حرجة في جهاز حماية مستعمل في عدة مواضع إلى تجاوز طبقات دفاعية متعددة ما لم يكن نهج الدفاع في العمق يكفل التنوع في الأجهزة أو في إعدادات التهيئة أو يوفر تدابير أخرى. وينبغي إدارة التنوع في تدابير الأمن الحاسوبي بطريقة تقيم توازناً بين الدفاع في العمق من ناحية ومستوى التعقيد الذي يتسم به النظام من ناحية أخرى.

44-2- وقد يعتمد الدفاع في العمق على تصميم للنظم يتألف من نطاقات تُحدّد لها مستويات مختلفة للأمن الحاسوبي. وعادة ما يُوضّح هذا التصميم برسم بياني في شكل حلقات متحدة المركز. ومن المبادئ الأساسية في هذا التصميم ألا توجد وصلات مباشرة إلا فيما بين نطاقات الأمن الحاسوبي المتجاورة.

2-45- ويمكن المساهمة أيضاً في تحقيق فعالية الدفاع في العمق عن طريق التأكد من أنَّ مختلف أجزاء المنظمة المشغلة تضطلع بأدوار ومسؤوليات يكمل بعضها بعضاً في مجال الأمن الحاسوبي، مع مراعاة الفصل الفعال بين المهام، بحيث يمكن إذا ارتكب أحد الأشخاص أية أخطاء أن يلاحظها شخص آخر ويصححها.

2-46- ويستند تحديد التدابير الأمنية المناسبة بناء على العلم بالمخاطر إلى الوقوف على التهديدات وجوانب الضعف وتقييم المخاطر المرتبطة بها. وفي هذا السياق، يُقصد بالمخاطر إمكانية أن يؤدي استغلال جوانب الضعف من قبل الأطراف التي تشكّل تهديدات للأمن النووي إلى التأثير سلباً في الأصول الرقمية الحساسة ومن ثم في الأمن والأمان النوويين، وبذلك يكون مستوى المخاطر متوقفاً على احتمالية وقوع هجوم ومستوى شدة عواقب ذلك الهجوم. ويمكن توضيح العلاقة بين هذه المفاهيم في سياق الأمن الحاسوبي على النحو التالي، كما هو مبين في الشكل-4:

- (أ) تسعى الجهات المالكة للنظم الحاسوبية في منظومة الأمن النووي إلى تجنب وقوع أحداث متصلة بالأمن النووي، ومن ثم تسعى إلى التقليل إلى أدنى حد من مخاطر أحداث الأمن الحاسوبي التي يمكن أن تسهم في وقوع أحداث متصلة بالأمن النووي.
- (ب) قد ترغب الأطراف التي تشكّل تهديدات للأمن النووي في التسبب في أحداث متصلة بالأمن النووي، وقد تستهدف الأصول الرقمية الحساسة للإخلال بها و/أو تخريبها.
- (ج) بناء على ذلك، يمكن للأطراف التي تشكّل تهديدات للأمن النووي أن تشرع في نشاط يستغل جوانب الضعف، مما يشكّل مخاطر متصلة بالأمن الحاسوبي على الأصول الرقمية الحساسة، ويمكن أن تؤدي هذه المخاطر إلى أحداث متصلة بالأمن النووي.
- (د) تطبّق الجهات المالكة تدابير للأمن الحاسوبي بهدف التقليل من المخاطر المتصلة بالأمن الحاسوبي على الأصول الرقمية الحساسة.
- (هـ) يمكن للنهج القائم على العلم بالمخاطر أن يشمل النظر في احتمالية وقوع أحداث معينة متصلة بالأمن الحاسوبي عند تحديد تدابير الأمن الحاسوبي المناسبة. ويمكن التقليل من المخاطر عن طريق القضاء على مصدر التهديد، أو تطبيق تدابير للأمن الحاسوبي تقلل من احتمالية وقوع هجوم يؤدي إلى وقوع حادثة متصلة بالأمن الحاسوبي، أو الحد أو التخفيف من شدة الأثر المترتب على حادثة الأمن الحاسوبي.
- (و) ينبغي أن تكون عمليات تحديد المخاطر وإدارتها عمليات مستمرة تواكب التغيرات التي تطرأ على عوامل الخطر.



الشكل 4- اتباع نهج قائم على العلم بالمخاطر إزاء تدابير الأمن الحاسوبي (منقولاً بتصرف من المعيار ISO/IEC 8102:50072) [9].

## المسؤوليات المتعلقة بالأمن الحاسوبي في إطار منظومة الأمن النووي

47-2- تضم منظومة الأمن النووي العديد من المنظمات التي تستخدم النظم الحاسوبية لأداء وظائف في مجالات مثل معالجة المعلومات، والأمن النووي، والأمان النووي، وحصر المواد النووية ومراقبتها.

48-2- وتحمل كل منظمة من هذا المنظمات المسؤولية عن حماية المعلومات السرية التي تحتوي عليها هذه النظم والأصول الرقمية الحساسة المرتبطة بها.

49-2- ويقدم الشكل 5 رسماً بيانياً لما تضمه منظومة الأمن النووي من المنظمات التي يمكن أن تتحمل مسؤوليات متعلقة بالأمن الحاسوبي. وتشمل هذه المنظمات السلطات

المختصة<sup>4</sup> والجهات المشغلة،<sup>5</sup> والتي تتحمل مسؤولياتها المتعلقة بالأمن الحاسوبي في إطار منظومة الأمن النووي بناءً على التوزيع الذي تحدده المتطلبات القانونية والرقابية الوطنية.

50-2- ويمكن أن تكون لدى الدولة سلطة مختصة (أو سلطات مختصة) مكلفة بشؤون الأمن الحاسوبي، وقد تكون هذه السلطة جهة مختلفة عن السلطات المختصة المسؤولة عن الأمن النووي. وبالإضافة إلى ذلك، فقد تكون السلطات المختصة خاضعة لمتطلبات ومعايير قانونية وطنية متعلقة بالأمن الحاسوبي خارج نطاق منظومة الأمن النووي.

51-2- ويشمل تعبير "البائعين والمتعاقدين والموردين" المنظمات التي توفر السلع والخدمات إلى السلطات المختصة والجهات المشغلة لكن مسؤولياتها المتصلة بالأمن الحاسوبي (مثل حماية المعلومات الحساسة والأصول الرقمية الحساسة ذات الصلة) لا تستند إلى المتطلبات القانونية والرقابية الوطنية، وإنما إلى الشروط المنصوص عليها في العقود المبرمة مع السلطات المختصة والجهات المشغلة.

52-2- ويوضح القسمان 3 و4 أدناه بمزيد من التفصيل الأدوار والمسؤوليات المتعلقة بالأمن الحاسوبي والمنوطة بالدولة والسلطات المختصة والجهات المشغلة، وبالبائعين والمتعاقدين والموردين.

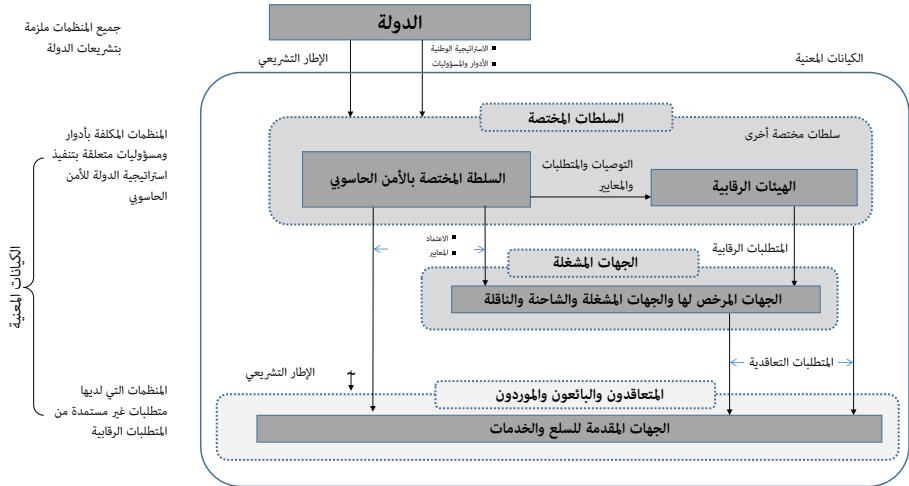
## الكفاءات والقدرات في مجال الأمن الحاسوبي

53-2- وحتى يكون الأمن الحاسوبي فعالاً ومُحكماً، ينبغي أن يقوم على تنفيذه وتعهده والمحافظة على استدامته موظفون يتمتعون بالكفاءة والجدارة بالثقة، في ظل إدارة فعالة وقيادة نشطة ومطلعة. وينبغي أن تعمل كل منظمة في منظومة الأمن النووي، وفقاً للأدوار والمسؤوليات المحددة المنوطة بها، على إرساء الكفاءات والقدرات في مجال الأمن الحاسوبي والمحافظة على استدامتها.

---

<sup>4</sup> تشمل السلطات المختصة أيضاً أجهزة الشرطة والإنقاذ وحرس الحدود وقوات الدفاع التي تؤدي دوراً في تأمين المرافق والأنشطة وفي الكشف عن الحوادث المنطوية على مواد نووية ومواد مشعة أخرى والتصدي لها.

<sup>5</sup> تشير عبارة "الجهات المشغلة" في هذا المنشور إلى الكيانات المرخص لها في منظومة الأمن النووي، بما في ذلك الجهات المشغلة للمرافق والأنشطة المنطوية على مواد نووية ومواد مشعة أخرى، والجهات الشاحنة والناقلة.



الشكل 5- المنظمات التي تتحمل مسؤوليات متعلقة بالأمن الحاسوبي في إطار منظومة الأمن النووي.

### 3- الأدوار والمسؤوليات المنوطة بالدولة

1-3- ينبغي أن تضع الدولة وتتعهد استراتيجية وطنية للأمن الحاسوبي في إطار منظومة الأمن النووي الخاصة بها (ويُشار إليها في بقية هذا المنشور باسم "الاستراتيجية"). وينبغي أن تعيّن الدولة سلطة مختصة تتحمل المسؤولية الرئيسية عن وضع الاستراتيجية.

#### الاعتبارات التشريعية والرقابية

2-3- ينبغي أن تكفل الدولة معالجة الأمن الحاسوبي على النحو المناسب في الإطار التشريعي والرقابي المنطبق على منظومة الأمن النووي وبما يتسق مع مقتضيات تلك المنظومة. وينبغي أن تنص الدولة في قانونها الوطني على متطلبات مناسبة للأمن الحاسوبي، بما يضمن التنفيذ السليم للأمن الحاسوبي في إطار الأمن النووي.

3-3- وينبغي أن تكفل الدولة أن تجرّم تشريعاتها الهجمات السيبرانية على النظم الحاسوبية المستعملة في منظومة الأمن النووي. وقد يتطلب الأمن الحاسوبي النص على أحكام تشريعية خاصة لمراعاة الخصائص الفريدة التي تتسم بها بعض الجرائم وطرائق

التنفيذ المرتبطة بالهجمات السيبرانية.

4-3- وينبغي أن تكفل الدولة أن ينصّ إطارها التشريعي أو الرقابي على فرض عقوبات على ارتكاب أعمال إجرامية أو أعمال متعمدة غير مأذون بها ضد الأصول الرقمية الحساسة بما من شأنه تعريض الأمن النووي للخطر.

5-3- وينبغي أن تنظر الدولة في أمثلة من القوانين الأخرى ومن الصكوك القانونية الدولية (مثل الاتفاقيات) لمساعدتها على تعريف الأمن الحاسوبي وتنفيذه فيما يتعلق بالأمن النووي. وقد يشمل ذلك ما يلي:

- (أ) القوانين المتعلقة بالجرائم الحاسوبية؛
- (ب) القوانين المتعلقة بالإرهاب؛
- (ج) القوانين المتعلقة بحماية البنى الأساسية الوطنية الحرجة؛
- (د) القوانين التي تُلزم بالإفصاح عن المعلومات؛
- (هـ) القوانين المتعلقة بالخصوصية وبالتعامل مع المعلومات الشخصية؛
- (و) الصكوك الدولية المتعلقة بالجريمة السيبرانية، مثل الاتفاقيات.

6-3- وينبغي أن تستعرض الدولة إطارها التشريعي والرقابي وتحديثه باستمرار لتضمينه أحكاماً تتناول التهديدات السيبرانية وجوانب الضعف الجديدة والناشئة.

7-3- وينبغي أن تعيّن الدولة سلطة مختصة رئيسية معنية بالأمن الحاسوبي،<sup>6</sup> لتتولى المسؤولية عن الإشراف على تطبيق القوانين واللوائح المتعلقة بالأمن الحاسوبي وإنفاذها فيما يتعلق بمنظومة الأمن النووي (ويُشار إلى هذه السلطة فيما يلي باسم "السلطة المختصة بالأمن الحاسوبي").

8-3- وقد تختار الدولة تنفيذ إطار تشريعي ورقابي للأمن الحاسوبي لا يقتصر على منظومة الأمن النووي، وقد يكون لبعض القوانين واللوائح نطاق تطبيق أوسع من

---

<sup>6</sup> يمكن للدولة أن تسند هذه المسؤولية إلى عدة سلطات مختصة تختلف طبيعة عملها باختلاف السياق؛ فعلى سبيل المثال، يمكن أن تكون السلطة المختصة المسؤولة عن الأمن الحاسوبي في المرافق النووية غير السلطة المختصة المسؤولة عن الأمن الحاسوبي في أماكن الممارسة الطبية أو في رصد الحدود. وتُستخدم عبارة "السلطة المختصة" في هذا المنشور للإشارة إلى السلطة التي تتحمل المسؤولية في سياق معين.

منظومة الأمن النووي. وفي مثل تلك الحالات، ينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من أنَّ الإطار المعمول به كافٍ لأغراض الأمن النووي، فإن لم يكن كافياً، ينبغي أن تكمل الدولة ذلك الإطار بالنص على أي متطلبات لازمة بطريقة تتناسب مع مقتضيات منظومة الأمن النووي.

3-9- وينبغي أن تكفل الدولة توافر الموارد المالية والبشرية والتقنية الكافية للسلطات المختصة على النحو الذي يمكّنها من الوفاء بمسؤولياتها المتعلقة بتفسير التزاماتها القانونية وتنفيذها بطريقة سليمة فيما يتصل بالأمن الحاسوبي في إطار منظومة الأمن النووي الخاصة بالدولة.

### السلطة المختصة بالأمن الحاسوبي في إطار منظومة الأمن النووي

3-10- بحسب التنظيم الهيكلي المعمول به في الدولة، قد تكون السلطة المختصة بالأمن الحاسوبي في إطار منظومة الأمن النووي هي الهيئة الرقابية المعنية بالأمن النووي، وقد تكون جهة أخرى. وبالمثل، فقد تكون المسؤوليات المتعلقة بالأمن الحاسوبي داخل الدولة موزعة على عدة منظمات، بيد أنَّه ينبغي أن تعيّن الدولة سلطة مختصة واحدة محددة تتحمل المسؤولية عن الأمن الحاسوبي في كل مجال محدد من مجالات منظومة الأمن النووي. وعلى سبيل المثال، فقد تكون السلطة المختصة بالأمن الحاسوبي في محطات القوى النووية غير السلطة المختصة بالأمن الحاسوبي في عمليات رصد الحدود.

3-11- وفي الحالات التي توجد فيها أكثر من سلطة واحدة مختصة بالأمن الحاسوبي في إطار منظومة الأمن النووي، أو تكون فيها السلطة المختصة بالأمن الحاسوبي غير السلطة المختصة بالأمن النووي، ينبغي أن تنشئ الدولة وتتعهد هيئة أو آلية مناسبة للتنسيق لضمان الوضوح في تحديد توزيع المسؤولية والمساءلة عن كل جانب من جوانب الأمن الحاسوبي على جميع السلطات المختصة المعنية.

3-12- وينبغي أن تحدد الدولة جميع السلطات المختصة<sup>7</sup> والجهات المشغلة التي تؤدي أدواراً وتتحمّل مسؤوليات فيما يتعلق بالأمن الحاسوبي في إطار منظومة الأمن النووي،

---

<sup>7</sup> تشمل السلطات المختصة التي ينبغي أن تؤخذ في الحسبان، حسب الاقتضاء، أي هيئة أو آلية للتنسيق، وأجهزة إنفاذ القانون والجمارك ومراقبة الحدود، ووكالات الاستخبارات والأجهزة الأمنية، والوكالات المعنية بالصحة والبيئة.

وأن تتأكد من أن كل جهة من هذه الجهات تخضع لإشراف السلطة المناسبة المختصة بالأمن الحاسوبي في إطار منظومة الأمن النووي.

13-3- وينبغي أن تُلزم الدولة السلطات المختصة والجهات المشغلة التي تحددها وفقاً للفقرة السابقة بوضع وتنفيذ برامج للأمن الحاسوبي وفقاً للاستراتيجية.

14-3- وينبغي أن تعرّف الدولة المسؤوليات المتعلقة بالأمن الحاسوبي وتسندّها إلى جميع الكيانات المعنية في منظومة الأمن النووي.

15-3- ويقدم المرفق الثالث قائمة بأمثلة للمسؤوليات المتعلقة بالأمن النووي التي يمكن استخلاص التكاليفات المتعلقة بالأمن النووي منها، بحسب طبيعة منظومة الأمن النووي الخاصة بالدولة وما تحتوي عليه من الأصول الرقمية الحساسة.

16-3- وقد توجد بعض المنظمات الداعمة التي لا تخضع لسلطة الهيئات الرقابية التابعة للدولة، ولكنها تؤدي دوراً محورياً في تحقيق مقاصد الأمن النووي فيما يتعلق بالأمن الحاسوبي. ويمكن تعريف مسؤوليات هذه المنظمات ومتطلبات الأمن الحاسوبي المنطبقة عليها من خلال اتفاقات تعاقدية مثل الاتفاقات التي تُبرم مع البائعين والمتعاقدين والموردين. ويمكن للدولة أن تفرض متطلبات للأمن الحاسوبي (على سبيل المثال فيما يتعلق بالتصميم والأداء وتدريب الموظفين) فيما يخص نظاماً حاسوبية معينة، وعلى البائعين والمتعاقدين والموردين في منظومة الأمن النووي، وفقاً للاستراتيجية.

## أوجه الترابط مع المجالات الأخرى

17-3- ينبغي أن تتأكد الدولة من فعالية قنوات الترابط بين الأمن الحاسوبي وسائر المجالات. وقد يتطلب ذلك من الدولة أن تتخذ إجراءات تتجاوز نطاق الأمن الحاسوبي (مثل فرض متطلبات على المجالات الأخرى).

18-3- وينبغي أن تكفل الدولة أن تعرّف الاستراتيجية أوجه الترابط بين الأمن الحاسوبي وسائر المجالات ذات الصلة حتى يتسنى للسلطات المختصة والجهات المشغلة المعنية أن تفهم أدوارها ومسؤولياتها في هذا الصدد.

## الأمان النووي

19-3- للأمن النووي والأمان النووي هدفٌ مشترك، ألا وهو حماية الأشخاص والممتلكات والمجتمع والبيئة. وينبغي تصميم وتنفيذ التدابير في مجالي الأمن والأمان بطريقة متكاملة تكفل التآزر بين هذين المجالين، وبحيث لا تُخلُّ تدابير الأمن بالأمان ولا تُخلُّ تدابير الأمان بالأمن [1].

20-3- ويؤدي الأمن الحاسوبي دوراً مهماً في مسألة الترابط بين الأمن النووي والأمان النووي، لا سيما بالنظر إلى تزايد الاعتماد على النظم الحاسوبية في جميع الجوانب التشغيلية بالمرافق النووية.

21-3- وينبغي أن تنظر الدولة في اللوائح المتعلقة بالأمن النووي والأمان النووي عند إعداد لوائح الأمن الحاسوبي، وأن تتأكد من الاتساق في تنفيذ هذه اللوائح.

22-3- وفيما يخص أي وظيفة من وظائف الأمان التي تعتمد على نظام حاسوبي أو يدعمها نظام حاسوبي، فإنَّ تأدية تلك الوظيفة على النحو المطلوب ستتوقف على سلامة المعلومات ذات الصلة (بما فيها البرامجيات) وتوافرها - وسريتها، عند الاقتضاء. ولذلك ينبغي تنفيذ الأمن الحاسوبي باعتباره جزءاً لا يتجزأ من عمليات دورة حياة النظم الحاسوبية المستخدمة لأغراض الأمان النووي، للتأكد من أخذ متطلبات الأمن الحاسوبي ومتطلبات الأمان النووي في الحسبان معاً.

23-3- وينبغي إقامة علاقة متسقة ومنطقية فيما بين فئات الأمان ومستويات الأمن الحاسوبي المحددة للأصول الرقمية، بما يكفل توفير مستوى مناسب من الأمن الحاسوبي للأصول الرقمية المندرجة ضمن فئة أمان معينة، إلا أنَّ ذلك لا يعني أن هذه العلاقة قائمة بالضرورة على التطابق البسيط. وبالإضافة إلى ذلك، فهناك بعض الأصول الرقمية الحساسة غير المصنفة رسمياً في فئة أمان معينة، بيد أنَّها قد تكون مهمة للأمان من المنظور الأمني، ومن ثم تُعتبر من الأصول الرقمية الحساسة. ويتوقف تحديد مستوى الأمن الحاسوبي المناسب على وظيفة النظام والأصل الرقمي الحساس المحدد في سياق النظام والمنظمة ككل. وبناء على تحديد مستوى الأمن الحاسوبي، يلزم تحديد الكفاءات والقدرات المناسبة وفقاً للتقدير القائم على مبادئ متفق عليها.

3-24- وينبغي ألا يؤدي تنفيذ تدابير الأمن الحاسوبي إلى التأثير سلباً في وظائف الأمان النووي من حيث أدائها أو فعاليتها أو موثوقيتها أو سير عملها.

3-25- ويرد في المرفق وصف لمزيد من الاعتبارات التي يتعين على الدولة أن تأخذها في الحسبان عند معالجة أوجه الترابط مع الأمان النووي.

### الحماية المادية

3-26- تعتمد نظم الحماية المادية في كثير من الأحيان على نظم حاسوبية، ومن الأمثلة على ذلك النظم التي تؤدي وظائف التحكم في الوصول المادي، والرصد والكشف الأمني، والإنذار والتصدي. وفي حالة الإخلال بهذه النظم بفعل عمل شرير (مثل الإخلال بسرية المعلومات الموجودة في هذه النظم و/أو سلامة تلك المعلومات و/أو توافرها)، فإن ذلك يمكن أن يؤدي إلى الإضرار بسير عمل نظام الحماية المادية ويمكن أن ييسر تنفيذ أعمال مادية تستهدف سحب المواد دون إذن أو التخريب. وينبغي تنفيذ الأمن الحاسوبي باعتباره جزءاً لا يتجزأ من عمليات دورة حياة النظم الحاسوبية المستخدمة لأغراض وظائف الحماية المادية أو نظمها.

3-27- وقد تقدم نظم الحماية المادية بدورها مساهمة قيمة في الأمن الحاسوبي، كما في حالة نظم التحكم في الوصول المادي، وينبغي أن يُنظر في استخدامها لحماية النظم الحاسوبية.

3-28- وقد تُعامل بعض الدول مجال الأمن الحاسوبي باعتباره جزءاً من الحماية المادية، وفقاً للتعريف الوارد في المرجع [3]. بيد أن هذا المنشور يتناول الأمن الحاسوبي على أنه موضوع منفصل يختلف عن موضع الحماية المادية، لتوضيح الاختلافات بينهما وإبرازها. وتتوقف طبيعة الترابط بين الأمن الحاسوبي والحماية المادية على الظروف القائمة في كل دولة.

3-29- وينبغي ألا يؤدي تنفيذ تدابير الأمن الحاسوبي إلى التأثير سلباً في وظائف نظام الحماية المادية من حيث أدائها أو فعاليتها أو موثوقيتها أو سير عملها.

## وظائف تكنولوجيا المعلومات والتكنولوجيا التشغيلية

30-3- في كثير من الأحيان، تكون المسؤوليات المتعلقة بإدارة أمن نظم تكنولوجيا المعلومات والتكنولوجيات التشغيلية (بما فيها التكنولوجيات المستخدمة في التحكم الصناعي وفي نظم الأجهزة والتحكم) مسندة إلى إدارات مختلفة داخل المنظمة. ويعد الترابط والتنسيق بين هذه الفرق عاملاً أساسياً في توفير الأمن الشامل. وتشير التجارب السابقة إلى أنَّ نظم تكنولوجيا المعلومات قد استُخدمت في الهجمات السيبرانية كمورد للاستطلاع وكذلك كوسيلة للهجوم على التكنولوجيات التشغيلية.

31-3- وقد توجد اختلافات بين الجهات المسؤولة عن نظم تكنولوجيا المعلومات والجهات المسؤولة عن التكنولوجيات التشغيلية من حيث الإجراءات والمصطلحات وتقييم المخاطر. ويُعدُّ التنسيق الفعال بين هذين الجانبين عاملاً أساسياً في تلافي حالات سوء الفهم وعدم الاتساق في تطبيق تدابير الأمن الحاسوبي.

## وكالات الاستخبارات

32-3- ينبغي أن تكفل الدولة اضطلاع وكالات الاستخبارات بتوفير مستوى مناسب من الدعم للمساهمة في إجراء التقييم الوطني للتهديدات أو المحافظة على دقته ومواكبته للمستجدات، بما يشمل التهديدات المتعلقة بالهجمات السيبرانية ضد منظومة الأمن النووي. وينبغي وضع بروتوكولات وعمليات لدعم نقل المعلومات بشأن التهديدات السيبرانية إلى الكيانات المعنية في منظومة الأمن النووي حسب الاقتضاء، بما يكفل توفير مستوى ملائم من الأمن الحاسوبي في مواجهة التهديدات المتغيرة.

33-3- وينبغي أن تتأكد الدولة من إلمام وكالات الاستخبارات بدور الأمن الحاسوبي في منظومة الأمن النووي، بما في ذلك الإلمام بأنواع الأصول الرقمية الحساسة الموجودة وأهميتها.

## الجهات المسؤولة عن التصدي

34-3- ينبغي أن تتأكد الدولة من أنَّ جميع السلطات المختصة والجهات المشغلة لديها نظم وتدابير للأمن النووي على النحو اللازم لاكتشاف وتقييم أحداثات الأمن الحاسوبي التي لها آثار فعلية أو محتملة في الأمن النووي، ومن إبلاغ السلطات المختصة المعنية

بهذه الحادثات حتى يمكن البدء في اتخاذ إجراءات التصدي المناسبة.

35-3- وينبغي أن تتضمن خطط الطوارئ بنوداً بشأن التصدي للهجمات السيبرانية والهجمات المختلطة.

### المساعدة والتعاون على الصعيد الدولي (بما في ذلك تبادل المعلومات)

36-3- تُشجّع الدول على التعاون فيما بينها ومع المنظمات الدولية، حسب الاقتضاء، من أجل تأمين الأصول الرقمية الحساسة والمعلومات الحساسة المرتبطة بها، ومن أجل الوقوف على تهديدات الهجمات السيبرانية، لا سيما أي تهديدات ذات مصداقية تنطوي على تخريب مواد نووية أو أحد المرافق النووية. (على سبيل المثال بمقتضى المادة 5 (3) من اتفاقية الحماية المادية للمواد النووية بصيغتها المعدلة [2]). ويمكن بناء الثقة وتحسين الأمن الحاسوبي عن طريق تقاسم وتحليل المعلومات المتعلقة بجوانب الضعف والتهديدات وحادثات الأمن الحاسوبي في الوقت المناسب، مع توفير الحماية المناسبة لسرية هذه المعلومات.

37-3- وينبغي أن تنشئ الدولة آليات آمنة وخاضعة للمراقبة من أجل تقاسم المعلومات بهدف تنسيق التصدي للهجمات السيبرانية على منظومة الأمن النووي الخاصة بالدولة. وتُشجّع الدولة على الانخراط في التعاون والمساعدة على الصعيد الدولي لدعم التحقيق في الهجمات السيبرانية والملاحقة القضائية لمرتكبيها.

38-3- وتُشجّع الدولة على الاستعانة دورياً بالخدمات الاستشارية أو خدمات التقييم للنظر في استراتيجيتها وبرامج الأمن الحاسوبي المعمول بها لديها وتنفيذها في منظومة الأمن النووي الخاصة بالدولة.

## 4- الأدوار والمسؤوليات المنوطة بالسلطات المختصة والجهات المشغلة

4-1- الأمن الحاسوبي هو موضوع مشترك بين عدة مجالات في عمل السلطات المختصة والجهات المشغلة المشمولة بمنظومة الأمن النووي. وتتحمل جميع هذه المنظمات قدراً ما من المسؤولية عن حماية الأصول الرقمية الحساسة.

4-2- والسلطات المختصة والجهات المشغلة هي أطراف منتجة ومستخدمة للمعلومات الحساسة في نفس الوقت، وكثيراً ما تخضع لسيطرتها الأصول الرقمية الحساسة المستخدمة في معالجة هذه المعلومات أو تخزينها، أو التي تشكّل تلك المعلومات جزءاً أساسياً منها. وينبغي أن تنفذ السلطات المختصة والجهات المشغلة تدابير للأمن الحاسوبي من أجل حماية هذه الأصول الرقمية الحساسة والمعلومات الحساسة المرتبطة بها.

4-3- وينبغي أن تضع السلطات المختصة والجهات المشغلة قائمة بالأصول الرقمية الحساسة الموجودة لديها، وأن تحدد خصائص هذه الأصول بناءً على التأثير الذي يمكن أن يؤدي إليه الإخلال بها في مجالي الأمن النووي والأمان النووي، وأن تنصّ في برامج الأمن الحاسوبي المعمول بها لديها على مستوى تدابير الأمن الحاسوبي المطلوب لكلّ من هذه الأصول الرقمية الحساسة.

4-4- وينبغي أن تنفذ السلطات المختصة والجهات المشغلة تدابير للأمن الحاسوبي تكفل حماية سرية الأصول الرقمية الحساسة والمعلومات الحساسة التي تحتوي عليها، وسلامة تلك الأصول والمعلومات وتوافرها. وعلى سبيل المثال، ينبغي أن تتسم تدابير الأمن الحاسوبي بالخصائص التالية:

- (أ) أن تكون مصمّمة بحيث تمنع الوصول غير المأذون به إلى الأصول الرقمية الحساسة من جانب أي أشخاص أو عمليات أو أجهزة (باتباع نهج متدرج).
- (ب) أن تكفل عدم إدخال شفرات أو بيانات خبيثة إلى الأصول الرقمية الحساسة.
- (ج) أن تكون مدمجة في ترتيبات إدارة سلسلة الإمداد.

4-5- وينبغي أن تضع السلطات المختصة والجهات المشغلة عملية رسمية لضمان عدم منح الأذن اللازمة لأداء الأنشطة المتصلة بالأمن الحاسوبي إلا للموظفين الذين يتأكد تحليلهم بمستوى مناسب من الكفاءة والجدارة بالثقة.

4-6- وينبغي ألا تسمح السلطات المختصة والجهات المشغلة للموظفين الذين لم تتأكد جدارتهم بالثقة بأداء هذه الأنشطة إلا في الحالات الاستثنائية وrehناً بوجود تدابير أمنية تعويضية محكمة لمنع الأعمال غير المأذون بها أو الكشف عنها.

4-7- وينبغي للسلطات المختصة والجهات المشغلة أن تُقيّم وتدير ما يتصل بالأمن الحاسوبي من أوجه الترابط بين الأمن والأمان النوويين [4] بطريقة تكفل ألا تؤثر التدابير المتخذة في أحد المجالين سلباً في المجال الآخر، بل أن يدعم كل منهما الآخر قدر الإمكان.

4-8- وينبغي لكل سلطة مختصة وجهة مشغلة أن تتعهد برنامجاً للأمن الحاسوبي يبيّن الكيفية التي ستوفر بها تلك السلطة أو الجهة مستوى ملائماً من الأمن الحاسوبي، وفقاً للمتطلبات المفروضة من الدولة وسلطتها المختصة بالأمن الحاسوبي. فإذا كانت هناك عدّة منظمات تشترك في نفس الأصول الرقمية الحساسة أو يعتمد بعضها على بعض في هذا الصدد، فينبغي تجسيد جميع المسؤوليات أو الارتباطات المشتركة في برامج الأمن الحاسوبي الخاصة بكل منها.

4-9- وينبغي أن تجري السلطات المختصة والجهات المشغلة تقييمات دورية لتدابير الأمن الحاسوبي المعمول بها لديها للتأكد من امتثالها للمتطلبات الرقابية. وينبغي تحديد الفترة الفاصلة بين هذه التقييمات بحيث تتيح الإسراع بمراجعة أي تغييرات تطرأ على التهديدات أو على أي عوامل أخرى تؤثر في المخاطر. ويمكن لأنشطة التقييم أن تشمل عمليات المراجعة والاستعراض واختبارات الأداء والتمارين، حسب الاقتضاء. وينبغي أن تجري السلطات المختصة والجهات المشغلة تقييمات ذاتية أيضاً عند تعديل النظم الحاسوبية، للنظر فيما إذا كانت التعديلات المدخلة على هذه النظم تنطوي على جوانب ضعف جديدة و/أو تستحدث أصولاً رقمية حساسة جديدة.

## العمل مع البائعين والمتعاقدين والموردين

10-4- ينبغي أن تفرض السلطات المختصة والجهات المشغلة شروطاً تعاقدية على البائعين والمتعاقدين والموردين لإلزامهم بتنفيذ تدابير الأمن الحاسوبي المناسبة مع الأدوار الموكلة إليهم. وينبغي أن تنص الشروط التعاقدية على تدابير للأمن الحاسوبي تكفل ألا تؤدي أنشطة أي من الطرفين إلى إيجاد مسار لتنفيذ هجوم سيبراني على الطرف الآخر وتوفير الحماية المناسبة للمعلومات الحساسة الخاصة بكل من الطرفين.

11-4- وينبغي أن تكون لدى السلطات المختصة والجهات المشغلة ومن تتعامل معهم من البائعين والمتعاقدين والموردين بروتوكولات وإجراءات تكفل الإبلاغ في الوقت المناسب عن المعلومات المتعلقة بحوادث الأمن الحاسوبي.

## السلطة المختصة بالأمن الحاسوبي

12-4- وينبغي أن تضع السلطة المختصة بالأمن الحاسوبي متطلبات ومعايير وتوصيات متعلقة بالأمن الحاسوبي لكل سلطة مختصة أو جهة مشغلة وفقاً لما يناسبها بناء على نهج متدرج قائم على العلم بالمخاطر.

13-4- وينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من أن هذه المتطلبات تجسّد مقتضيات الاستراتيجية، بمراعاة ما لدى السلطة المختصة أو الجهة المشغلة المعنية من المتطلبات التشغيلية والأمنية المحددة والقدرات والكفاءات المؤكدة.

14-4- وينبغي أن تتبّع السلطة المختصة بالأمن الحاسوبي نهجاً متدرجاً يقوم على العلم بالمخاطر [1] وعلى مبدأ الدفاع في العمق لتحقيق مستوى ملائم من الأمن الحاسوبي.

15-4- وينبغي أن تكفل كل سلطة مختصة خضوع جميع ما يدخل في نطاق مسؤوليتها من العمليات التي تُنفَّذ في أي مرحلة من مراحل دورة حياة الأصول الرقمية الحساسة (مثل التصميم والتنفيذ والصيانة والتخلص النهائي) للمراقبة والرصد والتوثيق على النحو المناسب.

16-4- وينبغي أن تتحقق كلُّ سلطة مختصة من الامتثال المستمر للوائح الأمن الحاسوبي الخاصة بها من خلال إجراء عمليات تقييم منتظمة، والتأكد، عند الاقتضاء، من اتخاذ الإجراءات التصحيحية اللازمة.

17-4- وقد تفرض السلطة المختصة بالأمن الحاسوبي على السلطات المختصة أو الجهات المشغلة تنفيذ تدابير معينة للأمن الحاسوبي بناءً على تقييمها للمخاطر (أي أن تأخذ بنهج أمر). أو بدلاً من ذلك، يمكن للسلطة المختصة بالأمن الحاسوبي أن تضع متطلبات قائمة على أساس الأداء فيما يتعلق بالأمن الحاسوبي، بحيث تسمح للسلطات المختصة أو الجهات المشغلة بأن تحدد بنفسها تدابير الأمن الحاسوبي المناسبة وفقاً لنهج قائم على العلم بالمخاطر. ويمكن أيضاً للسلطة المختصة بالأمن الحاسوبي أن تأخذ بنهج يجمع بين عناصر من كلا النهجين.

18-4- وتتوقف معايير الاختيار بين اتباع نهج أمر واتباع نهج قائم على أساس الأداء (أو مزيج مناسب من النهجين معاً) على الإطار التشريعي والهيكل التنظيمي في الدولة المعنية، بالإضافة إلى عدة عوامل أخرى، ومنها ما يلي:

- (أ) مدى كفاءة الجهة المشغلة في تفسير متطلبات الأداء وفي تصميم نظام فعال للأمن النووي وتنفيذ ذلك النظام وتقييمه؛
- (ب) عدد المرافق والجهات المشغلة المختلفة التي ستخضع للتنظيم الرقابي ومدى تنوعها، ومستوى التقييد الذي ستفرضه المتطلبات الأمرة على مرونة الجهة المشغلة في وضع التدابير المناسبة؛
- (ج) مدى شدة العواقب المحتملة للأعمال الشريرة المتوخى منعها أو الحماية منها [10].

### النهج الأمر

19-4- في حالة اتباع نهج أمر، تضع السلطة المختصة بالأمن الحاسوبي تدابير الأمن الحاسوبي المحددة التي تعتبرها لازمة لتحقيق مقاصد الأمن الحاسوبي التي حدتها.

20-4- وللنهج الأمر عدّة مزايا منها بساطة تنفيذه، سواء من منظور السلطة المختصة بالأمن الحاسوبي أو من منظور السلطة المختصة أو الجهة المشغلة المعنية، وتلافي الحاجة إلى تقاسم معلومات حساسة، وسهولة التفتيش والتقييم. وقد يكون استخدام النهج الأمر مناسباً بوجه خاص في الحالات التي يكون فيها كلُّ من مستوى التهديدات

ومستوى العواقب الإشعاعية المحتملة منخفضاً. وقد يكون النهج الأمر هو الأنسب أيضاً في الحالات التي لا يكون فيها من المجدي عملياً إجراء تقييم مفصل للتهديدات أو إعداد وصف للتهديدات المحتاط لها في التصميم.

4-21- بيد أن النهج الأمر قد يفتقر للمرونة اللازمة للتصدي لظروف معينة. وبالإضافة إلى ذلك، ففي حالة الأخذ بهذا النهج لا تتحمل السلطة المختصة المعنية المسؤولية عن التأكد من كفاية تدابير الأمن الحاسوبي المعمول بها؛ وإنما تقع المسؤولية الرئيسية عن التصدي للمخاطر على عاتق السلطة المختصة بالأمن الحاسوبي، لأنها هي التي تحدّد سلفاً تدابير الأمن الحاسوبي اللازمة للتصدي لتهديدات الهجمات السيبرانية. ولا تكون السلطة المختصة أو الجهة المشغلة المعنية مسؤولة إلا عن تنفيذ تدابير الأمن الحاسوبي المفروضة من سلطة الأمن الحاسوبي.

### النهج القائم على أساس الأداء

4-22- في حالة اتباع نهج قائم على أساس الأداء، تضع السلطة المختصة بالأمن الحاسوبي مجموعة من مقاصد الأمن الحاسوبي، وتُلزم السلطات المختصة والجهات المشغلة بتصميم وتنفيذ تدابير الأمن الحاسوبي الكفيلة ببلوغ هذه المقاصد، بحيث تحقّق مستوى محدداً من الفعالية في إرساء الحماية من الهجمات السيبرانية وتوفير إجراءات التصدي للطوارئ.

4-23- ويمتاز النهج القائم على أساس الأداء بأنه يكفل للسلطات المختصة والجهات المشغلة مرونة اقتراح تدابير الأمن الحاسوبي في توليفات تخصّ كل منظمة على حدة. وتخضع هذه التدابير للاختبار للتحقّق من كفايتها على أساس تقييم التهديدات أو وصف التهديدات المحتاط لها في التصميم، بما يكفل التأكد من أن مجموعة التدابير القائمة على أساس الأداء تفي بالمقاصد. ومن مزايا النهج القائم على أساس الأداء أنه يسلم بإمكانية تحقيق الأمن الحاسوبي الفعال عن طريق العديد من التوليفات المختلفة من تدابير الأمن الحاسوبي، وباختلاف حالة كلّ منظمة وظروفها التشغيلية.

4-24- ويتوقف اختيار هذا النهج على توافر الكفاءات والقدرات الكافية في مجال الأمن الحاسوبي، سواء لدى السلطة المختصة بالأمن الحاسوبي أو لدى السلطات المختصة والجهات المشغلة، على النحو اللازم لوضع المتطلبات وتنفيذ تدابير الأمن الحاسوبي. وقد يتطلب النهج القائم على أساس الأداء من الدولة أن تقدّم إلى السلطات المختصة والجهات المشغلة معلومات حساسة مستمدة من تقييم التهديدات أو من وصف

التحديات المحتاط له في التصميم.

## النهج المختلط

25-4- يتضمن النهج المختلط عناصر من كل من النهج الأمر والنهج القائم على أساس الأداء. وهناك طرائق عديدة لتطبيق النهج المختلط، ومنها الطريقتان التاليتان:

- (أ) يمكن للدولة أن تشترط تطبيق نهج قائم على أساس الأداء في الظروف التي يكون فيها الأثر المحتمل مرتفعاً أو مرتفعاً للغاية، مع السماح بتطبيق نهج أمر في الحالات التي يكون فيها الأثر المحتمل منخفضاً أو منخفضاً للغاية؛
- (ب) يمكن للدولة أن تفرض مجموعة من المتطلبات الأمر الواجبة الاتباع لمعالجة بعض جوانب الأمن الحاسوبي المحددة (مثل حماية المعلومات السرية)، على أن توضع تدابير الأمن الحاسوبي المكملّة اللازمة لمعالجة سائر الجوانب باستخدام نهج قائم على أساس الأداء.

26-4- والميزة الأساسية للنهج المختلط هي المرونة التي يتيحها. أمّا أوجه القصور في النهج المختلط فهي مماثلة لأوجه القصور في النهج القائم على أساس الأداء وفي النهج الأمر، وتتوقف على طريقة التنفيذ المحددة. بيد أن النهج المختلط، إذا ما نُفذ تنفيذاً جيداً، يمكن أن يقيم توازناً مناسباً ويقلل من الآثار المترتبة على ما ينطوي عليه كل من النهجين من أوجه القصور.

## الهيئة الرقابية

27-4- ينبغي أن تضع الهيئة الرقابية<sup>8</sup> المعنية بالأمن النووي متطلبات رقابية لتدابير الأمن الحاسوبي من أجل حماية الأصول الرقمية الحساسة والمعلومات الحساسة المرتبطة

<sup>8</sup> قد يوجد لدى الدولة أكثر من هيئة رقابية واحدة، بحيث تتولى كل هيئة رقابية المسؤولية عن الأمن النووي في سياق مختلف؛ فعلى سبيل المثال، يمكن أن تكون الهيئة الرقابية المسؤولة عن الأمن النووي في المرافق النووية غير الهيئة الرقابية المسؤولة عن الأمن النووي في القطاعات الصناعية التي تستخدم المصادر المشعة. وتُستخدم عبارة "الهيئة الرقابية" في هذا المنشور للإشارة إلى الهيئة التي تتحمل المسؤولية في سياق معين. وقد تكون الهيئة الرقابية المعنية بالأمن النووي هي نفسها السلطة المختصة بالأمن الحاسوبي، وفي هذه الحالة تنطبق عليها أيضاً الإرشادات الواردة في القسم الفرعي السابق.

بها. وينبغي أن تضع الهيئة الرقابية اللوائح الكفيلة بأن تؤدي جميع الكيانات المعنية مسؤولياتها المتعلقة بالأمن الحاسوبي وفقاً للمتطلبات الرقابية.

28-4- وينبغي أن تتأكد الهيئة الرقابية من أن لوائحها تتسم بقدر كاف من المرونة بحيث تكون قابلة للتكيف مع التغيرات التي تطرأ على طبيعة وظروف النظم الحاسوبية والهجمات السيبرانية و تدابير الأمن الحاسوبي.

29-4- ويُقترح أن تصدر الهيئة الرقابية دليلاً إلى لوائحها السارية في مجال الأمن الحاسوبي لمساعدة الكيانات المعنية على تنفيذها. وينبغي استعراض هذا الدليل دورياً للتأكد من أنه يتناول التهديدات السيبرانية ومقاصد اللوائح على نحو وافي.

30-4- وينبغي أن تكفل الهيئة الرقابية أن يكون الأمن الحاسوبي جزءاً من عمليات التقييم والترخيص وغيرها من إجراءات منح الأذن للجهات المرخص لها.

31-4- وينبغي أن تتأكد الهيئة الرقابية من أن كل جهة مشغلة لديها برنامج للأمن الحاسوبي يصف تدابير الأمن الحاسوبي المعمول بها لديها.

32-4- وينبغي أن تتحقق الهيئة الرقابية من الامتثال المستمر للمتطلبات الرقابية وشروط الترخيص المتعلقة بالأمن الحاسوبي، من خلال القيام بعمليات تفتيش منتظمة والاستعانة، عند الاقتضاء، بتدابير الإنفاذ اللازمة لضمان اتخاذ الإجراءات التصحيحية في الوقت المناسب.

## 5- وضع استراتيجية الأمن الحاسوبي

### استراتيجية الأمن الحاسوبي في إطار منظومة الأمن النووي

5-1- تبين الاستراتيجية<sup>9</sup> الأهداف الأساسية العامة المتوخاة في مجال الأمن الحاسوبي في إطار منظومة الأمن النووي الخاصة بالدولة، والتي ينبغي تجسيدها في الوثائق الفرعية الأكثر تفصيلاً التي ستستخدم في تنفيذ الاستراتيجية. ويلزم أن تكون الاستراتيجية قابلة للإنفاذ والتحقيق والمراجعة.

5-2- وينبغي أن تشمل الاستراتيجية على البنود التالية:

- (أ) كيفية إجراء تقييم التهديدات، بما في ذلك وضع سيناريوهات محتملة للهجمات السيبرانية؛
- (ب) كيفية تحديد مقاصد الأمن الحاسوبي؛
- (ج) كيفية تحديد الكفاءات ومستويات القدرات اللازمة في مجال الأمن الحاسوبي؛
- (د) طريقة توزيع الأدوار والمسؤوليات المتعلقة بالأمن الحاسوبي على جميع السلطات المختصة والجهات المشغلة (وربما أيضاً على البائعين والمتعاقدين والموردين)؛
- (هـ) تحديد الثغرات في القدرات القائمة، وإنشاء منظمات جديدة أو تعديل الأدوار الموكلة إلى المنظمات القائمة في مجال الأمن الحاسوبي لسد تلك الثغرات؛
- (و) النهج المتبعة في تنفيذ أنشطة الأمن الحاسوبي من جانب السلطات المختصة والجهات المشغلة، وفي تحقيق التكامل والتنسيق بين هذه الأنشطة؛
- (ز) التدابير اللازمة للمحافظة على استدامة قدرات الأمن الحاسوبي ضمن منظومة الأمن النووي.

5-3- وتقدّم الأقسام من 5 إلى 8 إرشادات إضافية بشأن هذه البنود التي ينبغي توثيقها في الاستراتيجية.

5-4- ويصف هذا القسم الأنشطة التحضيرية التي ينبغي أن تضطلع بها الدولة وسلطاتها

---

<sup>9</sup> للدولة أن تختار إدراج بعض المعلومات الحساسة في تذييلات تُلحق بالاستراتيجية، مما يسهّل تقييد توزيع تلك المعلومات.

المختصة بالأمن الحاسوبي في سبيل وضع الاستراتيجية، بما في ذلك ما يلي:

- (أ) إجراء تقييم للتهديدات؛
- (ب) تقييم الأثر المترتب على الأمن النووي في حال تعرّض الأصول الرقمية الحساسة لهجوم سيبراني؛
- (ج) الاختيار بين اتباع نهج أمر أو نهج قائم على أساس الأداء، أو مزيج من النهجين، فيما يخصّ التنظيم الرقابي للأمن الحاسوبي،
- (د) وضع إطار للقدرات والكفاءات في مجال الأمن الحاسوبي؛
- (هـ) تنفيذ (التكامل والتنسيق بين) أنشطة الأمن الحاسوبي من جانب السلطات المختصة والجهات المشغلة.

### تقييم التهديدات السيبرانية لمنظومة الأمن النووي

5-5- ينبغي أن تتعهد الدولة تقييماً محدثاً وفقاً لآخر المستجدات للتهديدات التي تمسُّ بمنظومة الأمن النووي الخاصة بها [5، 1]. ويمكن استخدام هذه المعلومات لإعداد بيانٍ وطني بالتهديدات أو وصف للتهديدات المحتاط لها في التصميم.

5-6- وينبغي أن يشمل تقييم الدولة للتهديدات و/أو وثقتها لوصف التهديدات المحتاط لها في التصميم الخصوم الذين يُحتمل أن ينفّذوا هجمات سيبرانية أو هجمات مختلطة، بما في ذلك إمكانية الاستعانة بأطراف داخلية في تنفيذ هذه الهجمات.

5-7- وتتيح الهجمات السيبرانية للخصم أن يشرع في تنفيذ عمله الشرير من خارج الموقع المستهدف، بل من خارج الولاية القضائية الوطنية التي يخضع لها الموقع المستهدف. ولذلك ينبغي أن تأخذ الدولة التهديدات الدولية في الحسبان عند إعداد التقييم.

5-8- وينبغي أن تتأكد الدولة من التحديث الدوري لتقييم تهديدات الهجمات السيبرانية (تقييم التهديدات السيبرانية). وينبغي استعراض تقييم التهديدات بوتيرة تواكب سرعة تطور التكنولوجيات والتقدم الذي تشهده النظم الحاسوبية وما يُستجد اكتشافه من جوانب الضعف، وكذلك الطابع المتغير الذي تتسم به الهجمات السيبرانية ومن ثم نُهج الأمن الحاسوبي.

9-5- وينبغي أن تتأكد الدولة من إبلاغ السلطات المختصة والجهات المشغلة المعنية بالتغيرات التي تطرأ على تقييم التهديدات السيبرانية، في الوقت المناسب وبطريقة آمنة.

10-5- وينبغي أن تتخذ الدولة جميع الخطوات المعقولة لكي تأخذ في الحسبان الطابع المتغير الذي تتسم به التهديدات السيبرانية، وأن تشجع الأخذ بتدابير الأمن الحاسوبي القادرة على استباق ما يطرأ على هذه التهديدات من تغيرات أو التكيف معها بسهولة بحيث تظل فعالة في مواجهة التهديدات.

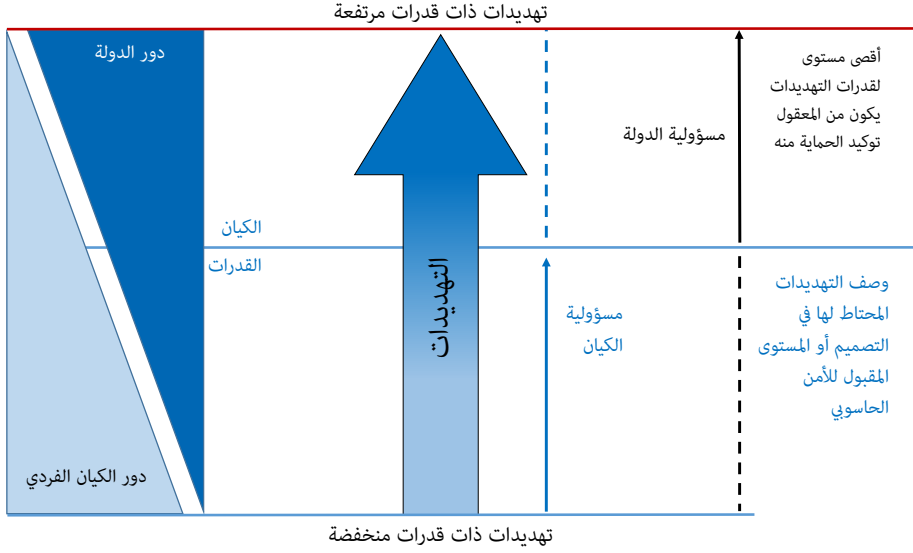
11-5- وبالإضافة إلى المعلومات المتاحة لوكالات الاستخبارات الوطنية، قد تكون لدى السلطات المختصة الأخرى والجهات المشغلة والبائعين والمتفاعدين والموردين معلومات يمكن أن تسهم في تقييم التهديدات.

12-5- ويمكن للدولة أن تضع بروتوكولات لتنظيم تقاسم المعلومات عن التهديدات على نحو آمن، بما في ذلك إنشاء قنوات اتصال مباشرة فيما بين المنظمات.

13-5- ولا يمكن أن يُتوقع من السلطات المختصة والجهات المشغلة أن توفر الحماية من التهديدات مهما كان مستواها. ففوق مستوى معين، يُتوقع من الدولة أن تتدخل لدعم السلطة المختصة أو الجهة المشغلة في التصدي للتهديدات التي تواجهها (الشكل-6). وفي حالة السلطات المختصة والجهات المشغلة التي تستخدم وصفاً للتهديدات المحتاط لها في التصميم، يُشار إلى ذلك باسم "الأحداث المجاوزة للتهديدات المحتاط لها في التصميم".

14-5- وينبغي أن تتأكد الدولة من أن تقييم التهديدات و/أو وصف التهديدات المحتاط لها في التصميم، المعد لأغراض الأمن الحاسوبي، يوفر التفاصيل الكافية لإجراء تقييمات المخاطر اللاحقة، ومن ثم تنفيذ الأمن الحاسوبي تنفيذاً مناسباً وفعالاً في جميع جوانب منظومة الأمن النووي الخاصة بالدولة.

15-5- وينبغي أن تحدد الدولة، عن طريق السلطة المختصة بالأمن الحاسوبي، المعايير والعمليات والموارد المتعلقة بالتصدي للهجمات السيبرانية ضد السلطات المختصة والجهات المشغلة ومن تتعامل معهم من البائعين والمتفاعدين والموردين. وينبغي أن تشمل هذه العمليات بروتوكولات للاتصالات الآمنة مع الجهة المسؤولة عن التصدي.



الشكل-6- الأدوار والمسؤوليات المتعلقة بالحماية من التهديدات.

## تعيين سلطة مختصة بتقييم التهديدات السيبرانية

16-5- ينبغي أن تكفل الدولة إجراء تقييم لتهديدات الهجمات السيبرانية بوتيرة منتظمة وفي الوقت المناسب. وينبغي أن تسند الدولة هذا الدور إلى سلطة مختصة لديها الخبرات اللازمة للوقوف على التهديدات السيبرانية وتقييمها. وقد تكون السلطة المختصة بتقييم التهديدات السيبرانية غير السلطة المختصة بالأمن الحاسوبي.

17-5- وينبغي للسلطة المختصة بتقييم التهديدات السيبرانية أن تضطلع بالمهام المسندة إليها بالتشاور والتعاون مع جميع السلطات المختصة والجهات المشغلة التي تقرر الدولة أنها تؤدي أدواراً وتحمل مسؤوليات في تقييمات التهديدات السيبرانية وأن لديها الكفاءات والقدرات اللازمة للمشاركة بصفة رسمية في عملية تقييم التهديدات السيبرانية. وينبغي أن تقود السلطة المختصة عملية التنسيق والجمع بين المساهمات المختلفة التي تقدمها هذه الجهات إلى عملية تقييم تهديدات الهجمات السيبرانية.

18-5- وينبغي أن تكون السلطة المختصة بتقييم التهديدات السيبرانية مسؤولة عن التأكد من أن تقييم التهديدات السيبرانية يوفر التفاصيل الكافية لإجراء تقييمات المخاطر

اللاحقة التي سوف تُستخدم في تصميم تدابير الأمن الحاسوبي المناسبة وتنفيذها بفعالية في جميع جوانب منظومة الأمن النووي الخاصة بالدولة.

## تقييم الأثر المترتب على اختلال تشغيل الأصول الرقمية الحساسة

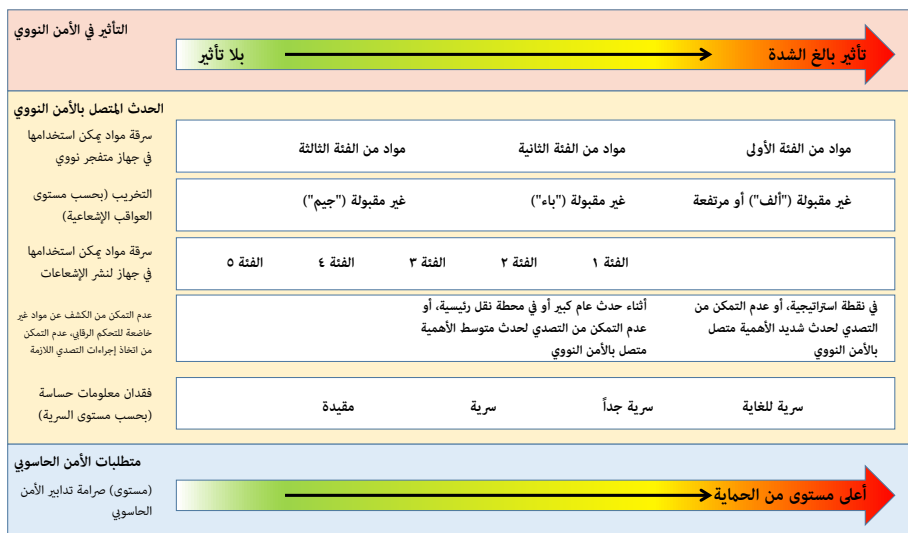
5-19- ينبغي أن تحدد السلطة المختصة بالأمن الحاسوبي، فيما يخص كل سلطة مختصة وجهة مشغلة معنية على حدة، مستوى شدة العواقب المحتملة للهجمات السيبرانية التي تلتزم تلك السلطة أو الجهة بتوفير الحماية منها عن طريق تنفيذ تدابير فعالة للأمن الحاسوبي.

5-20- وينبغي أن يستند تقييم شدة العواقب إلى الخصائص والسمات اللصيقة بالأصول الرقمية الحساسة. وينبغي أن تنظر السلطات المختصة والجهات المشغلة في شدة العواقب بمعزل عن احتمالية وقوعها وعن نوع الهجمات السيبرانية التي يمكن أن تفضي إليها.

5-21- ويقدم الشكل 7 توضيحاً بصرياً للمستويات المختلفة من الآثار التي تترتب على أنواع متعددة من الأحداث المتصلة بالأمن النووي في مختلف مجالات الأمن النووي التي تتناولها المراجع [3 إلى 5]. وينبغي أن تقف السلطة المختصة بالأمن الحاسوبي على مستوى شدة العواقب وتقيم مدى كفاية تدابير الأمن الحاسوبي المعمول بها لضمان منع وقوع تلك العواقب أو التخفيف من آثارها إذا وقعت.

5-22- ويمكن للسلطة المختصة بالأمن الحاسوبي أن تحدد، بالتعاون مع السلطات المختصة المعنية الأخرى، مستوى الحماية الواجب لكل مستوى من مستويات شدة العواقب.

5-23- ويتطلب تنفيذ الأمن الحاسوبي بفعالية وجود نطاق من الكفاءات ومستويات القدرات التي تتناسب مع الأدوار والمسؤوليات المسندة إلى كل جهة معنية من السلطات المختصة والجهات المشغلة والبائعين والمتعاقدين والموردين. وفي الحالات التي تتطلب اتخاذ قرارات وإجراءات بناءً على أحكام تقديرية، يلزم توافر مستويات أعلى من القدرات بالضرورة. وتشمل متطلبات فعالية الأمن الحاسوبي تحديد هذه الكفاءات والقدرات لكل جهة معنية من السلطات المختصة والجهات المشغلة والبائعين



الشكل 7-7- رسم توضيحي للتفاوت في شدة العواقب الناجمة عن أنواع مختلفة من الأحداث المتصلة بالأمن النووي (وتجدر الإشارة إلى عدم التكافؤ بين مقاييس أثر الأنواع المختلفة من الأحداث، وينبغي تقييم شدة أثر كل نوع منها على حدة).

والمتعاقدين والموردين، والتأكد من المحافظة على هذه الكفاءات والقدرات وتطبيقها.

24-5- وينبغي أن تضع السلطة المختصة بالأمن الحاسوبي إطاراً للكفاءات ومستويات القدرات في مجال الأمن الحاسوبي. ويرد في المرفق الرابع مثال لهذا الإطار.

25-5- وينبغي أن يكفل الإطار أن تكون الكفاءات ومستويات القدرات المطلوب توافرها لدى كل جهة معنية من السلطات المختصة والجهات المشغلة والبائعين والمتعاقدين والموردين متناسبة مع المسؤوليات المسندة إلى تلك الجهة في مجال الأمن الحاسوبي. ويمكن الاطلاع على مزيد من الإرشادات بشأن تعريف الأدوار، وإرساء الكفاءات والمحافظة عليها داخل المنظمات، وبناء قدرات المنظمات والأفراد، في منشورين آخرين صادرين عن الوكالة في سلسلة الأمن النووي [11، 3].

## طريقة تقييم المخاطر لتحديد تدابير الأمن الحاسوبي

26-5- ينبغي أن يستند تطبيق تدابير الأمن الحاسوبي إلى نهج قائم على العلم بالمخاطر. وينبغي أن تحدد السلطة المختصة بالأمن الحاسوبي طريقة تقييم المخاطر أو سلسلة الطرائق التي تستخدمها المنظمات المسؤولة للقيام بما يلي:

- (أ) تحديد ما إذا كان كل نظام من النظم الحاسوبية يؤدي وظيفة ذات صلة بمنظومة الأمن النووي؛
- (ب) تحديد ما إذا كان كل أصل من الأصول الرقمية يمثل أصلاً رقمياً حساساً؛
- (ج) إجراء تحليل لمخاطر الأمن الحاسوبي لتحديد مستوى الصرامة المطلوب لتدابير الأمن الحاسوبي المنطبقة على كل أصل رقمي حساس أو غير حساس، على النحو المبين في الشكل-3.

27-5- وينبغي أن تأخذ طريقة التقييم في الحسبان ما يلي:

- (أ) أي تشريعات أو لوائح ذات صلة؛
- (ب) أهمية الوظائف التي يؤديها الأصل الرقمي الحساس، بما في ذلك أهمية حماية سرية وسلامته وتوافره، هو والمعلومات التي يحتوي عليها، لكل من الأمن والأمان النوويين (أي تصنيفه من حيث فئة الأمان)؛
- (ج) تقييم عواقب تعرض الأصل الرقمي الحساس لهجمات سيبرانية؛
- (د) البيئة التشغيلية للأصل الرقمي الحساس؛
- (هـ) تحديد وتقييم التهديدات ذات الصلة بالسلطات المختصة والجهات المشغلة، ومن تتعامل معهم من البائعين والمتعاقدين والموردين، وبالأصل الرقمي الحساس وفقاً للتقييم الوطني للتهديدات أو وصف التهديدات المحتاط لها في التصميم أو بيان التهديدات؛
- (و) مدى جاذبية الأصل الرقمي الحساس للأطراف التي تشكّل تهديدات للأمن النووي؛
- (ز) جوانب الضعف اللصيقة بالأصل الرقمي الحساس.

28-5- ويمكن للسلطة المختصة بالأمن الحاسوبي أن تعدّل نتائج تقييم المخاطر بناءً على الأثر المحتمل في حال الإخلال بالأصل الرقمي الحساس، وخصوصاً إذا كان ذلك

يؤدي إلى أي مما يلي:

- (أ) أن يصبح أداء الأصل الرقمي الحساس لوظيفته غير معروف النتيجة سلفاً؛
- (ب) أن يتصرف الأصل الرقمي الحساس وفقاً لسلوكيات أو إجراءات غير متوقعة؛
- (ج) أن يتعطل الأصل الرقمي الحساس؛
- (د) أن يؤدي الأصل الرقمي الحساس وظيفته كما هو متوقع (أي أن يتجاوز عن الخطأ).

5-29- وينبغي أن تنظر عملية تقييم المخاطر في جميع جوانب الأمن مجتمعة حتى تتناول مخاطر الهجمات المختلطة، التي يمكن أن تجمع بين الهجوم على الحماية المادية (بما في ذلك عن طريق الأفراد، ولا سيما الأطراف الداخلية) والهجوم السيبراني على الأمن الحاسوبي. وبناءً على ذلك، ينبغي أن تكون لدى القائمين على إجراء تقييم المخاطر القدرة على الوصول إلى الأفراد المختصين بجميع المجالات ذات الصلة، بما في ذلك الحماية المادية والأمن الحاسوبي لأغراض الأمن والأمان النوويين.

## 6- تنفيذ استراتيجية الأمن الحاسوبي

6-1- يصف هذا القسم مسؤوليات السلطة المختصة بالأمن الحاسوبي فيما يتعلق بإسناد الأدوار والمسؤوليات المتعلقة بالأمن الحاسوبي إلى السلطات المختصة والجهات المشغلة.

6-2- وينبغي توثيق هذه الأدوار والمسؤوليات في الاستراتيجية أو الوثائق الداعمة لها.

6-3- ويمكن للسلطة المختصة بالأمن الحاسوبي أن تضع متطلبات في شكل معايير، أو متطلبات رقابية عن طريق الهيئة الرقابية، أو متطلبات تعاقدية تُفرض على البائعين والمتعاقدين والموردين، ويمكن أن توفر وثائق إرشادية تبين فيها كيفية استيفاء هذه المتطلبات.

## إسناد المسؤوليات المتعلقة بالأمن الحاسوبي

4-6- ينبغي أن تكفل السلطة المختصة بالأمن الحاسوبي أن تُسند إلى جميع السلطات المختصة والجهات المشغلة التي تشغل أصولاً رقمية حساسة المسؤولية الرئيسية عن الأمن الحاسوبي لتلك الأصول الرقمية الحساسة ولأي أصول رقمية أخرى يمكن أن يؤدي الإخلال بها إلى التأثير سلباً في الأمن النووي أو الأمان النووي.

5-6- وينبغي أن تكفل السلطة المختصة بالأمن الحاسوبي أن تُسند إلى جميع الجهات المشاركة في دورة حياة الأصول الرقمية الحساسة، بما في ذلك السلطات المختصة والجهات المشغلة والبائعين والمتعاقدين والموردين، المسؤوليات المناسبة عن الأمن الحاسوبي لتلك الأصول الرقمية الحساسة.

6-6- وينبغي أن تكفل السلطة المختصة بالأمن الحاسوبي تقاسم المسؤوليات على نحو مناسب بين الدولة من ناحية والسلطات المختصة والجهات المشغلة من ناحية أخرى لضمان الإبقاء على المخاطر الناشئة عن تهديدات الأمن النووي الأكبر قدرة عند مستوى مقبول.

7-6- وينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من أن السلطات المختصة والجهات المشغلة المعنية تخطط للأمن الحاسوبي وتعالجه فيما يخص جميع المراحل التي ينطوي عليها اكتشاف حادثة من أحداث الأمن الحاسوبي والتصدي لها.

## العلاقات بين السلطات المختصة والجهات المشغلة

8-6- ينبغي أن تضع السلطة المختصة بالأمن الحاسوبي ترتيبات لتنسيق المسؤوليات المتعلقة بالأمن الحاسوبي فيما بين السلطات المختصة والجهات المشغلة في منظومة الأمن النووي وخارجها. وعلى سبيل المثال، فقد تكون هناك سلطات وطنية مسؤولة عن الأمن الحاسوبي خارج منظومة الأمن النووي، مما يستلزم التنسيق مع السلطات المشاركة في منظومة الأمن النووي.

9-6- وينبغي أن تقيم السلطة المختصة بالأمن الحاسوبي خطوطاً واضحة للاتصال بين السلطات المختصة والجهات المشغلة، ومع الهيئة أو الآلية التنسيقية المشار إليها في

الفقرة 3-11، إن وُجدت.

10-6- وينبغي أن تكفل السلطة المختصة بالأمن الحاسوبي وجود آلية للتعاون والتنسيق وتبادل المعلومات، ولتحقيق التكامل في أنشطة الأمن الحاسوبي عند الاقتضاء، بين السلطات المختصة والجهات المشغلة.

11-6- وعند إسناد المسؤوليات المتعلقة بالأمن الحاسوبي إلى السلطات المختصة والجهات المشغلة، ينبغي للسلطة المختصة بالأمن الحاسوبي أن تقيم توازناً بين مطلبين متنافسين هما الحاجة إلى إرساء الدفاع في العمق، والحاجة إلى تحقيق الكفاءة والفعالية في استخدام الموارد المتاحة لمنظومة الأمن النووي الخاصة بالدولة، وذلك بمراعاة الاعتبارين التاليين:

(أ) أن الاستقلالية تسهم في إرساء الدفاع في العمق لأنَّ الأخذ بخيارات تصميمية وتشغيلية مستقلة يقلل من احتمالية وقوع أعطال ترجع لسبب مشترك أو تتخذ نمطاً مشتركاً. وتشمل الاستقلالية كلاً من الاستقلالية الوظيفية والمالية عن المنظمات الخاضعة للرقابة وعن أي هيئات أخرى معنية باستخدام المواد النووية أو المواد المشعة الأخرى. وينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من أن السلطات المختصة والجهات المشغلة لديها الكفاءات ومستويات القدرات الكافية لدعم استقلاليتهما في اتخاذ القرارات بشأن الأمن الحاسوبي.

(ب) أنه يمكن تحسين الكفاءة والفعالية في استخدام الموارد عن طريق تقاسم القدرات. فعلى سبيل المثال، يمكن للسلطة المختصة أو الجهة المشغلة أن تعتمد على سلطة أخرى في المجالات المتخصصة من التحليل الجنائي لأغراض الأمن الحاسوبي، لأنَّه قلَّما يكون هناك احتياج إلى هذا الاختصاص. وفي مثل هذه الحالة، ينبغي إبرام اتفاق بين الكيانات يحدد وقت الاستجابة المتفق عليه لتقديم الدعم عند الطلب. وينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من وضع الترتيبات اللازمة لضمان تقديم الدعم بفعالية وفي الوقت المناسب في الحالات التي تحتاج فيها السلطات المختصة والجهات المشغلة للدعم من سلطات مختصة أخرى.

12-6- وعند النظر في كيفية إقامة التوازن بين استقلالية السلطات المختصة والجهات المشغلة من ناحية واعتماد بعضها على بعض من ناحية أخرى، ينبغي أن تنظر السلطة المختصة بالأمن الحاسوبي في الموارد اللازمة لتوفير الحماية من الهجمات المختلطة

والتصدي لها، وهو ما قد يتطلب مزيجاً من تدابير الأمن الحاسوبي وتدابير الأمن النووي الأخرى التي قد توفرها سلطات مختصة أخرى (مثل قوات التصدي المعنية بالحماية المادية).

13-6- وقد تؤدي عملية إسناد المسؤوليات وتحديد الكفاءات ومستويات القدرات اللازمة إلى الوقوف على الحاجة لإنشاء منظمات جديدة أو تعديل المنظمات القائمة.

### الكفاءات والقدرات في مجال الأمن الحاسوبي

14-6- ينبغي للسلطة المختصة بالأمن الحاسوبي أن تُلزم السلطات المختصة والجهات المشغلة بإجراء تحليل لمقاصدها في مجال الأمن الحاسوبي من أجل وضع قائمة شاملة بالكفاءات الواجب توافرها لديها. وقد تختار السلطة المختصة بالأمن الحاسوبي إجراء هذا التحليل بنفسها، لا سيما في الحالات التي تكون فيها أغلب تدابير الأمن الحاسوبي التي تطبقها السلطة المختصة أو الجهة المشغلة مفروضة من السلطة المختصة بالأمن الحاسوبي.

15-6- وينبغي للسلطة المختصة بالأمن الحاسوبي أن تُلزم السلطات المختصة والجهات المشغلة بأن تثبت أن لديها الكفاءات ومستويات القدرات الكافية للوفاء بالمسؤوليات المسندة إليها في مجال الأمن الحاسوبي. ويبيّن المرفق الثالث طريقة إسناد المسؤوليات للسلطات المختصة وفقاً للتوزيع النمطي، في حين يعرض المرفق الرابع مثلاً لإطار الكفاءات ومستويات القدرات.

16-6- وينبغي للسلطة المختصة بالأمن الحاسوبي أن تُلزم السلطات المختصة والجهات المشغلة بأن تثبت أن جميع الأفراد المكلفين بمسؤوليات متعلقة بالأمن الحاسوبي يتمتعون بالجدارة بالثقة، وأنهم مدربون على النحو المناسب ولديهم من المهارات والكفاءة ما يكفي لأداء واجبات وظائفهم، وأنهم على وعي بالتهديدات التي تطرحها الهجمات السيبرانية.

17-6- وينبغي للسلطة المختصة بالأمن الحاسوبي أن تُلزم السلطات المختصة والجهات المشغلة بتنفيذ برامج للتدريب المستمر لتنمية الكفاءات والمحافظة عليها بما يكفل الوفاء بمسؤولياتها في مجال الأمن الحاسوبي.

18-6- وينبغي للسلطة المختصة بالأمن الحاسوبي أن تشجع السلطات المختصة والجهات المشغلة على تقييم مستويات قدراتها في مجالات الكفاءات ذات الصلة بمسؤولياتها، وأن تدعم إرساء وتطوير الكفاءات اللازمة في تلك المجالات.

19-6- وينبغي للسلطة المختصة بالأمن الحاسوبي أن تضطلع بأنشطة توكيدية لتقييم ما يتمتع به موظفو السلطات المختصة والجهات المشغلة من التدريب والمهارات في مجال الأمن الحاسوبي. وينبغي للسلطة المختصة بالأمن الحاسوبي أن تفرض على كل سلطة مختصة وجهة مشغلة متطلبات تُلزمها بإثبات محافظتها باستمرار على الكفاءات ومستويات القدرات المحددة لها بما يتناسب مع المسؤوليات المسندة إليها فيما يتعلق بالأمن الحاسوبي.

### التصدي لحادثات الأمن الحاسوبي

20-6- ينبغي للسلطة المختصة بالأمن الحاسوبي أن تُلزم السلطات المختصة والجهات المشغلة بوضع إجراءات للأمن الحاسوبي وتنفيذها والتمرن عليها، لأغراض منع وقوع حادثات الأمن الحاسوبي والكشف عنها والتصدي لها إذا وقعت.

21-6- وينبغي أن توفر السلطة المختصة بالأمن الحاسوبي إرشادات للسلطات المختصة والجهات المشغلة بشأن تحديد الحادثات التي يمكن أن تكون متصلة بالأمن الحاسوبي. ويمكن لحادثات الأمن الحاسوبي أن تشكّل أيضاً أحداثاً متصلة بالأمن النووي، كما في حالة سرقة المعلومات الحساسة أو تعطيل وظائف الأمن النووي أو الأمان النووي. وبالإضافة إلى ذلك، يمكن أن تكون الهجمات السيبرانية جزءاً من هجمات مختلطة. وقد يعطي النجاح في الكشف عن الهجمات السيبرانية غير الملحوظة أو المستترة مؤشرات مسبقة على نوايا الخصوم المحتملة.

22-6- وينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من أنّ السلطات المختصة والجهات المشغلة والجهات المسؤولة عن التصدي لديها مستوى مناسب من قدرات التصدي اللازمة لمعالجة حادثات الأمن الحاسوبي، ومن أنّ برامج الأمن الحاسوبي الخاصة بهذه المنظمات تحدد الظروف التي تُفَعَّل فيها هذه القدرات.

23-6- وينبغي أن تضع السلطة المختصة بالأمن الحاسوبي متطلبات بشأن إبلاغ الهيئة الرقابية المعنية بالأمن النووي و/أو السلطات المختصة المعنية الأخرى عن حادثات

الأمن الحاسوبي في الوقت المناسب.

24-6- وينبغي أن تكفل السلطة المختصة بالأمن الحاسوبي أن تتولى سلطة مختصة أو جهة مشغلة لديها قدرات متقدمة بما في الكفاية (على سبيل المثال سلطة أو جهة لديها الكفاءة اللازمة في مجال التحليل الجنائي لأغراض الأمن الحاسوبي) إجراء عملية تقنية لتحديد خصائص أي حادثة متصلة بالأمن الحاسوبي تنطوي على أصل رقمي حساس.

## التمارين

25-6- وينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من اشتغال تمارين الأمن النووي المعقودة على مكوّن متعلق بالأمن الحاسوبي، لتقييم قدرة الدولة على التصدي لحادثات الأمن الحاسوبي، بما في ذلك الهجمات المختلطة.

26-6- وينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من أن السلطات المختصة والجهات المشغلة تجري تمارين منتظمة في مجال الأمن الحاسوبي لتدريب المشاركين والتحقق من صلاحية برامج الأمن الحاسوبي الخاصة بها، بما في ذلك خطط الطوارئ. وعند الاقتضاء، ينبغي إدماج هذه التمارين مع تمارين الأمن النووي الأخرى، وينبغي تنظيمها دورياً بالاقتران مع تمارين الطوارئ.

## الأنشطة التوكيدية

27-6- ينبغي للسلطة المختصة بالأمن الحاسوبي أن تنفذ أنشطة توكيدية لضمان الفعالية في تنفيذ الأمن الحاسوبي في جميع جوانب منظومة الأمن النووي الخاصة بالدولة والتحقق من أن تدابير الأمن الحاسوبي المعمول بها توفر الحماية بمستوى يتوافق مع تقييم التهديدات ومستوى المخاطر المقبول الذي حدده الدولة.

28-6- وينبغي للسلطة المختصة بالأمن الحاسوبي أن توفر للدولة توكيدات رسمية ومنتظمة بشأن توافر الكفاءات ومستويات القدرات الكافية في مجال الأمن الحاسوبي لدى جميع السلطات المختصة والجهات المشغلة.

## التأهيل الأمني للقطاع والخدمات

29-6- يتعيّن على السلطات المختصة والجهات المشغلة ومن تتعامل معهم من البائعين والمتعاقدين والموردين التأكد من أنّ المعدات والقطع والخدمات المشتراة تُنفَّذ بشأنها تدابير للأمن الحاسوبي تكفل منع استغلالها لإيجاد ثغرات تشكّل جوانب ضعف، بما في ذلك إدخال برامجيات خبيثة أو وضع مسارات لتنفيذ هجمات سيبرانية.

30-6- وينبغي للسلطات المختصة والجهات المشغلة أن تتأكد من أنّ من تتعامل معهم من البائعين والمتعاقدين والموردين الذين يساهمون في الأصول الرقمية الحساسة الخاضعة لمسؤوليتها ينفّذون متطلبات الأمن الحاسوبي ذات الصلة (مثل التطوير الآمن للبرامجيات) بهدف التقليل إلى أدنى حد من جوانب الضعف في الأصول الرقمية الحساسة ومنع استغلال سلسلة الإمداد كمسار لتنفيذ هجمات سيبرانية. ويشمل ذلك استعراض المنهجيات والعمليات والمعدات المستخدمة لدى البائعين والمتعاقدين والموردين.

31-6- ويمكن للسلطة المختصة بالأمن الحاسوبي أن تحدد معايير وطنية أو دولية لتستخدمها السلطات المختصة والجهات المشغلة والبائعون والمتعاقدون والموردون في وضع مواصفات المشتريات لأغراض الأصول الرقمية الحساسة والخدمات ذات الصلة. وينبغي أن تتناول هذه المعايير جميع مراحل دورة حياة الأصل الرقمي الحساس.

32-6- ويمكن للسلطة المختصة بالأمن الحاسوبي أن تسمي سلطة اعتماد تتولى تنفيذ الأنشطة اللازمة لتوكيد التزام البائعين والمتعاقدين والموردين القائمين على تصميم الأصول الرقمية الحساسة وتوفيرها ودعمها بممارسات الأمن الحاسوبي المطلوبة.

33-6- وتُشجّع السلطات المختصة والجهات المشغلة على إخضاع البائعين والمتعاقدين والموردين لفحوص توكيدية إضافية حسب الاقتضاء، مثل اختبارات قبول المرافق وعمليات التفتيش و/أو المراجعة لأغراض الأمن الحاسوبي (بناءً على المتطلبات التعاقدية).

## التعاون والمساعدة على الصعيد الدولي

34-6- ينبغي أن تكفل السلطة المختصة بالأمن الحاسوبي إقامة العلاقات اللازمة مع السلطات النظيرة في الدول الأخرى ومع الهيئات الدولية بما يتيح الاستفادة بفعالية من التعاون والمساعدة على الصعيد الدولي، حسب الاقتضاء، لدعم الأمن الحاسوبي فيما يتعلق بمنظومة الأمن النووي. وينبغي أن تنظر السلطة المختصة بالأمن الحاسوبي في هذه العلاقات في ضوء مسؤوليات جميع المنظمات المعنية وقدراتها وكفاءاتها.

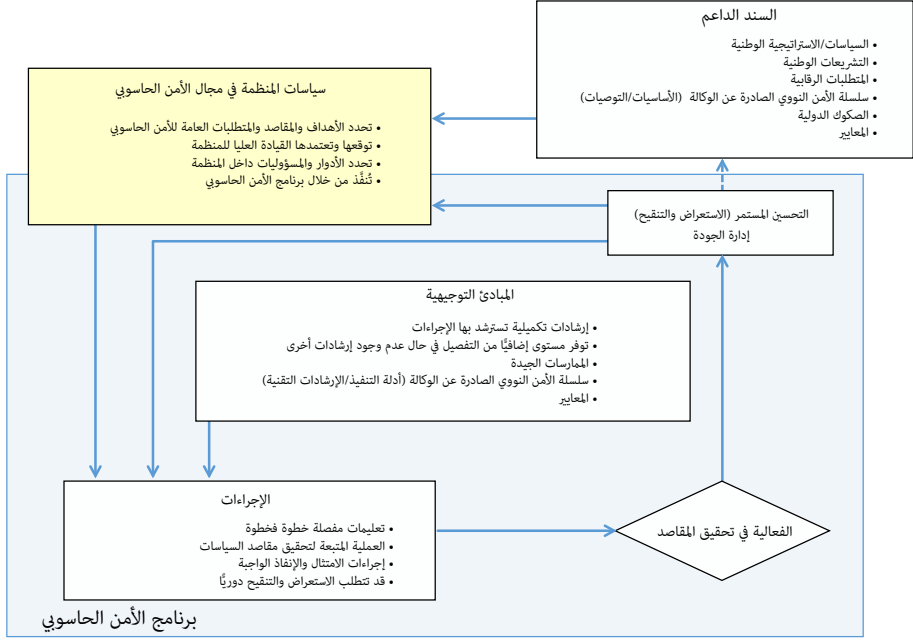
### 7- وضع برنامج للأمن الحاسوبي

1-7- يصف هذا القسم المكونات والتدابير الموصى بأن يتضمنها برنامج الأمن الحاسوبي الخاص بكل منظمة. ويعرض الشكل 8 إطاراً نموذجياً لبرنامج الأمن الحاسوبي، بما في ذلك الوثائق الداعمة والفرعية.

2-7- ويعرّف برنامج الأمن الحاسوبي الخاص بكل سلطة مختصة وجهة مشغلة الدور الذي تؤديه تلك السلطة أو الجهة في تنفيذ الاستراتيجية، في شكل أدوار ومسؤوليات وإجراءات مؤسسية. ويحدد برنامج الأمن الحاسوبي أيضاً الوسائل التي تسعى من خلالها السلطة المختصة أو الجهة المشغلة إلى تحقيق مقاصد الأمن الحاسوبي و/أو تنفيذ تدابير الأمن الحاسوبي المتوخاة في التشريعات واللوائح والمعايير والإرشادات الصادرة من الهيئة الرقابية التي تخضع لها ومن السلطة المختصة بالأمن الحاسوبي.

3-7- وينبغي أن تتأكد السلطة المختصة بالأمن الحاسوبي من وضع كل سلطة مختصة أو جهة مشغلة برنامجاً للأمن الحاسوبي وتعهدتها إياه على النحو المبين في هذا القسم. وينبغي وضع برنامج الأمن الحاسوبي ضمن إطار الخطة الشاملة لأمن الموقع والنظام الإداري لكل منظمة.

4-7- وينبغي أن تكفل السلطة المختصة بالأمن الحاسوبي تشجيع النظر إلى الأمن الحاسوبي بوصفه مكوناً أساسياً في ثقافة الأمن النووي، وأن تشجع الالتزام بتحسين المستمر من خلال التزامات صريحة من الإدارة العليا لكل سلطة مختصة أو جهة مشغلة.



الشكل 8- نظرة عامة على برنامج نمطي للأمن الحاسوبي.

## محتويات برنامج الأمن الحاسوبي

5-7- ينبغي أن يقدم برنامج الأمن الحاسوبي وصفًا للأمن الحاسوبي في المنظمة، من حيث إمكانية التأثير بمواطن الضعف وتدابير الحماية المعمول بها وتدابير تحليل العواقب والتخفيف منها، لتحديد المستوى المقبول من المخاطر الناشئة عن الهجمات السيبرانية والمحافظة عليه، وتيسير العودة إلى حالة تشغيلية مأمونة بعد وقوع الهجوم.

6-7- وينبغي أن يشمل برنامج الأمن الحاسوبي على المحتويات التالية على الأقل:

(أ) التنظيم والمسؤوليات:

- (1) الهياكل التنظيمية؛
- (2) الأشخاص المسؤولون والمسؤوليات المتعلقة بتقديم التقارير؛
- (3) العقوبات والإجراءات التصحيحية؛
- (4) عملية استعراض البرنامج دوريًا واعتماده؛

(5) أوجه الترابط مع البرامج الأخرى.

#### إدارة الأصول الرقمية:

- (1) قائمة بجميع النظم الحاسوبية؛
- (2) قائمة بجميع تطبيقات النظم الحاسوبية؛
- (3) رسوم تخطيطية لتدفق البيانات والشبكات، بما في ذلك جميع الوصلات بنظم حاسوبية خارجية؛
- (4) إدارة التهيئة (الأجهزة، البرامجيات الثابتة، التطبيقات البرمجية، حالة المعدات، وإعدادات التهيئة ذات الصلة)؛
- (5) تصنيف الأصول الرقمية وتحديد الأصول الرقمية الحساسة، بما في ذلك تصنيفها من حيث الأهمية (أي مدى مساهمتها في وظائف الأمن النووي والأمان النووي وحصر المواد النووية ومراقبتها).

#### تقييم المخاطر وجوانب الضعف والامتثال:

- (1) الوثيرة الدورية لعملية استعراض برنامج الأمن الحاسوبي وإعادة تقييمه؛
- (2) التقييم الذاتي (بما في ذلك إجراءات الاختبار النشط والخامل)؛
- (3) عملية إعادة تقييم المخاطر دورياً وعند الاقتضاء، والمنهجية ذات الصلة؛
- (4) إجراءات المراجعة وتتبع أوجه القصور وتصحيحها؛
- (5) استعراض الامتثال التشريعي والرقابي؛

#### تصميم أمن النظم:

- (1) المبادئ الأساسية للهندسة والتصميم؛
- (2) النهج الأساسية المتبعة في تصميم النظم (على سبيل المثال المستويات الأمنية والنطاقات الأمنية)؛
- (3) إضفاء طابع رسمي على متطلبات الأمن الحاسوبي المنطبقة على البائعين والمتعاقدين والموردين؛
- (4) الأمن على مدى دورة الحياة بأكملها.

## الإجراءات الأمنية التشغيلية:

- (1) التحكم في الوصول؛
- (2) أمن البيانات؛
- (3) أمن الاتصالات؛
- (4) أمن المنصات والتطبيقات (مثل التحصين، وإدارة برامج التصحيح، والحماية من البرامجيات الخبيثة)؛
- (5) رصد النظم (بما في ذلك إدارة السجلات)؛
- (6) صيانة الأمن الحاسوبي؛
- (7) التعامل مع الحوادث؛
- (8) استمرارية الأعمال والتعافي من الكوارث؛
- (9) النسخ الاحتياطي للنظم.

## إدارة شؤون الموظفين:

- (1) فحوص الجدارة بالثقة (إجراء تحريات عن الموظفين)؛
- (2) التوعية والتدريب؛
- (3) تأهيل الموظفين؛
- (4) إنهاء خدمة الموظفين أو نقلهم.

7-7- وينبغي أن يكون برنامج الأمن الحاسوبي جزءاً مدمجاً في النظام الإداري ومنسقاً مع سائر الأجزاء. ويمكن تقسيم برنامج الأمن الحاسوبي إلى أجزاء ذات مستويات مختلفة التصنيف الأمني، لتيسير استخدام البرنامج بكفاءة واتساق على أساس قاعدة "المعرفة حسب الحاجة" ومتطلبات السرية.

8-7- وينبغي استعراض برنامج الأمن الحاسوبي بانتظام وتحديثه لمواكبة ما يستجد من معارف مستمدة من داخل منظومة الأمن النووي ومن خارجها، بما في ذلك ما يلي:

- (أ) التكنولوجيات الجديدة التي يمكن استخدامها في تنفيذ الهجمات السيبرانية أو الحماية منها؛
- (ب) الخصائص الجديدة للتهديدات السيبرانية، بما في ذلك أي تغيرات تطرأ على التكتيكات والتقنيات وإجراءات العمل؛

(ج) الأنواع الجديدة من حوادث الأمن الحاسوبي أو الأحداث المتصلة بالأمن النووي.

9-7- وينبغي أن يتضمن برنامج الأمن الحاسوبي إجراء تمارين منتظمة لتدريب المشاركين والتحقق من صلاحية برنامج الأمن الحاسوبي، بما في ذلك خطط الطوارئ. وعند الاقتضاء، ينبغي إدماج هذه التمارين مع التمارين الأمنية الأخرى، وينبغي تنظيمها دورياً بالاقتران مع تمارين الطوارئ.

### تقييم المخاطر على مستوى المنظمة الواحدة

10-7- رهنأً بالقدرات المتوفرة لدى السلطات المختصة والجهات المشغلة والتأثير السلبي المحتمل للهجمات السيبرانية على الأصول الرقمية الحساسة الخاضعة لمسؤولية تلك المنظمات، يمكن لبرنامج الأمن الحاسوبي أن يتضمن منهجية لإجراء تقييمات داخلية للمخاطر المتعلقة بالنظم الحاسوبية الموجودة لدى المنظمة بمراعاة بيئة التهديدات الخاصة بتلك المنظمة.

11-7- ويتمثل الغرض من هذا النوع من التقييمات فيما يلي:

- (أ) تحديد وفهم المخاطر والعوامل المساهمة فيها؛
- (ب) توفير الأساس الذي يُستند إليه في تحديد النظم الحاسوبية والأصول الرقمية الحساسة؛
- (ج) إرساء قاعدة مرجعية لدعم عمليات تحليل التغيُّرات التي تطرأ على الأصول الرقمية الحساسة وغير الحساسة، والتهديدات، والتأثير المحتمل في الأمن الحاسوبي ومن ثم في الأمن النووي؛
- (د) المساعدة على التحقق من الامتثال للمتطلبات العامة.

12-7- ويمكن للمنظمة أن تجري تقييمات للمخاطر على مستوى المنظمة ككل أو على مستوى النظام الواحد.

13-7- وينبغي أن تستند هذه التقييمات إلى بيان التهديدات الوطني و/أو وصف التهديدات المحتاط لها في التصميم، وأن تأخذ في الحسبان المصادر الأخرى المتاحة للمعلومات عن التهديدات السيبرانية حتى يُسترشد بها في عملية التقييم.

14-7- وينبغي لعملية تقييم المخاطر أن تحدد الأصول الرقمية الحساسة بناءً على دراسة كل نظام حاسوبي من حيث ما يمكن أن يترتب على الإخلال بذلك النظام و/أو اختلال تشغيله من عواقب سلبية على الأمن النووي أو الأمان النووي.

15-7- وإذا كانت نتائج تقييم المخاطر تحيد كثيراً عما تفترضه السلطة المختصة بالأمن الحاسوبي، ينبغي أن تعتمد السلطات المختصة أو الجهات المشغلة إلى تسوية هذه المسألة على وجه السرعة. وقد ترجع أسباب التباين، على سبيل المثال، إلى تغيرات طرأت على بيئة التهديدات الخاصة بالمنظمة أو ظهور جوانب ضعف جديدة بسبب إدخال تغييرات على المعدات.

16-7- وينبغي أن تعالج تقييمات المخاطر جميع جوانب الأمن النووي مجتمعةً، بما فيها على سبيل المثال الحماية المادية والحماية من التهديدات الداخلية فضلاً عن الأمن الحاسوبي، حتى يتسنى تقييم مخاطر الهجمات المختلطة. وبناءً على ذلك، ينبغي إجراء تقييمات المخاطر بمساهمات من خبراء في كل مجال من هذه المجالات.

## تدابير الأمن الحاسوبي

17-7- يحدد برنامج الأمن الحاسوبي تدابير الأمن الحاسوبي التي توفر وظائف المنع والكشف والتعطيل والتصدي والتخفيف من العواقب وتكفل أيضاً ألا تؤدي الأعمال غير الشريرة إلى الإضرار بالأمن الحاسوبي بما يفضي إلى زيادة قابلية التعرض للهجمات السيبرانية.

18-7- وتنتمي تدابير الأمن الحاسوبي المحددة إلى أحد الأنواع الثلاثة التالية:

(أ) تدابير المراقبة التقنية: وهي الحلول القائمة على مكونات مادية و/أو برمجية والتي توفر الحماية من التسلل أو غيره من الأعمال الشريرة التي تستهدف الأصول الرقمية الحساسة، كما تكفل الكشف عن هذه الأعمال والتخفيف من عواقبها والتعافي منها. وعند تقييم أنواع التدابير المختلفة من حيث الفعالية، ينبغي أن تؤخذ مزايا تدابير المراقبة التقنية في الحسبان، ولا سيما أنها توفر إجراءات الحماية بصورة مستمرة وتلقائياً.

(ب) تدابير المراقبة المادية: وهي الحواجز المادية الموضوعة لحماية الأصول الرقمية الحساسة من الأضرار المادية والوصول المادي غير المأذون به. وتشمل تدابير المراقبة المادية أفراد الحراسة والحواجز مثل الأقفال والأسوار والبوابات والأغلفة المادية وأجهزة اكتشاف التلاعب وغرف العزل.

(ج) تدابير المراقبة الإدارية: وهي السياسات والإجراءات والممارسات المصممة لحماية الأصول الرقمية الحساسة عن طريق مراقبة تصرفات الموظفين وسلوكهم. وتشمل تدابير المراقبة الإدارية تدابير تشغيلية وأخرى متعلقة بالشؤون الإدارية، وعادة ما تكون ذات طابع توجيهي، حيث تنص على ما ينبغي للموظفين والأفراد من الأطراف الثالثة عمله وما ينبغي لهم الامتناع عنه، ولكنها قد تشمل أيضاً تدابير ذات طابع تحفيزي، مثل التشجيع على إرساء ثقافة أمنية راسخة.

### اتباع نهج متدرج في تحديد تدابير الأمن الحاسوبي

19-7- ينبغي أن تستند تدابير الأمن الحاسوبي المشمولة ببرنامج الأمن الحاسوبي إلى نهج متدرج، بحيث تُطبّق التدابير الأمنية بالتناسب مع العواقب المحتملة للهجمات السيبرانية. ومن أوجه التنفيذ العملي للنهج المتدرج تجميع النظم الحاسوبية في نطاقات لأغراض الأمن النووي، مع تطبيق تدابير متدرجة للأمن الحاسوبي على كل نطاق. ومن النهج الشائعة في تطبيق تدابير الأمن الحاسوبي بأسلوب متدرج استعمال التصنيف إلى مستويات للأمن الحاسوبي (انظر الفقرات من 2-41 إلى 2-46).

20-7- وينبغي أن يتضمن برنامج الأمن الحاسوبي طريقة موثقة، مثل الطريقة المبينة في القسم 2، لتحديد مستوى الأمن الحاسوبي المناسب لكل أصل رقمي، بما في ذلك الأصول الرقمية الحساسة، إذا كانت السلطة المختصة بالأمن الحاسوبي تشترط ذلك. وعلى سبيل المثال، فقد تكون بعض السلطات المختصة أو الجهات المشغلة ملزمة بتنفيذ تدابير للأمن الحاسوبي بمقتضى نهج أمر، بدلاً من أن تحدد بنفسها متطلبات المستويات الأمنية للنظم الحاسوبية والأصول الرقمية الحساسة وغير الحساسة.

21-7- وينبغي أن تعتمد السلطة المختصة بالأمن الحاسوبي الطريقة المستخدمة في تحديد مستويات الأمن الحاسوبي.

## تصميم تدابير الأمن الحاسوبي

22-7- ينبغي أن يشجع برنامج الأمن الحاسوبي إدماج تدابير الأمن الحاسوبي، إلى أقصى درجة ممكنة، في تصميم النظم الحاسوبية. وعادة ما يكون تنفيذ تدابير الأمن الحاسوبي أيسر وأكثر فعالية بكثير عند إدماجها في التصميم بدلاً من إضافتها في وقت لاحق.

23-7- وينبغي أن تؤخذ متطلبات الأمن والأمان النوويين في الحسبان عند تصميم النظم الحاسوبية.

## الدفاع في العمق في سياق تدابير الأمن الحاسوبي

24-7- يُعتبر مفهوم الدفاع في العمق من المفاهيم الأساسية في مجال الأمن النووي. وينبغي أن يحدد برنامج الأمن الحاسوبي كيفية تطبيق الدفاع في العمق على تدابير الأمن الحاسوبي. ويمكن تحقيق ذلك بطرق مختلفة، ومنها ما يلي:

(أ) الأخذ بتدابير متنوعة ومستقلة للأمن الحاسوبي، واشتراط الاستقلالية في تصميمها وتشغيلها وصيانتها. وعلى سبيل المثال، سيكفل ذلك ألا تؤدي ثغرة واحدة في الأمن الحاسوبي إلى إتاحة الفرصة أمام أحد الخصوم ليتجاوز عدة طبقات من الدفاع في العمق بطريقة منهجية.

(ب) فصل مهام الموظفين أو الأفرقة من ذوي الامتيازات الخاصة في الوصول إلى الأصول الرقمية الحساسة. وينبغي أن يشمل ذلك النظر في فصل المهام المرتبطة بتصميم تدابير الأمن الحاسوبي وتنفيذها وإدارتها عن المهام المتعلقة بعمليات تشغيل المرفق أو النشاط المعني.

## إدارة شؤون البائعين والمتعاقدين والموردين

25-7- قد تستعين السلطات المختصة أو الجهات المشغلة ببائعين أو متعاقدين أو موردين لتوفير سلع أو خدمات تنطوي بالضرورة على وصول أولئك البائعين أو المتعاقدين أو الموردين إلى المعلومات الحساسة والأصول الرقمية الحساسة. وفي مثل هذه الحالات، ينبغي أن ينص الاتفاق القانوني بين الطرفين، مثل الترخيص أو عقد توفير السلع أو

الخدمات، على شروط مناسبة فيما يتعلق بالأمن الحاسوبي.

26-7- وعند صياغة التراخيص أو العقود من هذا القبيل، ينبغي أن تنظر السلطات المختصة والجهات المشغلة في إدراج أحكام تأخذ في الحسبان أن البائعين والمتعاقدين والموردين قد تكون بحوزتهم معلومات فريدة ومسجلة الملكية عن منتجاتهم أو خدماتهم (على سبيل المثال معلومات عن جوانب ضعف في مواجهة الهجمات السيبرانية قد تظهر بعد إنجاز العقد الأصلي) وأنهم قد يكونوا ملزمين بتقاسم هذه المعلومات مع السلطات المختصة والجهات المشغلة.

27-7- وينبغي أن تنص السلطات المختصة والجهات المشغلة في برامج الأمن الحاسوبي الخاصة بها على فرض متطلبات محددة متعلقة بالأمن الحاسوبي على البائعين والمتعاقدين والموردين. وقد يشمل ذلك متطلبات متعلقة بالأعمال المنفذة داخل الموقع وخارجه على السواء.

28-7- وينبغي للسلطات المختصة والجهات المشغلة أن تتأكد من أن البائعين والمتعاقدين والموردين ينفذون تدابير الأمن الحاسوبي اللازمة عند تطوير وتقديم منتجاتهم وخدماتهم.

29-7- ويمكن للسلطات المختصة والجهات المشغلة أن تنص في الاتفاقات التعاقدية على متطلبات معينة للأمن الحاسوبي. ويمكن أن تشمل هذه المتطلبات ما يلي:

- (أ) عدم الإفصاح عن المعلومات الحساسة وغيرها من المعلومات المحددة؛
- (ب) متطلبات حماية المعلومات الحساسة، بما في ذلك المتطلبات المتعلقة بالاحتفاظ بتلك المعلومات أو إتلافها؛
- (ج) القيود المفروضة على الوصول المسموح به للنظم الحاسوبية والأنشطة التي يمكن أداؤها عبر تلك النظم؛
- (د) الأنشطة المحظورة؛
- (هـ) العقوبات المفروضة على عدم الامتثال لمتطلبات الأمن الحاسوبي المنصوص عليها؛
- (و) القيود المفروضة على الوصول عن بعد؛
- (ز) متطلبات اختبار الخدمات والمنتجات المقدمة بموجب العقد.

30-7- ويمكن للسلطات المختصة والجهات المشغلة أن تنظر في إلزام البائعين والمتعاقدين والموردين بإثبات امتثالهم للمتطلبات التعاقدية المتعلقة بالأمن الحاسوبي.

31-7- وينبغي للسلطات المختصة والجهات المشغلة أن تُلزم البائعين والمتعاقدين والموردين بالإبلاغ عن أحداثات الأمن الحاسوبي على وجه السرعة، بما يشمل تحديد التهديدات وجوانب الضعف المحتملة التي يمكن أن تؤثر في الأمن النووي. وينبغي أن تكون الالتزامات والبروتوكولات المتعلقة بالإبلاغ جزءاً من العقد.

32-7- وقد تؤدي الاستعانة بالبائعين والمتعاقدين والموردين إلى نقل المخاطر أو تقاسمها. وقد يتطلب هذا النقل أو التقاسم أيضاً الحصول على موافقة الهيئة الرقابية المعنية بالأمن النووي أو السلطة المختصة بالأمن الحاسوبي. بيد أنه لا يمكن نقل المسؤولية عن الأمن النووي، بما يشمل الأمن الحاسوبي، إلى البائعين والمتعاقدين والموردين.

## 8- المحافظة على استدامة الأمن الحاسوبي

1-8- يصف هذا القسم العناصر والتدابير الموصى بالأخذ بها من أجل المحافظة على استدامة الأمن الحاسوبي في إطار منظومة الأمن النووي. وينبغي توثيق هذه العناصر والتدابير في برنامج الأمن الحاسوبي.

2-8- وينبغي أن تكون لدى السلطات المختصة والجهات المشغلة برامج مناسبة في مجال تنمية الموارد البشرية لضمان محافظتها على توافر الكفاءات ومستويات القدرة اللازمة لأداء المسؤوليات المسندة إليها فيما يتعلق بالأمن الحاسوبي.

3-8- وينبغي أن تكون لدى السلطات المختصة والجهات المشغلة إجراءات لتطبيق أفضل الممارسات والدروس المستفادة من التجارب [1]، ولا سيما من أحداثات الأمن الحاسوبي، وكذلك من السلطات المختصة والجهات المشغلة الأخرى والقطاعات الأخرى والمنظمات المكافئة في الدول الأخرى حيثما أمكن ذلك.

4-8- وينبغي للسلطات المختصة والجهات المشغلة أن تدرج الأمن الحاسوبي في برامج الاستدامة الخاصة بها، وأن تدعم ذلك بتوفير الموارد اللازمة. وينبغي أن تتناول برامج الاستدامة الجوانب ذات الصلة من الكفاءات ومستويات القدرات اللازمة لتطوير الأصول الرقمية الحساسة وغيرها من الأصول الرقمية ولتنفيذ تلك الأصول وصيانتها وإخراجها من الخدمة أو سحبها.

## ثقافة الأمن

5-8- يُعدُّ إرساء ثقافة راسخة في مجال الأمن النووي وتعزيز تلك الثقافة والحفاظ عليها أحد العناصر الأساسية في منظومة الأمن النووي [1]. وفيما يخصُّ الأمن الحاسوبي، غالباً ما تكون العناصر البشرية والعمليات هي العامل الرئيسي في توفير الأمن للنظم الحاسوبية، والخطأ البشري هو أحد أكبر العوامل مساهمة في حوادث الأمن الحاسوبي. وينبغي أن تؤدي ثقافة الأمن النووي إلى دعم الموظفين في التعرف على الحالات التي تتصرَّف فيها النظم الحاسوبية أو مستخدموها على نحو غير معتاد، وفي الإبلاغ عن تلك الحالات وعن الأخطاء البشرية التي يمكن أن تؤثر سلباً في الأمن الحاسوبي.

6-8- وينبغي تشجيع النظر إلى الأمن الحاسوبي بوصفه مكوناً أساسياً في ثقافة الأمن النووي من خلال التزامات صريحة من الإدارة العليا وعن طريق التوعية والتدريب. وينبغي أن يتضمن برنامج الأمن الحاسوبي أنشطة لتعزيز ثقافة الأمن النووي.

7-8- وفي إطار إرساء ثقافة فعالة في مجال الأمن النووي، ينبغي أن تتأكد جميع المنظمات من أنَّ موظفيها والمتعاقدين معها لديهم فهم كامل لمسؤولياتهم المتعلقة بالأمن الحاسوبي ولأهمية هذه المسؤوليات، لا سيما فيما يتعلق بالأمن والأمان النوويين. وينبغي أن يتلقى الموظفون والمتعاقدون التعليم والتدريب في مجال الأمن الحاسوبي بمستوى يتناسب مع الأدوار والمسؤوليات المسندة إليهم.

## التدريب

8-8- ينبغي أن تضع السلطات المختصة والجهات المشغلة برامج لتدريب جميع الموظفين والمتعاقدين على الأمن الحاسوبي وفقاً لمقتضيات الاستراتيجية، بهدف

تزويدهم بالكفاءات ومستويات القدرات المحددة لهم والمحافظة على استدامتها.

8-9- وينبغي أن تشمل برامج التدريب أنشطة للتوعية وتنمية الكفاءات والمهارات.

8-10- ويوصى بأن تشمل مواضيع التوعية والتدريب في مجال الأمن الحاسوبي ما يلي:

- (أ) التوعية بأنواع التهديدات السيبرانية وتقنيات الهجوم المرتبطة بها؛
- (ب) التوعية بالهندسة الاجتماعية وتوفير إرشادات بشأن مقاومتها؛
- (ج) التعرف على الهجمات السيبرانية والتصدي لها؛
- (د) مسؤوليات الأفراد المتعلقة بالأمن الحاسوبي والعقوبات المفروضة على عدم الامتثال؛
- (هـ) التأثير المحتمل للهجمات السيبرانية في الأمن والأمان النوويين؛
- (و) الممارسات الجيدة في مجال الأمن الحاسوبي؛
- (ز) استخدام الأجهزة المحمولة والوسائط القابلة للنقل؛
- (ح) استخدام وسائل التواصل الاجتماعي؛
- (ط) التغيرات التي تطرأ على التهديدات السيبرانية أو المخاطر من حيث مستواها أو طبيعتها.

8-11- وينبغي أن يكون الموظفون في مجالات الصيانة والعمليات التشغيلية والهندسة المسؤولون عن النظم النووية على وعي بالمخاطر المحدقة بكل من الأمن والأمان النوويين والمرتبطة بالهجمات السيبرانية التي يُحتمل أن تؤثر في عناصر الأجهزة والتحكم.

8-12- وينبغي أن يكون الموظفون في مجالات الصيانة والعمليات التشغيلية والهندسة المسؤولون عن نظم الحماية المادية على وعي بالآثار المحتملة للهجمات السيبرانية في وظائف نظم الحماية المادية.

8-13- وينبغي إبلاغ جميع الموظفين والمتعاقدين المعنيين في أقرب وقت ممكن عملياً بالتغيرات التي تطرأ على القواعد والإجراءات الأمنية.

8-14- وينبغي توفير التدريب على المهارات المتخصصة، بما يتناسب مع المهام المحددة لكل وظيفة، للموظفين والمتعاقدين المكلفين بمسؤوليات إدارية وتقنية متعلقة بالأمن

الحاسوبي (مثل موظفي دعم تكنولوجيا المعلومات، وموظفي الأجهزة والتحكم، ومسؤولي إدارة النظم الأمنية، وموظفي صيانة المعدات التقنية).

15-8- وينبغي أن تحدد البرامج التدريبية متطلبات التدريب المنطبقة على البائعين والمتعاقدين والموردين فيما يخص الأعمال المنفذة داخل الموقع وخارجه على السواء.

16-8- وينبغي أن يتلقى موظفو الإدارة العليا تدريبات وجلسات إحاطة دورية بشأن التهديدات السيبرانية وإدارة المخاطر.

17-8- وينبغي للسلطات المختصة والجهات المشغلة أن تستعرض برامج التدريب وتحديثها بانتظام لمراعاة الطابع الدينامي الذي يتسم به الأمن الحاسوبي، بما في ذلك التغيرات التي تطرأ على التهديدات السيبرانية وعلى التقنيات المستخدمة في الهجمات السيبرانية.

18-8- وينبغي للسلطات المختصة والجهات المشغلة أن تحدد المسؤولية عن برامج التدريب وأن تخصص الموارد الكافية لدعم هذه البرامج والمحافظة على استدامتها.

19-8- وينبغي الاحتفاظ بسجلات للتدريبات الرسمية التي يكملها جميع الموظفون والمتعاقدون.

20-8- وعادة ما يُجمع بين أنشطة التدريب والتوعية المتعلقة بأمن المعلومات والأمن الحاسوبي. ويقدم المرفق الثالث بالمرجع [8] نموذجاً لبرنامج للتوعية بأمن المعلومات، يمكن تكييفه بحيث يشمل أيضاً الأمن الحاسوبي.

## خطط الطوارئ والتصدي

21-8- ينبغي أن يؤثق برنامج الأمن الحاسوبي تدابير الأمن الحاسوبي المعمول بها للكشف عن أحداثات الأمن الحاسوبي والتصدي لها والتخفيف من عواقبها.

22-8- وينبغي أن يحدد برنامج الأمن الحاسوبي إجراءات التحليل والتصدي التي تُنفَّذ للوقوف على أسباب أحداثات الأمن الحاسوبي وأثارها المباشرة وتأثيرها المحتمل. وقد لا تكون هذه العناصر واضحة للعيان، بيد أنه يلزم تحديدها في أقرب وقت ممكن.

23-8- وعند تحليل أحداث الأمن الحاسوبي، ينبغي أن تشتمل عملية التحليل على النظر في إمكانية أن تكون الحادثة مقدمة أو نشاطاً استطلاعيًا لهجوم مقبل.

24-8- وينبغي أن يتضمن برنامج الأمن الحاسوبي خطط طوارئ بشأن التصدي للهجمات السيبرانية. وينبغي أن تأخذ هذه الخطط في الحسبان احتمالات وقوع هجمات من أطراف داخلية أو هجمات مختلطة. وينبغي أن تحدد خطة الطوارئ أنواع أحداث الأمن الحاسوبي وأن تبيّن الإجراءات اللازمة للتصدي لتلك الحوادث.

25-8- وفي الحالات التي تشكّل فيها حادثة الأمن الحاسوبي أيضاً حدثاً متصلاً بالأمن النووي، ينبغي تفعيل خطة الطوارئ ذات الصلة. وينبغي أن ينصّ برنامج الأمن الحاسوبي وخطة الطوارئ ذات الصلة على إجراءات فورية تُتخذ عندما يكون الأمن النووي معرضاً للخطر (وفي هذه الحالات يمكن أيضاً تفعيل خطط التصدي للكوارث، بيد أن هذه الخطط خارجة عن نطاق هذا المنشور).

26-8- وينبغي أن يتضمن برنامج الأمن الحاسوبي معايير الاستعانة بموارد إضافية والدور الذي تضطلع به تلك الموارد في التصدي لحوادث الأمن الحاسوبي.

27-8- وقد ينطوي تحليل أحداث الأمن الحاسوبي على تشكيل فريق شامل لعدة مجالات يتولى تحليل تأثير الحادثة في كلّ من الأمن والأمان النوويين.

## أنشطة توكيد الأمن الحاسوبي

28-8- وينبغي أن تكفل السلطات المختصة والجهات المشغلة اشتغال نظمها الإدارية على وسائل فعالة لتوفير توكيدات باستيفاء متطلبات الأمن الحاسوبي، بما في ذلك ضمن سلسلة الإمداد.

29-8- وينبغي للسلطات المختصة والجهات المشغلة (باستثناء السلطات والجهات التي لا تطبق في مجال الأمن الحاسوبي سوى تدابير مفروضة من الهيئة الرقابية أو السلطة المختصة بالأمن الحاسوبي) أن توفر توكيدات للسلطة المختصة بالأمن الحاسوبي بأنّ

الموارد المخصصة للأمن الحاسوبي كافية ومتناسبة مع مستوى التهديدات المحدد في تقييم التهديدات.

8-30- وينبغي أن تتأكد السلطات المختصة والجهات المشغلة من أن عمليات التفتيش والتقييم المنفذة للتحقق من الامتثال لمتطلبات الأمن النووي تشمل تقييم تدابير الأمن الحاسوبي.

## التذييل

### اعتبارات متعلقة بالترابط مع الأمان النووي لأغراض الأمان الحاسوبي في المرافق

ألف-1- إذا تعرّض أحد المرافق للتخريب، يمكن أن يؤدي ذلك إلى الإخلال بأمانه النووي أو بتوافر خدماته، وقد يكون ذلك بفعل هجوم سيبراني على النظم المهمة للأمان في المرفق والتي تستخدم النظم الحاسوبية أو تعتمد عليها أو تتلقى الدعم منها. ويمكن لهذه الهجمات أن تتسبب في تعطل هذه النظم المهمة للأمان أو اختلال تشغيلها بطرق لم تكن لتغدو ممكنة لو كانت تلك النظم في حالتها التشغيلية العادية أو في وضعية توقُّع الأعطال.

ألف-2- ويمكن للأعمال الشريرة أن تؤثر في نظام واحد (أو مفردة واحدة) أو أن تكون السبب وراء تصرف مجموعة متعددة من النظم (أو المفردات) بطريقة غير مرغوب فيها. وينبغي تصميم المرفق على نحو يكفل ألا تتسبب الأعمال الشريرة في تعطيل أو تجاوز مستويات متعددة من الأمان، وهو ما يُعرف بمبدأ الدفاع في العمق.

ألف-3- ويهدف الأمان الحاسوبي إلى التقليل من احتمالية تمكّن الخصوم من ارتكاب أعمال تخريبية عن طريق هجمات سيبرانية يمكن أن تخلّ بأمن المرفق أو أمانه أو توافر خدماته. ويسهم الأمان الحاسوبي في جميع مستويات الدفاع في العمق، كما هو مبين في المرجع [12]، ومن ثم يلزم تطبيقه على الوظائف والنظم والمعدات في جميع المستويات.

ألف-4- ويشتمل الترابط بين الأمان والأمن في مجال الأمان الحاسوبي على عدة عناصر مهمة لكل من الأمان النووي والأمان النووي. وتشمل هذه العناصر النظم والإجراءات والموظفين. وكثيراً ما تؤدي تدابير الأمان النووي أيضاً وظائف قيّمة للأمن النووي (والعكس)، وينبغي أن تؤخذ فرص الاستفادة من هذه الوظائف التكاملية في الحسبان عند وضع تدابير الأمان الحاسوبي.

ألف-5- ومن أمثلة تدابير الأمان التي يمكن أن تكون لها أيضاً فوائد أمنية وجود عنصر يكفل التحقق الآلي من صحة البيانات الواردة وأصالتها وسلامتها قبل استخدامها في وظيفة من وظائف الأمان. وقد تؤدي صيانة هذا العنصر أو تعديله إلى الإضرار بوظائف الأمان أو الوظائف الأمنية إذا لم يكن القائمون على أنشطة الصيانة أو التعديل على علم بتعدد وظائفه (حالات الاعتماد المتبادل). ولذلك ينبغي تضمين وثائق النظم والمكونات وصفاً لوظائف الأمان والوظائف الأمنية التي تؤديها العناصر من هذا القبيل.

ألف-6- ويمكن أيضاً أن تؤثر استراتيجية الأمان سلباً في الأمن (أو العكس). وعلى سبيل المثال، ففي كثير من الأحوال ينطوي التصميم لأغراض الأمان على توزيع الوظائف على مفردات أو نظم مختلفة من أجل عزل آثار الأعطال، وعلى مراعاة الوفرة الاحتياطية والتنوع في النظم بحيث لا تؤدي فرادي الأعطال إلى الإخلال بوظائف مهمة. وقد يؤدي اتباع هذه الاستراتيجية إلى زيادة عدد المفردات في النظام المهم للأمان، مما يزيد من تعقيد النظام ومن ثم من عدد الأهداف المحتملة للهجمات السيبرانية. ولذلك ينبغي النظر في تدابير الأمن والأمان على الدوام من أجل الوقوف على أي حالات تعارض وتسويتها.

ألف-7- وتتوقف ملاءمة أي تدبير من تدابير الأمن الحاسوبي على اعتبارات تتعلق بكل من الأمن والأمان، ولذلك يتطلب تصميم هذه التدابير توافر خبرات في كلا المجالين. ومن شأن تدابير الأمن الحاسوبي أن تشمل تدابير تقنية ومادية وإدارية، ويتعين أن تعمل كل هذه التدابير معاً. وقد يستلزم هذا النهج، على سبيل المثال، تنفيذ بعض وظائف الأمن (مثل جمع سجلات المراجعة وتوليد الإنذارات الأمنية) عن طريق نظم يمكنها رصد نظم الأجهزة والتحكم دون التأثير فيها، أو قصر عمليات الفحص الأمني النشاط على الأوقات التي تكون فيها نظم الأجهزة والتحكم غير موصلة. وقد يُسمح ببعض الاستثناءات من هذا النهج، لكن سيلزم تحليل تلك الاستثناءات وتبريرها في كل حالة على حدة.

ألف-8- ومن المرجح أن يكون مستوى المخاطر المقبول في المرفق واحداً سواء كان العامل المتسبب في المخاطر حدثاً متصلاً بالأمان أو بالأمن. ويمكن تلخيص النهج الشائعة لتحقيق ذلك على النحو التالي:

(أ) تطبيق مفهوم الدفاع في العمق (أي استخدام طبقات متعددة من الحماية) في مجالي الأمان والأمن على السواء.

- (ب) النظر في منع وقوع الأحداث البادئة، والكشف المبكر عن أي أوضاع غير عادية، والتصدي الفوري لتلافي تصعيد الموقف.
- (ج) إدماج التخطيط للتخفيف من العواقب في التصميم، في حال فشل الخطوة السابقة.
- (د) وجود خطط موسّعة لمواجهة الطوارئ من أجل معالجة الحالات التي يفشل فيها المنع والكشف والتخفيف من العواقب.

ألف-9- وتتطلب العلاقة بين الأمن الحاسوبي والأمان التنسيق الفعال، مثلاً في سياق تصنيف الأصول وإدارتها بمراعاة اعتبارات الأمن والأمان. ومما قد يزيد ذلك تعقيداً الاعتماد المتزايد على البرمجيات والشبكات في النظم الحاسوبية ومن ثم اتسامها بطابع التغيّر السريع، وهو ما يعني أنّ تدابير الأمن الحاسوبي تخضع بدورها للتغيّر السريع في تصميمها وتشغيلها. وي طرح هذا الأمر تحدياً في الحالات التي تعتمد فيها عمليات تحليل الأمان على التوصل إلى تنبؤات دقيقة بشأن السلوك الحتمي في المستقبل. وقد يزداد هذا التحليل تعقيداً بفعل عدم التيقّن من فعالية تدابير الأمن الحاسوبي، وهو ما يعني أن التحليل قد لا يوفر تنبؤات دقيقة بسلوك النظم في المستقبل في حال وقوع أحداث بادئة (على سبيل المثال في حال استهدافها بهجمات سيبرانية).

ألف-10- ومن المرجح أنّ تطبيق تدابير الأمن الحاسوبي على النظم القائمة سوف يستلزم استعراض تحليل الأمان القائم. وتنطوي تدابير الأمن الحاسوبي المتكاملة عموماً على إمكانية تقييد سلوك النظم المهمة للأمان أو تغييره بطريقة أخرى إذا ما قورنت بالتدابير المنفصلة أو القائمة بذاتها.



## المراجع

- [1] الوكالة الدولية للطاقة الذرية، الهدف والعناصر الأساسية لمنظومة الأمن النووي الخاصة بالدولة، العدد 20 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2014).
- [2] اتفاقية الحماية المادية للمواد النووية، INFCIRC/274/Rev.1، الوكالة الدولية للطاقة الذرية، فيينا (2021)؛ تعديل اتفاقية الحماية المادية للمواد النووية، INFCIRC/274/Rev.1/Mod.1، الوكالة الدولية للطاقة الذرية، فيينا (2016).
- [3] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن الحماية المادية للمواد النووية والمرافق النووية (INFCIRC/225/Revision 5) العدد 13 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2011).
- [4] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن المواد المشعة والمرافق ذات الصلة، العدد 14 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2011).
- [5] مكتب الشرطة الأوروبي (اليوروبول)، والوكالة الدولية للطاقة الذرية، ومنظمة الطيران المدني الدولي (إيكاو)، والمنظمة الدولية للشرطة الجنائية (الإنتربول)، ومعهد الأمم المتحدة الأقليمي لبحوث الجريمة والعدالة، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، ومنظمة الجمارك العالمية، توصيات الأمن النووي بشأن المواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي، العدد 15 من سلسلة الوكالة للأمن النووي، الوكالة الدولية للطاقة الذرية، فيينا (2012).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (in preparation).
- [8] الوكالة الدولية للطاقة الذرية، أمن المعلومات النووية، العدد 23-G من سلسلة منشورات الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2016).
- [9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2008, ISO, Geneva (2018).
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).
- [11] الوكالة الدولية للطاقة الذرية، ثقافة الأمن النووي، العدد 7 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2011).
- [12] الوكالة الدولية للطاقة الذرية، أمان محطات القوى النووية: التصميم، العدد SSR-2/1 (الصيغة المنقحة Rev.1) من سلسلة معايير الأمان الصادرة عن الوكالة الدولية للطاقة الذرية، الوكالة الدولية للطاقة الذرية، فيينا (2016).



## المرفق الأول

### إرشادات في شكل توصيات مقترحة بشأن الأمن الحاسوبي لأغراض منظومة الأمن النووي الوطنية

أولاً-1- شارك في وضع "عناصر منظومة الأمن النووي الخاصة بالدولة لأغراض الأمن الحاسوبي" الواردة في هذا المرفق خبراء من أكثر من 20 دولة عضواً، والغرض منها هو تقديم إرشادات مكملّة لمنشورات التوصيات التي أصدرتها الوكالة في سلسلة الأمن النووي [أولاً-1 إلى أولاً-3]، وذلك في شكل توصيات مقترحة بشأن تصميم الأمن الحاسوبي وتنفيذه والمحافظة على استدامته في إطار منظومة الأمن النووي الخاصة بالدولة. وللدول أن تختار معاملة هذا النص باعتباره يقدّم إرشادات في شكل توصيات. والإرشادات التنفيذية الواردة في متن هذا المنشور متوافقة مع الإرشادات المقدمة في شكل توصيات في هذا المرفق.

#### الخلفية

أولاً-2- الغرض من منشورات التوصيات الصادرة عن الوكالة ضمن سلسلة الأمن النووي [أولاً-1 إلى أولاً-3] هو توفير إرشادات للدول وسلطاتها المختصة بشأن كيفية إرساء منظومة وطنية فعالة في مجال الأمن النووي، وكيفية تحسين هذه المنظومة وتنفيذ عناصرها والمحافظة عليها، وذلك بغرض توفير الأمن لكلّ مما يلي، على التوالي: المواد النووية والمرافق النووية، والمواد المشعة والمرافق المرتبطة بها، والمواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي.

أولاً-3- وتعرض منشورات التوصيات ممارسات جيدة ينبغي أن تعتمد عليها الدول الأعضاء عند تطبيق أساسيات الأمن النووي [أولاً-4]. وتنصّ هذه الأساسيات على مسؤولية الدول عن كفالة الحماية للمعلومات الحساسة وأصول المعلومات الحساسة من تهديدات الأمن النووي.

أولاً-4- وقد تسعى الأطراف التي تشكّل تهديدات للأمن النووي إلى استهداف المعلومات الحساسة وأصول المعلومات الحساسة للإخلال بأداء وظائف نظم الأمن النووي أو الأمان النووي. ويمكن أن يكون الهجوم عملاً منعزلاً أو أن يكون جزءاً من هجوم مختلط على أحد المرافق أو إحدى المنظمات، بحيث يشتمل على عناصر هجوم السيبراني وهجوم مادي في الوقت نفسه، بهدف الوصول غير المأذون به إلى المواد. ولذلك يُعدّ الأمن الحاسوبي مكوناً أصيلاً من مكونات منظومة الأمن النووي الخاصة بالدولة وعاملاً ضرورياً لتحقيق مقاصدها.

أولاً-5- والأصول الرقمية الحساسة هي أصول المعلومات الحساسة المؤلفة من نظم حاسوبية، والتي يمكن أن يؤدي الإخلال بها إلى آثار سلبية في الأمن النووي. ولذلك تتطلب الأصول الرقمية الحساسة تطبيق تدابير للأمن الحاسوبي.

أولاً-6- وتهدف تدابير الأمن الحاسوبي إلى المحافظة على سرية المعلومات الحساسة الموجودة في الأصول الرقمية الحساسة وسرية الأصول الرقمية الحساسة نفسها، وعلى سلامة تلك المعلومات والأصول وتوافرها.

أولاً-7- ولا توفّر منشورات التوصيات بصيغتها الحالية إرشادات كافية بشأن تدابير الأمن الحاسوبي اللازمة لحماية الأصول الرقمية الحساسة.

## الغرض

أولاً-8- يقدّم هذا المرفق إرشادات مقترحة في مجال الأمن الحاسوبي فيما يتعلق بتنفيذ العناصر الجوهرية لأساسيات الأمن النووي [أولاً-4] في الحالات التي لم تُعالج بما فيه الكفاية في منشورات التوصيات [أولاً-1 إلى أولاً-3]. ولا يُقصد بهذه الإرشادات تغيير التوصيات القائمة بأي شكل من الأشكال.

أولاً-9- والغرض من هذا المرفق هو أن تستخدمه الدول والسلطات المختصة والجهات المشغلة<sup>1</sup> والموردون والبائعون والمتعاقدون والمهنيون العاملون في مجال الأمن النووي والأمان النووي.

---

<sup>1</sup> يُقصد بـ"الجهات المشغلة" في هذا السياق الجهات المرخص لها والجهات الشاحنة والناقلة.

## النطاق

أولا-10- تنطبق هذه الإرشادات على جوانب الأمن النووي المتعلقة بالأمن الحاسوبي.

أولا-11- وتتناول هذه الإرشادات الأمن الحاسوبي من حيث جوانبه العامة المنطبقة على جميع مجالات الأمن النووي، بما في ذلك الجوانب المتعلقة بالمواد النووية والمرافق النووية [أولا-1]، والمواد المشعة الأخرى والمرافق المرتبطة بها [أولا-2]، والمواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي [أولا-3]. وينبغي تطبيق هذه الإرشادات باتباع نهج متدرج.

عناصر منظومة الأمن النووي الخاصة بالدولة لأغراض الأمن الحاسوبي

### مسؤولية الدولة

أولا-12- ينبغي أن تضع الدولة استراتيجية للأمن الحاسوبي<sup>2</sup> تدعم منظومة الأمن النووي الخاصة بها.

### إسناد المسؤوليات المتعلقة بالأمن الحاسوبي

أولا-13- ينبغي أن تعيّن الدولة سلطات مختصة وتمنحها الصلاحيات اللازمة لتتولى المسؤولية عن وضع وتنفيذ الإطار التشريعي والرقابي الذي ينظم الأمن الحاسوبي لأغراض منظومة الأمن النووي. وقد تكون السلطة المختصة بالأمن الحاسوبي غير السلطة المختصة (أو السلطات المختصة) بسائر جوانب الأمن النووي.

أولا-14- وينبغي أن تكفل الدولة تعريف الوظائف والأدوار وسائر الترتيبات المتعلقة بالأمن الحاسوبي وتنسيقها تنسيقاً وثيقاً فيما بين جميع السلطات المختصة المعنية بالأمن النووي وداخل تلك السلطات.

---

<sup>2</sup> يمكن أن تكون هذه الاستراتيجية مخصصة لمنظومة الأمن النووي وحدها أو أن تكون ذات نطاق أكثر عمومية، كأن تنطبق مثلاً على حماية البنى الأساسية الحساسة. وقد تستخدم بعض الدول تعبير "سياسة" بدلاً من "استراتيجية" في هذا السياق.

## الإطار التشريعي والرقابي

أولاً-15- ينبغي أن تكفل الدولة أن يشتمل الإطار التشريعي والرقابي على متطلبات للأمن النووي بشأن منع ارتكاب أعمال غير مآذون بها ضد النظم الحاسوبية بما من شأنه التأثير سلباً في الأمن النووي، والكشف عن هذه الأعمال والتصدي لها في حال ارتكابها. وينبغي استخدام هذه المتطلبات في إعداد تقييم التهديدات الخاص بالدولة.

أولاً-16- وينبغي أن تُنشئ الدولة عملية للتفتيش والإنفاذ من أجل التحقق من الامتثال لمتطلبات الأمن الحاسوبي المنصوص عليها في إطارها التشريعي والرقابي.

أولاً-17- وينبغي أن تكفل الدولة أن ينصّ إطارها التشريعي والرقابي على فرض عقوبات على ارتكاب أعمال غير مآذون بها ضد النظم الحاسوبية بما من شأنه التأثير سلباً في الأمن النووي.

## السلطات المختصة

أولاً-18- ينبغي أن تتأكد السلطات المختصة من أن الجهات المشغلة تنفذ سياسة الأمن الحاسوبي وتضع وتنفذ برامج الأمن الحاسوبي المرتبطة بها وفقاً لمتطلبات الأمن الحاسوبي الوطنية.

أولاً-19- وينبغي أن تكفل السلطات المختصة أن يكون الأمن الحاسوبي جزءاً من عمليات التقييم والترخيص وغيرها من إجراءات منح الأذون.

أولاً-20- وينبغي أن تتحقق السلطات المختصة من امتثال الجهة المشغلة المستمر لمتطلبات الأمن الحاسوبي من خلال الاضطلاع بعمليات تفتيش منتظمة، والاستعانة عند الاقتضاء بتدابير الإنفاذ لضمان اتخاذ الإجراءات التصحيحية اللازمة.

## مسؤولية الجهات المشغلة

أولاً-21- ينبغي للجهات المشغلة أن تحدد الأصول الرقمية الحساسة وتصنفها بناءً على العواقب المحتملة للإخلال بها من حيث التأثير في الأمن النووي.

أولا-22- وينبغي للجهات المشغلة أن تضع التدابير المناسبة في مجال الأمن الحاسوبي<sup>3</sup> وأن تتأكد من تنفيذ هذه التدابير لحماية الأصول الرقمية الحساسة من الإخلال بها طوال دورة حياتها (إلى أقصى درجة ممكنة) وفقاً لمفهوم النهج المتدرج والدفاع في العمق.

أولا-23- وينبغي للجهات المشغلة أن تطبق الأمن الحاسوبي باعتباره أحد مبادئ تصميم واستخدام الأصول الرقمية الحساسة، بما يشمل الحماية من الوصول غير المأذون به (جانب أي أشخاص أو عمليات أو أجهزة) ومن البرامجيات الخبيثة.

أولا-24- وينبغي للجهات المشغلة أن تقيّم وتدير تدابير الأمن الحاسوبي بحيث لا تؤثر سلباً في أنشطة الحماية المادية والأمان النووي وحصر المواد النووية ومراقبتها.

أولا-25- وينبغي أن تضطلع الجهات المشغلة بأنشطة توكيدية للتحقق من امتثال تدابير الأمن الحاسوبي المعمول بها لديها لمتطلبات الأمن الحاسوبي.

أولا-26- وينبغي أن تتأكد الجهات المشغلة من إدماج تدابير الأمن الحاسوبي في ترتيبات إدارة سلسلة الإمداد الخاصة بها، بهدف التقليل إلى أدنى حد من جوانب الضعف في النظم الحاسوبية ومنع استغلال سلسلة الإمداد كمسار لتنفيذ هجمات سيبرانية.

أولا-27- وينبغي للمنظمات التابعة للدولة، بما فيها السلطات المختصة، أن تأخذ بالتوصيات الواردة في الفقرات من أولا-21 إلى أولا-26 عند توفير الحماية للأصول الرقمية الحساسة التي تكون تلك المنظمات مسؤولة عنها.

### التعاون والمساعدة على الصعيد الدولي

أولا-28- وينبغي لأنشطة التعاون والمساعدة على الصعيد الدولي أن تشمل اعتبارات الأمن الحاسوبي ذات الصلة بالأمن النووي.

---

<sup>3</sup> يمكن للتدابير الأمنية أن تشمل تدابير مراقبة مادية وتقنية وإدارية.

## تحديد التهديدات وتقييمها

أولا-29- ينبغي لتقييم التهديدات<sup>4</sup> الخاص بالدولة (ووصف التهديدات المحتاط لها في التصميم، إن وُجد) أن يأخذ في الحسبان إمكانية استخدام الخصوم المحتملين للقدرات الحاسوبية، بما في ذلك إمكانية تنفيذ أنشطة من قبل أطراف داخلية وإمكانية وقوع هجمات مختلطة. وينبغي استعراض تقييم التهديدات وتحديثه لمواكبة التغيرات التي تطرأ على التهديدات السيبرانية، وينبغي الإبلاغ به بطريقة ملائمة وفي الوقت المناسب.

أولا-30- وفي الأحوال التي يكون فيها وصف التهديدات المحتاط لها في التصميم أو تقييم التهديدات فيما يخص الهجمات السيبرانية منفصلاً عن وصف التهديدات المحتاط لها في التصميم أو تقييم التهديدات فيما يخص الهجمات المادية، ينبغي أن تكفل الدولة إعداد تقييم التهديدات (ووصف التهديدات المحتاط لها في التصميم، إن وُجد) في الحالتين بمراعاة التنسيق بينهما.

## الترابط بين الأمان والأمن

أولا-31- ينبغي إدارة الترابط بين الأمان والأمن، بما في ذلك الأمن الحاسوبي، بطريقة تكفل ألا يؤثر أحد المجالين سلباً في الآخر، بل أن يدعم كل منهما الآخر قدر الإمكان.

## المحافظة على استدامة الأمن الحاسوبي

أولا-32- ينبغي تناول الأمن الحاسوبي بطريقة متكاملة ومنسقة داخل النظام الإداري لكل سلطة مختصة وجهة مشغلة.

أولا-33- وينبغي تشجيع النظر إلى الأمن الحاسوبي بوصفه مكوناً أساسياً في ثقافة الأمن النووي.

أولا-34- وينبغي أن يشكّل الأمن الحاسوبي جزءاً من برامج الاستدامة لدى السلطات المختصة والجهات المشغلة، مع دعمه بتخصيص الموارد الكافية.

---

<sup>4</sup> قد يُشار إليه باسم "تقييم التهديدات الوطني".

## التخطيط والتأهب والتصدي لحادثات الأمن الحاسوبي

أولا-35- ينبغي أن تتأكد الدولة من أنَّ السلطات المختصة والجهات المشغلة وسائر الأطراف المعنية لديها خطط الطوارئ والقدرات اللازمة للتصدي على نحو ملائم لحادثات الأمن الحاسوبي التي يمكن أن تؤثر سلباً في الأمن النووي.

أولا-36- وينبغي أن تتأكد الدولة من أنَّ السلطات المختصة والجهات المشغلة وسائر الأطراف المعنية تعقد تمارين منتظمة لتقييم الجوانب المتعلقة بالأمن الحاسوبي في خطط التصدي والتحقق منها.

أولا-37- وينبغي لمنظومة الأمن النووي الخاصة بالدولة أن تشمل متطلبات بشأن إبلاغ السلطة (أو السلطات) المختصة في الوقت المناسب عن حادثات الأمن الحاسوبي.

## مراجع المرفق الأول

[أولا-1] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن الحماية المادية للمواد النووية والمرافق النووية (INFCIRC/225/Revision 5) العدد 13 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2011).

[أولا-2] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن المواد المشعة والمرافق ذات الصلة، العدد 14 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2011).

[أولا-3] مكتب الشرطة الأوروبي (اليوروبول)، والوكالة الدولية للطاقة الذرية، ومنظمة الطيران المدني الدولي (إيكاو)، والمنظمة الدولية للشرطة الجنائية (الإنترپول)، ومعهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، ومنظمة الجمارك العالمية، توصيات الأمن النووي بشأن المواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي، العدد 15 من سلسلة الوكالة للأمن النووي، الوكالة الدولية للطاقة الذرية، فيينا (2012).

[أولا-4] الوكالة الدولية للطاقة الذرية، الهدف والعناصر الأساسية لمنظومة الأمن النووي الخاصة بالدولة، العدد 20 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2014).

## المرفق الثاني

### أنماط التهديدات السيبرانية

ثانيا-1- يُعدُّ فهم التهديدات السيبرانية عنصراً مهماً في وضع تدابير الحماية وتنفيذها. وتختلف التهديدات السيبرانية عن التهديدات المادية للمواد النووية والمواد المشعة الأخرى والمرافق والعمليات المرتبطة بها. فالتهديدات السيبرانية لا تتطلب عدداً معيناً من المهاجمين ولا تتقيد بعامل القرب من مكان المرفق المستهدف ولا بحدوده. ويتيح فهم خصائص التهديدات السيبرانية وسيناريوهات الهجمات الممكنة منظوراً قيماً للتفكير في تدابير المنع وتدابير التصدي على السواء. والخصوم وأدواتهم وتكتيكاتهم وأهدافهم عناصر ديناميكية، ولذلك يلزم بذل العناية الواجبة عند تقييم التهديدات الحالية.

ثانيا-2- وتشمل الاتجاهات السائدة ما يلي [ثانيا-1، ثانيا-2]:

- (أ) تزايد عدد الخصوم الذين لديهم القدرة على تنفيذ هجمات سيبرانية؛
- (ب) تزايد عدد الأفراد أو الجماعات الذين يعرضون "الجريمة السيبرانية على أنها خدمة"، ومن ثم تيسير دخول هذا المعترك على الخصوم الذين كانوا يفتقرون في السابق إلى المهارات اللازمة؛
- (ج) تزايد مستوى التعقيد الذي تنطوي عليه التقنيات المستخدمة في الهجمات السيبرانية، مما يزيد من صعوبة الكشف والتصدي؛
- (د) استمرار استخدام الهندسة الاجتماعية في الهجمات السيبرانية، بما في ذلك تقنيات "التصيد الموجه" و"نصب الشرك عند البئر"؛
- (هـ) تركيز الخصوم بصورة متزايدة على العثور على جوانب الضعف في نظم التحكم الصناعي واستغلالها؛
- (و) انتشار برامجيات الابتزاز؛
- (ز) الصعوبة المستمرة في توفير الأمن لسلسلة الإمداد في مواجهة الهجمات السيبرانية.

ثانيا-3- وكحدٍّ أدنى، يجب على السلطة المختصة بتقييم التهديدات السيبرانية والسلطة المختصة بالأمن الحاسوبي والجهات المشغلة المشاركة في عملية تقييم التهديدات أن تنظر في السمات والخصائص الوارد وصفها في القسم التالي فيما يخص كل طرف داخلي

وخارجي يُعتبر أنه يشكل تهديداً. ويُعدُّ تحديد خصائص التهديدات السيبرانية أمراً صعباً بالنظر إلى التحدي الذي يطرحه الوقوف على هوية المهاجمين وإمكانية وقوع هجمات لا تُعرف هوية منفذها. بيد أنَّ استنباط أنماط للتهديدات يمكن أن يكون مفيداً.

## سمات وخصائص التهديدات السيبرانية

ثانياً-4- قد يكون من المفيد استخدام الفئات التالية من سمات وخصائص التهديدات السيبرانية في استنباط أنماط لتلك التهديدات:

- (أ) الدوافع: سياسية أو مالية أو أيديولوجية أو شخصية.
- (ب) النوايا: تخريب مواد مشعة أو مرفق إشعاعي، سرقة مواد مشعة أو مواد نووية، التسبُّب في حالة من الذعر العام والاضطرابات الاجتماعية، إثارة قلق سياسي، التسبُّب في إصابات وخسائر جماعية جسيمة، سرقة معلومات حساسة.
- (ج) المهارات ذات الصلة (القدرات): مهارات متعلقة باستخدام الحواسيب ونظم التحكم المؤتمتة لتوفير دعم مباشر لهجمات مادية أو جمع المعلومات الاستخبارية أو تنفيذ هجمات حاسوبية أو كسب الأموال.
- (د) المعارف: العناصر المستهدفة، خطط الموقع والإجراءات المعمول بها فيه، التدابير الأمنية، تدابير الأمان وإجراءات الوقاية من الإشعاعات، العمليات، إمكانية استخدام المواد النووية أو مواد مشعة أخرى.
- (هـ) التمويل: مصدره ومقداره وتوافره.
- (و) التكتيكات: استخدام التخفي أو الخداع أو القوة.

## الوصف الأساسي للتهديدات السيبرانية

ثانياً-5- هناك طرق عديدة لتصنيف التهديدات. والغرض من الفئات الواردة فيما يلي هو تقديمها كأمثلة للتصنيف (وقد تتداخل بعض الفئات).

ثانياً-6- الطرف الداخلي الذي يشكل تهديداً تُعدُّ الهجمات التي تنفذها أطراف داخلية من أكثر أنواع الهجمات صعوبة في الدفاع ضدها. و"الطرف الداخلي" هو فرد مأذون له بالوصول إلى المرافق ذات الصلة أو الأنشطة ذات الصلة أو إلى المعلومات الحساسة

أو أصول المعلومات الحساسة، ويمكنه ارتكاب أو تسهيل ارتكاب "أفعال إجرامية أو أفعال متعمدة غير مأذون بها تتعلق بمواد نووية أو مواد مشعة أخرى أو مرافق ذات صلة أو أنشطة ذات صلة، أو أفعال موجهة نحو هذه المواد أو المرافق أو الأنشطة، أو أي أفعال أخرى تقرر الدولة أنها تؤثر سلباً في الأمن النووي" [ثانياً-3]. والطرف الداخلي هو شخص موثوق فيه ومدرب على النظم الداخلية، ولسبب ما يستخدم حقوقه في الوصول ومعارفه بطريقة تخل بالأمّن وربما لغرض شرير. وتتفاوت الأسباب المحددة وراء أنشطة الأطراف الداخلية تفاوتاً كبيراً، وتشمل هذه الفئة أنماطاً مختلفة من الأشخاص، من الموظفين الساخطين إلى العملاء السريين. وهناك حالة خاصة هي الأطراف الداخلية الغافلة. والطرف الداخلي الغافل هو طرف داخلي ليست لديه النية ولا الدافع لارتكاب عمل شرير، وإنما يستغله الخصم دون أن يدري [ثانياً-3].

ثانياً-7- المتطرفون: يشير مفهوم التطرف إلى الجماعات التي تتجاوز الأساليب المتعارف عليها للتعبير عن آرائها السياسية والاجتماعية (أي أنّ التطرف هو النشاط السياسي أو الاجتماعي الذي يتجاوز حدود السلوك المقبول). وقد يعتمد المتطرفون إلى تنفيذ عمل واحد أو ينسقون جهودهم بطريقة غير محكمة مع أشخاص من ذوي التوجهات المشابهة من أجل تنفيذ هجمات سيبرانية ضد هدف معين. وقد لا تكون هذه التجمعات خاضعة لسيطرة شخصية قيادية مركزية وقد لا تعمل وفقاً لقواعد اشتباك محددة.

ثانياً-8- القراصنة الهواة: القراصنة الهواة هم أفراد أو جماعات تتعلق دوافعهم بتحقيق الشهرة أو المكانة لا بالإيذاء أو المكاسب المالية. وقد يتسبب القراصنة الهواة في أضرار أمنية دون استهداف هدف معين (أي دون أن يكون المرفق النووي هو هدفهم المحدد؛ لكن هذه الأضرار قد تنشأ بسبب بيئة عدوانية. فعلى سبيل المثال، يمكن أن يُصاب أحد أنظمة التحكم في مرفق نووي بفيروس شائع بسبب عدم الالتزام بالإدارة الآمنة للأجهزة المحمولة والوسائط القابلة للنقل.

ثانياً-9- الجريمة المنظمة: نجحت الجريمة المنظمة في الإعداد لهجمات سيبرانية موجهة ومتطورة للغاية ضد قطاعات صناعية متعددة. والغرض من هذه الهجمات هو تحقيق مكاسب مالية، إما مباشرة عن طريق سرقة الأموال أو بطريقة غير مباشرة عن طريق بيع البيانات المسروقة أو بيع معلومات بشأن خلل أمني إلى أطراف تشكّل تهديداً من نوع آخر.

ثانياً-10- الدول القومية: الدول القومية هي غالباً مصدر تهديد عالي القدرة وشديد المثابرة. وعادة ما تقتصر دوافع الهجمات التي تنفذها الدول على جمع المعلومات، وكثيراً ما تكون مقيّدة بقواعد اشتباك منهجية.

ثانياً-11- الإرهابيون: تشير التجارب السابقة إلى أنّ الهجمات السيبرانية التي نُسب ارتكابها لإرهابيين كانت في معظمها نتاج جهود غير متطورة مثل "إغراق البريد الإلكتروني" للأعداء الأيديولوجيين أو الهجمات الرامية إلى حجب الخدمات أو تشويه مواقع الإنترنت، بيد أنّه من المحتمل أنّ هناك إرهابيون يكتسبون كفاءة تقنية متزايدة لتنفيذ هجمات على مستوى الشبكات. وقد تُستمد هذه الكفاءة التقنية من خبرات داخلية أو عن طريق الاستعانة بقرصنة مرتزقة [أولاً-4]. وقد يحاول الإرهابيون استهداف وتخريب البنى الأساسية الحساسة مثل محطات القوى النووية، لكن تركيزهم قد ينصبّ أيضاً على الحصول على مواد نووية أو مواد مشعة أخرى.

### خصائص الهجمات

ثانياً-12- من المهم أيضاً فهم خصائص الهجمات حتى يتسنى وضع تدابير الردع والمنع والكشف والتخفيف من العواقب والتصدي. ويرد في الأقسام التالية وصف عدة أنواع من الهجمات (والانتماء إلى إحدى الفئات لا يستبعد الانتماء إلى فئة أخرى في الوقت نفسه).

### الهجمات غير الموجهة لهدف بعينه

ثانياً-13- من بين الأطراف التي تشكّل تهديداً الوارد وصفها أعلاه، هناك العديد من الأطراف التي يُرجح أن تسعى إلى تنفيذ هجمات موجهة ضد أهداف معينة متصلة بالأمن النووي. ومع ذلك، قد تقع أيضاً هجمات غير موجهة لهدف بعينه، فعلى سبيل المثال يمكن إدخال شفرة خبيثة غير موجهة إلى النظم والشبكات الحاسوبية دون قصد ويترتب على ذلك تأثير سلبي في الأمن النووي. ومن أمثلة ذلك أن يُصاب أحد أنظمة التحكم في مرفق نووي بفيروس شائع بسبب عدم الالتزام بالإدارة الآمنة للوسائط النقالة.

## الهجمات المتواصلة

ثانياً-14- قد يستهدف الهجوم السيبراني إحداث أثر فوري أو قد يشكّل جزءاً من حملة متواصلة ضد مرفق أو منظمة. وقد يبدأ الهجوم المتواصل بالإخلال بأمن أحد النظم الحاسوبية ثم يعقب ذلك حملة مطولة من جمع المعلومات. وقد ينجم عن ذلك حدث مؤثر، أو قد يقتصر هدف الهجوم على إرساء موطئ قدم لتنفيذ أنشطة أخرى في المستقبل.

## الهجمات المختلطة

ثانياً-15- الهجوم المختلط هو عمل منسق يجمع بين الهجوم السيبراني وعمل مادي. وعلى سبيل المثال، يمكن الإخلال بأحد أنظمة التحكم في الوصول المادي للسماح بدخول أفراد غير مأذون لهم إلى مكان فعلي.

## جدول أنماط التهديدات

ثانياً-16- يعرض الجدولان ثانياً-1 و ثانياً-2 وصفاً لمجموعة من أنماط المهاجمين المحتملين. ويركز الجدول ثانياً-1 على التهديدات الداخلية (انظر أيضاً المرجع [ثانياً-3])، في حين يبيّن الجدول ثانياً-2 بعض التهديدات الخارجية الممكنة. ويعرض الجدولان أنماطاً عامة من المهاجمين وعدداً من الخصائص المرتبطة بتلك الأنماط، وهي الموارد المتوفرة لدى المهاجمين، والوقت المتاح لتنفيذ الهجوم، والأدوات التي يُرجّح استخدامها في الهجوم، ودوافع المهاجمين. ويجب تكييف وصف هذه الأنماط بحسب الظروف القائمة في أي حالة معينة.

## مراجع المرفق الثاني

- [II-1] AUSTRALIAN CYBER SECURITY CENTRE, ACSC 2015 Threat Report (2015), [www.cyber.gov.au/sites/default/files/2020-04/ACSC\\_Threat\\_Report\\_2015.pdf](http://www.cyber.gov.au/sites/default/files/2020-04/ACSC_Threat_Report_2015.pdf)
- [II-2] GEORGIA INSTITUTE OF TECHNOLOGY, Emerging Cyber Threats Report 2016 (2015), [https://iisp.gatech.edu/sites/default/files/documents/threats\\_report\\_2016.pdf](https://iisp.gatech.edu/sites/default/files/documents/threats_report_2016.pdf)

- [II-3] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).
- [II-4] CONGRESSIONAL RESEARCH SERVICE, Terrorist Use of the Internet: Information Operations in Cyberspace (2011), [www.hsdl.org/?view&did=8233](http://www.hsdl.org/?view&did=8233)

الجدول 1-2- التهديدات الداخلية

| نمط التهديد | الموارد (المهارات، المعارف، إمكانية الوصول، التمويل)                                                                     | الوقت المتاح                                                                                                      | التكيزات المستعملة                                                                                                                                                                                                                                                             | الدافع                                                                                                                     | النوايا                                                                         |
|-------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| عميل سري    | تيسير "الهذسة الاجتماعية"<br>إمكانية الوصول إلى النظام<br>عند مستوى معين<br>توافر وثائق النظام والخبرات الفنية ذات الصلة | يتفاوت بحسب الحال، لكن<br>عموماً ما يكون محدوداً<br>بفعل عدم التمكن من تخصيص ساعات طويلة خارج وظائف العمل العادية | صلاحيات الوصول القائمة، والمعرفة بالبرمجة وبهندسة النظام<br>المعرفة المحتملة بكلمات السر المستخدمة<br>إمكانية إدخال شفرات أبواب خلفية و/أو فيروسات<br>طروادية مصممة لأغراض معينة<br>إمكانية الحصول على دعم من جهات خارجية لديها الجبرات اللازمة<br>قد يكون موجهاً من طرف خارجي | دوافع سياسية أو مالية أو أيديولوجية<br>أو السرقة المعلومات التجارية أو الأسرار التكنولوجية أو المعلومات الشخصية<br>التخريب | سرقّة المعلومات التجارية أو السرّات التكنولوجية أو المعلومات الشخصية<br>التخريب |

الجدول ثانيا-1- التهديدات الداخلية (تابع)

| نمط التهديد     | الموارد (المهارات، المعارف، إمكانية الوصول، التمويل)                                  | الوقت المتاحة                                                                                               | التكتيكات المستعملة                                                                                                                                                      | الدافع    | النوايا                                                                     |
|-----------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------------------------------------------------------------------|
| طرف داخلي مُكره | إمكانية الوصول إلى النظام عند مستوى معين توافر وثائق النظام والخبرات الفنية ذات الصلة | يتفاوت بحسب الحال، لكن عموماً ما يكون محدوداً بفعل عدم التمكن من تخصيص ساعات طويلة خارج وظائف العمل العادية | ملاحيات الوصول القائمة، والمعرفة بالبرمجة وبهندسة النظام المعرفة المحتملة بكلمات السر المستخدمة إمكانية إدخال شفرات أبواب خلفية و/أو فيروسات طرودانية مصممة لأغراض معينة | دافع شخصي | سرقة المعلومات التجارية أو الأسرار التكنولوجية أو المعلومات الشخصية التخريب |
|                 |                                                                                       |                                                                                                             | إمكانية الحصول على دعم من جهات خارجية لديها الخبرات اللازمة                                                                                                              |           |                                                                             |
|                 |                                                                                       |                                                                                                             | موجه من طرف خارجي                                                                                                                                                        |           |                                                                             |

الجدول ثانيا-1- التهديدات الداخلية (تابع)

| نمط التهديد                         | الموارد (المهارات، المعارف، إمكانية الوصول، التمويل)                                                                                                      | الوقت المتاحة                                                                                                               | التكريرات المستعملة                                                                                                                                                                                        | الدافع                       | النوايا                                                                                                                        |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| طرف داخلي غافل                      | إمكانية الوصول للنظم بموجب الصلاحيات المرتبطة بوظائف العمل العادية                                                                                        | لا يلزم أن يكون لديه الوصول للنظم الداخلية دون أن يدري                                                                      | تزويد الخصم بإمكانية الوصول للنظم الداخلية                                                                                                                                                                 | لا يلزم أن يكون لديه أي دافع |                                                                                                                                |
| موظف/مستعمل ساخط (أنواع متعددة)     | مستوى متوسط/مرتفع من الموارد إمكانية الوصول إلى النظام عند مستوى معين توافر وثائق النظم والخبرات الفنية فيما يتعلق بنظم خاصة بأعمال وعمليات تشغيلية معينة | يتفاوت بحسب الحال، لكن عموماً ما يكون محدوداً بفعل عدم التمكن من تخصيص ساعات طويلة (وقد لا يكون ذلك دقيقاً في جميع الحالات) | صلاحيات الوصول القائمة، والمعرفة بالبرمجة وبهندسة النظام المعرفة المعتمدة بكلمات السر المستخدمة القدرة على إدخال أدوات أو سكريبتات "صيبانية" (يمكن أن تكون أكثر إنقفاً إذا كان يتمتع بمهارات حاسوبية خاصة) | دوافع شخصية مالية            | الانتقام، التدمير، إيجاد حالة من الفوضى سرقة المعلومات التجارية إخراج جهة العمل/موظف آخر الإضرار بالسمعة أو تفويض الثقة العامة |
| موظف حالي — مستخدم غير تقني للحاسوب |                                                                                                                                                           |                                                                                                                             |                                                                                                                                                                                                            |                              |                                                                                                                                |

الجدول ثانيا-1- التهديدات الداخلية (تابع)

| نمط التهديد                                                        | الموارد (المهارات، المعارف، إمكانية الوصول، التمويل)                                   | الوقت المتاح      | التكتيكات المستعملة                                                                                          | الدافع            | النوايا |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------|-------------------|---------|
| موظف حالي – مستخدم تقني للحاسوب، مدير نظام، مطور نظام، وما إلى ذلك | مستوى مرتفع من صلاحيات الوصول للحواسيب ومن النفوذ<br>إمكانية الوصول عن بعد             | الكثير من الوقت   | اختراق عناصر من سلسلة الإمداد عن طريق الإخلال بأمن المكونات<br>الاختراق باستخدام وسيط تقال أو الاتصال عن بعد | دوافع شخصية مالية |         |
| معتقد حالي - طرف ثالث                                              | إمكانية الوصول للنظم في الموقع أو عن بعد بموجب الصلاحيات المرتبطة بوظيفة الدعم الحالية | يتفاوت بحسب الحال |                                                                                                              | دوافع شخصية مالية |         |

الجدول ثانيا-1- التهديدات الداخلية (تابع)

| نمط التهديد                                                 | الموارد (المهارات، المعارف، إمكانية الوصول، التمويل) | الوقت المتاحة                                        | التكتيكات المستعملة                                            | الدافع                                | النوايا                                 |
|-------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------|---------------------------------------|-----------------------------------------|
| موظف/مستخدم ساخط مستوى محدود من الموارد (لم يعد قيد الخدمة) | قد تظل بحوزته بعض وثائق النظام                       | قد يستخدم صلاحيات الوصول السابقة غير الخاضعة للإدارة | المعرفة المحتملة بكلمات السر المستخدمة                         | دافع شخصي                             | الانتقام، التدمير، إيجاد حالة من القوضى |
| مجموعة أكبر من الأشخاص                                      | قد تظل بحوزته بعض وثائق النظام                       | قد يستخدم صلاحيات الوصول السابقة غير الخاضعة للإدارة | قد يستخدم صلاحيات الوصول السابقة غير الخاضعة للإدارة           | سروقة المعلومات التجارية              | إجراج جهة العمل/موظف آخر                |
|                                                             |                                                      |                                                      | يمكن أن يكون قد أدخل شغرات أبواب خلفية للنظام أثناء فترة خدمته | الإضرار بالسمعة أو تفويض الثقة العامة |                                         |
|                                                             | المصلات المحتملة مع موظفي المرفق                     |                                                      | "الهندسة الاجتماعية"                                           |                                       |                                         |

الجدول ثانيا-2- التهديدات الخارجية

| نمط التهديد                       | الموارد (المهارات، المعارف، إمكانية الوصول، التمويل)                                                          | الوقت المتاح                                                                                     | التكتيكات المستعملة                                                                                                 | الدافع                                                                                           | النوايا                  |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------------------|
| الهجمات غير الموجهة<br>لهدف بعينه | مستويات متفاوتة من المهارات                                                                                   | يتفاوت بحسب الحال                                                                                | من دون هدف محدد، وعادة ما يعتمد الهجوم على عمليات وثغرات تكنولوجيا المعلومات العادية، بما في ذلك الهندسة الاجتماعية | دوافع شخصية – التنسيلية، الشهرة، اجتذاب وسائل الإعلام<br>تحقيق المكانة                           | استهداف الفرص السانحة    |
| شخص متطرف                         | مستويات متفاوتة من المهارات وإن كانت محدودة عموماً<br>معرفة ضئيلة بالنظام خارج ما هو في نطاق المعلومات العامة | يمكن أن يكون حساساً<br>لعامل الوقت لأنّ الأنشطة قد تتمحور حول أحداث لا تزال جارية أو وقعت حديثاً | أنشطة قرصنة على المستوى الفردي أو على نطاق مجموعة صغيرة<br>توزيع الأدوات على مجموعة أكبر                            | تحقيق أثر سياسي<br>اجتذاب اهتمام وسائل الإعلام<br>الإجراج العلني                                 | جذب اهتمام وسائل الإعلام |
| قرصان هاو                         | مستويات متفاوتة من المهارات وإن كانت محدودة عموماً<br>معرفة ضئيلة بالنظام خارج ما هو في نطاق المعلومات العامة | الكثير من الوقت، مع ضعف القدرة على الصبر                                                         | سكريبتات وأدوات مناصرة<br>للعوموم<br>إمكانية تطوير بعض الأدوات                                                      | دوافع شخصية – التنسيلية، استهداف الفرص السانحة<br>تحقيق المكانة<br>استغلال "الثمار السهلة المال" | استهداف الفرص السانحة    |

الجدول ثانيا-2- التهديدات الخارجية (تابع)

| نمط التهديد     | الموارد (المهارات، المعارف، إمكانية الوصول، التمويل)                                                                                                   | الوقت المتاح                                           | التنكيكات المستعملة                                                                                                           | الدافع                                                                                                                                                                     | النوايا                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| الجريمة المنظمة | مستوى مرتفع من الموارد المستعانة بخبرات متخصصة                                                                                                         | يتفاوت بحسب الحال، لكنه غالباً ما يكون قصير الأجل      | سكربتات، وأدوات مصممة بالجهود الذاتية إمكانية الاستعانة بقراصنة مرتزقة إمكانية الاستعانة بموظف سابق/حالي "الهندسة الاجتماعية" | استغلال التهديد بالانتشهر الابتزاز (لغرض الكسب المالي) اللعب على مخاوف الأعمال فيما يتعلق بوضعها المالي وصورتها العامة الحصول على معلومات للبيع (تقنية أو تجارية أو شخصية) | سرقة مواد سرقة معلومات حساسة بيع المعلومات أو إمكانية الوصول   |
| دولة قومية      | مستوى مرتفع من الموارد والخبرات أنشطة لجمع المعلومات الاستخبارية إمكانية التدريب على تشغيل النظام أو توافر الخبرات التشغيلية أفرقة من الخبراء المدربين | يتفاوت بحسب الحال، ولكنه يكفي لدعم تنفيذ هجمات متواصلة | أدوات متطورة إمكانية الاستعانة بموظف سابق/حالي "الهندسة الاجتماعية"                                                           | دوافع سياسية جمع المعلومات الاستخبارية إرساء نقاط وصول لتنفيذ أعمال لاحقة                                                                                                  | سرقة التكنولوجيا الاستطلاع لغرض تنفيذ هجوم في المستقبل التخريب |

الجدول ثانيا-2- التهديدات الخارجية (تابع)

| نمط التهديد | الموارد (المهارات، المعارف، إمكانية الوصول، التمويل)                                                                                                                       | الوقت المتاحة                            | التكتيكات المستعملة                                                                                                                     | الدافع                                                                                                                                     | النوايا                                                                         |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| إرهابي      | مستويات متفاوتة من المهارات<br>إمكانية التدريب على تشغيل النظام أو توافر الخبرات التشغيلية<br>إمكانية الاختراق عن طريق عميل سري<br>قد يكون مموّلًا جيدًا<br>مهارات متنامية | الكثير من الوقت، مع قدرة كبيرة على الصبر | سكربتات، وأدوات مصممة بالجهود الذاتية<br>إمكانية الاستعانة بقراصنة متروقة<br>إمكانية الاستعانة بموظف سابق/حالي<br>"المهندسة الاجتماعية" | جمع المعلومات الاستخبارية<br>إرساء نقاط وصول لتنفيذ أعمال الاحقة<br>إيجاد حالة من الفوضى الانتقام<br>التأثير في الرأي العام (بإشاعة الخوف) | دعم تنفيذ هجوم مختلط الاستطلاع لغرض تنفيذ هجوم في المستقبل التخريب<br>سرقة مواد |

## المرفق الثالث

### إسناد المسؤوليات المتعلقة بالأمن الحاسوبي

ثالثاً-1- يبيّن الجدول ثالثاً-1 طريقة إسناد المسؤوليات المتعلقة بالأمن النووي إلى السلطات المختصة وفقاً للتوزيع النمطي. وقد يكون من المفيد وضع جدول بالمسؤوليات النمطية المتعلقة بالأمن الحاسوبي التي تقابل هذه المسؤوليات النمطية المتعلقة بالأمن النووي.

الجدول ثالثاً-1- التوزيع النمطي للمسؤوليات المتعلقة بالأمن الحاسوبي في إطار منظومة الأمن النووي

| نوعية الجهة     | المسؤوليات المتعلقة بالأمن النووي                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| الهيئة الرقابية | إنشاء نظام للتحكم الرقابي في المواد المشعة والمرافق ذات الصلة والأنشطة ذات الصلة يضع المسؤولية الرئيسية عن الأمن النووي على عاتق الأشخاص المأذون لهم<br>إنشاء نظام للتصنيف الأمني<br>وضع وتعهد سجل وطني للمواد المشعة<br>المشاركة في التقييم الوطني للتهديدات<br>إعداد وتطبيق وصف التهديدات المحتاط لها في التصميم أو بيان التهديدات البديل أو غير ذلك من وثائق تعريف التهديدات لأغراض التنظيم الرقابي الأمني<br>تنفيذ عملية إصدار الأذن (الترخيص)، بما في ذلك استعراض وتقييم النظم الأمنية وتدابير الإدارة الأمنية<br>وضع المتطلبات الرقابية وتوفير المبادئ التوجيهية الأمنية، بما في ذلك متطلبات حماية المعلومات |

الجدول ثالثا-1- التوزيع النمطي للمسؤوليات المتعلقة بالأمن الحاسوبي في إطار منظومة الأمن النووي (تابع)

| نوعية الجهة                                        | المسؤوليات المتعلقة بالأمن النووي                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                    | <p>إدارة الترابط بين الأمان والأمن</p> <p>إجراء عمليات التفتيش الأمني</p> <p>اتخاذ تدابير الإنفاذ في حالات عدم الامتثال</p> <p>المشاركة في قواعد البيانات الإقليمية والدولية وغيرها من الأنشطة التعاونية</p> <p>تشجيع وتعزيز إرساء ثقافة راسخة في مجال الأمن النووي</p> <p>المشاركة في جهود التخطيط والتأهب والتصدي لأحداث الأمن النووي، بما في ذلك المشاركة في التمارين التي تُعقد لهذا الغرض</p> <p>إدارة إجراءات منح الأذون لعمليات استيراد المواد المشعة وتصديرها، وإجراءات مراقبة تلك العمليات</p> <p>إشعار الجهات المشغلة بوجود تهديد محدد أو بتزايد مستوى التهديد</p> <p>استعراض وتقييم تصميم النظام الأمني (في سياق عملية إصدار الأذون)</p> |
| سلطات إنفاذ القانون                                | <p>اتخاذ تدابير التصدي اللازمة لقطع الطريق أمام الأعمال الشريرة (الوصول دون إذن، السحب دون إذن، التخريب)</p> <p>المشاركة في جهود التخطيط والتأهب والتصدي لأحداث الأمن النووي، بما في ذلك المشاركة في التمارين التي تُعقد لهذا الغرض</p> <p>المشاركة في التقييم الوطني للتهديدات</p> <p>الوقوف على التهديدات المحددة أو المتزايدة المستوى</p> <p>إجراء عمليات فحص السَّير الشخصية لأغراض التحقق من الجدارة بالثقة</p> <p>الكشف عن الأحداث المتصلة بالأمن النووي والتحقيق فيها</p>                                                                                                                                                                    |
| هيئات الجمارك ومراقبة الحدود                       | <p>المشاركة في التقييم الوطني للتهديدات</p> <p>الوقوف على التهديدات المحددة أو المتزايدة المستوى</p> <p>مراقبة حالات عدم الامتثال والكشف عنها فيما يتعلق بعمليات الاستيراد والتصدير</p> <p>التواصل مع الهيئة الرقابية فيما يتعلق برصيد المخزون الوطني من المواد المشعة</p>                                                                                                                                                                                                                                                                                                                                                                          |
| وكالات الاستخبارات والأجهزة الأمنية                | <p>الإشراف على التقييم الوطني للتهديدات</p> <p>الوقوف على التهديدات المحددة أو المتزايدة المستوى</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| الوكالة المعنية بالتصدي للطوارئ على المستوى الوطني | <p>تنسيق التخطيط للأحداث المتصلة بالأمن النووي والتأهب والتصدي لها</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

الجدول ثالثا-1- التوزيع النمطي للمسؤوليات المتعلقة بالأمن الحاسوبي في إطار منظومة الأمن النووي (تابع)

| نوعية الجهة                                    | المسؤوليات المتعلقة بالأمن النووي                                     |
|------------------------------------------------|-----------------------------------------------------------------------|
| الوكالات المعنية بالدفاع المدني والصحة والبيئة | المشاركة في التخطيط للأحداث المتصلة بالأمن النووي والتأهب والتصدي لها |
| وزارة العدل وسلطات الملاحقة القضائية           | فرض العقوبات على مرتكبي الأعمال الشريرة                               |
| وزارة الشؤون الخارجية                          | المشاركة في التعاون الإقليمي والدولي                                  |

## المرفق الرابع

### مثال لإطار الكفاءات ومستويات القدرات في مجال الأمن الحاسوبي

رابعا-1- يؤدي إطار الكفاءات ومستويات القدرات دوراً رئيسياً في ضمان تمتع المنظمات والأفراد بالكفاءة المستمرة اللازمة لأداء الأدوار والمسؤوليات الموكلة إليهم في مجال الأمن الحاسوبي.

رابعا-2- ويقدم هذا المرفق توضيحاً للمقصود بإطار الكفاءات ومستويات القدرات. ولا يتمثل الغرض منه في تقديم إرشادات كافية بشأن وضع إطار من هذا القبيل.

رابعا-3- ويحدد الإطار الكفاءات اللازم توافرها لدى كل منظمة أو فرد في مجالات الأمن الحاسوبي المحددة. وفيما يلي مثال لقائمة بهذه المجالات:

- (أ) الإدارة (القدرات، الاستراتيجية، إدارة الأزمات، الحوكمة، الهيكل التنظيمي)؛
- (ب) التصدي للحوادث (التحليل الجنائي الحاسوبي، الدفاع الشبكي)؛
- (ج) الإطار التشريعي والرقابي (القانون الجنائي، اللوائح)
- (د) أمن المعلومات وإدارتها (الترميز، التشفير، التخزين)؛
- (هـ) المشتريات (العقود، سلسلة الإمداد)؛
- (و) أنشطة التوكيد (الاختبار، الاعتماد، إدارة التهيئة)؛
- (ز) هيكل الأمن الحاسوبي؛
- (ح) التنسيق والمساعدة على الصعيد الدولي.

وبدلاً مما تقدم، ترد في المعيارين الدوليين ISO 27002 [رابعا-1] (بشأن نظم إدارة أمن المعلومات) و IEC 63096 [رابعا-2] (بشأن تطبيق المعيار 27002 على محطات القوى النووية) قوائم بمجالات المراقبة، ويمكن تكييف هذه القوائم لاستخدامها كمجالات للكفاءات.

رابعا-4- ويحدد الإطار المهارات والمعارف المحددة اللازمة في كل مجال من مجالات الكفاءات، بناءً على الاسترشاد بتقييم تهديدات الهجمات السيبرانية، والعلم بطبيعة النظم

الحاسوبية المتاحة لمنظومة الأمن الحاسوبي وبجوانب الضعف التي تنطوي عليها تلك النظم الحاسوبية.

رابعا-5- وتتفاوت المنظمات والأفراد من حيث مستويات نضج كفاءات الأمن الحاسوبي. ويصنف الإطار القدرات اللازم توافرها لكل مجال من مجالات الكفاءات، وفقاً لمقياس من ثلاث مستويات مختلفة على الأقل، مما يكفل اتباع نهج متدرج. وفيما يلي مثال لتصنيف من هذا القبيل، من المستوى الأدنى من النضج إلى المستوى الأعلى:

- (أ) المستوى الأساسي القدرات (مستوى المبتدئين): التصرف على نحو آلي قائم على القواعد، مع التحفظ الشديد وانعدام المرونة.
- (ب) المستوى المتوسط القدرات (مستوى الممارسين): التصرف عن وعي لتحقيق الأهداف الطويلة الأجل والتخطيط وفقاً لسياسة محددة سلفاً.
- (ج) المستوى المتقدم القدرات (مستوى الخبراء): فهم الموقف بداهة والقدرة على التركيز مباشرة على الجوانب الرئيسية.

رابعا-6- ويلزم توافر مستويات مرتفعة من القدرات لضمان الحماية في مواجهة التهديدات المرتفعة القدرات أو لمنع وقوع العواقب الإشعاعية الشديدة. وعلى سبيل المثال، يُعتبر أنَّ السلطات المختصة والجهات المشغلة تدير عواقب شديدة أو بالغة الشدة إذا كان عملها ينطوي على خزن مواد نووية من الفئة الأولى أو الثانية أو نقل مواد من هاتين الفئتين أو استخدامها، أو على تنفيذ أنشطة يمكن أن تؤدي إلى عواقب إشعاعية شديدة.

رابعا-7- ويكفل الإطار التأكد من أنَّ المنظمات والأفراد المسؤولين عن تصميم تدابير الأمن الحاسوبي يتمتعون بمستوى مرتفع من الكفاءات ذات الصلة.

رابعا-8- وهناك بعض المنظمات التي تشترط توافر هذه القدرات بصورة مستمرة داخل الموقع، في حين يعتمد البعض الآخر على المساعدة التي تقدمها منظمات أخرى.

رابعا-9- ويحدد الإطار بالتفصيل نوعية الأنشطة المعتادة التي يمكن أن يسمح لسلطة مختصة أو جهة مشغلة أو طرف ثالث بالاضطلاع بها. وعلى سبيل المثال، يجوز لسلطة مختصة أو جهة مشغلة لديها الكفاءات اللازمة بمستوى قدرات متقدم أن تضطلع بدور قيادي في أنشطة التقييم الوطني للتهديدات المتعلقة بالأمن الحاسوبي. في حين أن

## الجدول رابعا-1- تصنيف الأنشطة بحسب مستوى القدرات

| نوع النشاط                                        | الجهات الأساسية القدرات                                                                               | الجهات المتوسطة القدرات (بالإضافة إلى القدرات الأساسية)                                                                                                               | الجهات المتقدمة القدرات (بالإضافة إلى القدرات المتوسطة)                                                                                                                                                |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| أنشطة متعلقة بمعرفة بيئة التهديدات                | المحافظة على مستوى أساسي من الوعي بسلوكيات الأطراف التي تشكّل تهديداً (مثل هجمات "التصيد" (phishing)) | فهم عواقب تهديدات الأمن الحاسوبي على بيئة الجهة نفسها                                                                                                                 | الرصد المستمر والاستباقي لتهديدات الأمن الحاسوبي السريعة التطور                                                                                                                                        |
| أنشطة متعلقة بتقييمات التهديدات ووضع السيناريوهات | أداء دور مساهم عند الطلب (مثل تقديم تفاصيل عملية بشأن ما يحدث فعلياً في مكان العمل)                   | المشاركة في التقييم الوطني للتهديدات وضع سيناريوهات للموقع المحدد لتوضيح تقييم التهديدات في الحالات التي يكون فيها الأثر المحتمل مرتفعاً أو منخفضاً أو منخفضاً للغاية | الاضطلاع بالدور القيادي في أنشطة التقييم الوطني للتهديدات وضع سيناريوهات للموقع المحدد في الحالات التي يكون فيها الأثر المحتمل مرتفعاً أو مرتفعاً تقييم السيناريوهات الواردة من الجهات المعنية الوسيطة |

السلطة المختصة أو الجهة المشغلة التي تكون كفاءاتها قاصرة على المستوى الأساسي للقدرات لا يجوز لها أن تشارك في تقييم التهديدات الوطني إلا بدور داعم. ويوضح الجدول رابعا-1 ذلك.

## مراجع المرفق الرابع

[IV-1]INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Technology — Security Techniques — Code of Practice for Information Security Controls, ISO/IEC 27002:2013, ISO, Geneva (2013).

[IV-2]INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems — Security Controls, IEC 63096:2020, IEC, Geneva (2020).



## مسرد المصطلحات

**أصول المعلومات الحساسة:** أي معدات أو مكونات تُستخدم لتخزين المعلومات الحساسة أو معالجتها أو التحكم فيها أو إرسالها. وعلى سبيل المثال، تشمل أصول المعلومات الحساسة نظم المراقبة والشبكات ونظم المعلومات وأي وسائط إلكترونية أو مادية.

**الأمن الحاسوبي:** جانب محدد من أمن المعلومات يتعلق بحماية النظم الحاسوبية مما قد يخل بها.

**أمن المعلومات:** الحفاظ على سرية المعلومات وسلامتها وتوافرها.

**الأصول الرقمية الحساسة:** أصول المعلومات الحساسة المؤلفة من نظم حاسوبية (أو التي تشكل أجزاءً من نظم حاسوبية).

**برنامج الأمن الحاسوبي:** الخطة الموضوعة لتنفيذ استراتيجية الأمن الحاسوبي والتي تحدد الأدوار والمسؤوليات والإجراءات على مستوى المنظمة الواحدة. ويحدّد البرنامج بالتفصيل سبل تحقيق أهداف الأمن الحاسوبي ويشكل جزءاً من الخطة الأمنية العامة (أو يكون مرتبطاً بها).

**تدابير الأمن الحاسوبي:** التدابير المتخذة بقصد منع وقوع أعمال شريرة أو أعمال أخرى يمكن أن تخل بالأمن الحاسوبي، أو للكشف عن هذه الأعمال أو تعطيلها أو التصدي لها أو التخفيف من عواقبها في حال وقوعها.

**حادثة الأمن الحاسوبي:** أي واقعة تؤدي بالفعل أو يمكن أن تؤدي إلى الإخلال بسرية النظم الحاسوبية (بما فيها المعلومات) أو سلامتها أو توافرها، أو تشكل مخالفة للسياسات الأمنية أو خطراً وشيكاً بمخالفة السياسات الأمنية.

**مستوى الأمن الحاسوبي:** مدى صرامة الحماية المطلوبة لتحقيق متطلبات الأمن الحاسوبي المتعلقة بوظيفة ذات صلة بالأمن النووي و/أو الأمان النووي و/أو حصر المواد النووية ومراقبتها و/أو إدارة المعلومات الحساسة.

**المعلومات الحساسة:** المعلومات الموجودة في أي شكل من الأشكال، بما في ذلك البرامج الحاسوبية، والتي يمكن أن يؤدي إفشاؤها أو تعديلها أو تبديلها أو إتلافها دون إذن أو الحرمان من استخدامها إلى الإخلال بالأمن النووي.

**النطاق الأمني الحاسوبي:** أي مجموعة من النظم التي لها حدود مادية و/أو منطقية مشتركة -وتخضع لترتيبات قائمة على معايير إضافية، عند الاقتضاء -والتي يُحدّد لها مستوى واحد من مستويات الأمن الحاسوبي بهدف تبسيط إدارة تدابير الأمن الحاسوبي والتواصل بشأنها وتطبيقها.

**النظم الحاسوبية:** التكنولوجيات التي تُنتج المعلومات الرقمية أو تتيح الوصول إليها أو تعالجها أو ترسلها أو تخزينها، أو التي تؤدي خدمات تنطوي على هذه المعلومات أو تقدم خدمات من هذا القبيل أو تتحكم فيها.

① يمكن لهذه النظم أن تكون مادية أو افتراضية. وهي تشمل: الحواسيب المكتبية والنقالة واللوحية وغيرها من الحواسيب الشخصية، والهواتف الذكية، والحواسيب الكبيرة، ووحدات الخدمة، والحواسيب الافتراضية، والتطبيقات البرمجية، وقواعد البيانات، والوسائط القابلة للنقل، والأجهزة الرقمية وأجهزة التحكم الرقمي، والطابعات، وأجهزة الشبكات، والمكونات والأجهزة المدمجة.

**الهجوم السيبراني:** عمل شرير يُنفَّذ بنية سرقة بند مستهدف محدد أو تعديله أو منع الوصول إليه أو إتلافه، من خلال الوصول غير المأذون به إلى نظام حاسوبي حساس أو تنفيذ إجراءات داخل هذا النظام.

**الهجوم المختلط:** عمل شرير ينطوي على تنفيذ هجوم سيبراني بالتنسيق مع هجوم مادي.



## طلب شراء المنشورات محلياً

يمكن شراء المنشورات المسعّرة الصادرة عن الوكالة الدولية للطاقة الذرية من المصادر المذكورة في القائمة أدناه أو من المكتبات المحلية الكبرى.

أمّا المنشورات غير المسعّرة فينبغي توجيه طلبات شرائها إلى الوكالة مباشرة. وترد تفاصيل الاتصال في آخر هذه القائمة.

### أمريكا الشمالية

#### **Bernan / Rowman & Littlefield**

15250 NBN Way, Blue Ridge Summit, PA 17214, USA

Telephone: +1 800 462 6420 • Fax: +1 800 338 4550

Email: orders@rowman.com • Web site: www.rowman.com/bernan

### سائر بلدان العالم

برجاء الاتصال بالمورّد المحلي المفضّل لديكم، أو بالموزّع الرئيسي الخاص بنا:

#### **Eurospan Group**

Gray's Inn House

127 Clerkenwell Road

London EC1R 5DB

United Kingdom

الطلبات التجارية والاستفسارات:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640

Email: eurospan@turpin-distribution.com

الطلبات الفردية:

www.eurospanbookstore.com/iaea

للحصول على مزيد من المعلومات:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609

Email: info@eurospangroup.com • Web site: www.eurospangroup.com

ويمكن توجيه طلبات شراء المنشورات، المسعّرة وغير المسعّرة على السواء، مباشرة إلى العنوان التالي:

Marketing and Sales Unit

International Atomic Energy Agency

Vienna International Centre, PO Box 100, 1400 Vienna, Austria

Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529

Email: sales.publications@iaea.org • Web site: https://www.iaea.org/ar/almanshurat





يقدم هذا المنشور إرشادات بشأن إرساء وتنفيذ الأمن الحاسوبي باعتباره مكوناً رئيسياً من مكونات الأمن النووي. وينطبق هذا المنشور على الجوانب المتصلة بالأمن النووي وبالترابط بينه وبين الأمان النووي وسائر عناصر منظومة الأمن النووي في الدولة، بما في ذلك أمن المواد النووية والمرافق النووية، وأمن المواد المشعة والمرافق المرتبطة بها، وأمن المواد النووية والمواد المشعة الأخرى غير الخاضعة للتحكم الرقابي. ويشمل نطاق هذا المنشور ما يلي: النظم الحاسوبية التي يمكن أن يؤدي الإخلال بها إلى تأثير سلبي في الأمن النووي أو الأمان النووي؛ والأدوار والمسؤوليات المنوطة بالدولة وبالكيانات المعنية الأخرى فيما يتعلق بالأمن الحاسوبي ضمن منظومة الأمن النووي؛ والأنشطة التي تضطلع بها الدولة من أجل وضع وتنفيذ استراتيجية للأمن الحاسوبي لأغراض الأمن النووي؛ والعناصر التي تتكون منها برامج الأمن الحاسوبي؛ والأنشطة اللازمة للمحافظة على استدامة نظم الأمن الحاسوبي ضمن منظومة الأمن النووي.