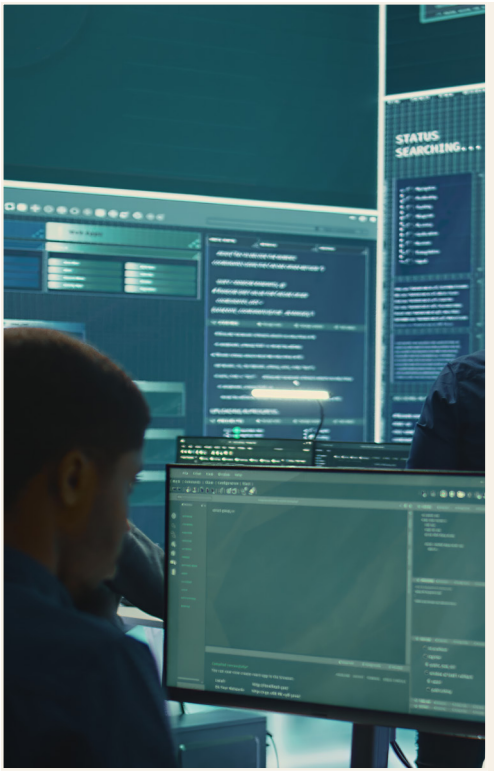
Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
رؤى أمنية

التحديات الناشئة في مجال جرائم تقنية المعلومات

The Emerging Challenges in Cybercrimes



الرسائل الأساسية

- **التحول الرقمي والأصول المعلوماتية:** مع زيادة الاعتماد على التقنيات الرقمية، أصبحت الأصول المعلوماتية هدفًا جذابًا للهجمات السيبرانية.
- **التطور التكنولوجي:** تسهم التقنيات الحديثة، مثل: الذكاء الاصطناعي، وإنترنت الأشياء في زيادة تعقيد الهجمات السيبرانية، وجعلها أكثر دقة وسرعة.
- **التهديدات الجيوسياسية:** تستخدم الدول قدراتها السيبرانية لتحقيق أهداف إستراتيجية، وهو ما يزيد من حدة التنافس السيبراني.
- **انتهاكات الخصوصية:** يتم استغلال البيانات الشخصية لأغراض تجارية، وهو ما يمثل انتهاكًا للخصوصية، ويؤدي إلى غرامات باهظة.

وتكمن آثار هذه التحديات في الآتي:

- عرقلة تحقيق أهداف التنمية المستدامة: تؤثر الهجمات السيبرانية في البنية التحتية الحيوية، وهو ما يعوق تحقيق أهداف التنمية المستدامة.
- تآكل الثقة في المؤسسات: تؤدي الهجمات السيبرانية إلى فقدان الثقة في المؤسسات الحكومية والشركات.
- خسائر اقتصادية فادحة: تتسبب الهجمات السيبرانية في خسائر مالية كبيرة للمؤسسات والأفراد.

المقدمة

فِي عصرِنَا الحاليِّ، الذي يشهد تحولًا رقميًّا متسارعًا، وتطورًا تقنيًّا مستمرًّا، أصبحت تقنية المعلومات جزءًا لا يتجزأ من حياتنا اليومية وعملياتنا التجارية. ومع هذا التقدم، برزت تحديات جديدة تتعلق بجرائم تقنية المعلومات؛ حيث يسعى مرتكبو الجرائم السيبرانية إلى استغلال هذه التطورات؛ لتحقيق مكاسب غير مشروعة، وهو ما يشكل تهديدًا متزايدًا للأفراد والمؤسسات والدول على حد سواء.

إن هذه التحديات الناشئة لم تعد تقتصر على الهجمات التقليدية كاختراق الشبكات وسرقة البيانات، بل امتدت لتشمل أساليب أكثر تعقيدًا وخطورة، مثل: التزييف العميق، وهجمات الفدية التي تستهدف

البنية التحتية الحيوية، والتلاعب بالبيانات الحساسة عبر الحوسبة السحابية. هذه التهديدات تتطلب تفكيرًا جديدًا وإستراتيجيات مبتكرة لمواجهتها والتصدي لها، وبالرغم من تسابق الدول على استخدام التقنيات الناشئة والتحول الرقمي لتقديم خدمات إلكترونية لمجتمعاتها وبناء اقتصادات تعتمد على التقنيات، إلا أنها خلقت تحديات للدول؛ حيث يتجه العالم وبشكل متسارع إلى عصر سباق التسلح السيبراني، وكذلك يتجه المجرمون والإرهابيون لاستغلال تقنية المعلومات، لعدة أسباب من أهمها:

أهداف التنمية المستدامة

تُمَثِّلُ أهدافُ التنمية المستدامة، التي أطلقتها الأمم المتحدة، خارطةَ طريقٍ لتحقيق عالم أفضل. وقد حققت الدول تقدمًا ملحوظًا في العديد من المجالات، بدعم من التكنولوجيا الرقمية. ومع ذلك، فإن تحقيق هذه الأهداف يواجه تحديات جديدة، تتمثل في التهديدات السيبرانية المتزايدة. فالهجمات السيبرانية تستهدف البنية التحتية الحيوية، وهو ما يعرض تحقيق أهداف (مثل: القضاء على الجوع، وتحسين الصحة، وتوفير التعليم الجيد، والمساواة بين الجنسين) للخطر. ولذلك، فإن تعزيز الأمن السيبراني أصبح ضرورة ملحة لضمان استدامة التنمية. فمن خلال حماية البنية التحتية الرقمية، يمكن للدول تعزيز الثقة في التقنيات الرقمية، وتحقيق أقصى استفادة من إمكاناتها في دفع عجلة التنمية المستدامة؛ لذا أشارت الإنتربول إلى أن الجرائم السيبرانية قد تمثل تحديًا لثمانية أهداف للتنمية المستدامة، وهي: الهدف الأول (القضاء على الفقر)، والثالث (الصحة الجيدة والرفاء)، والرابع (التعليم الجيد)، والخامس (المساواة بين الجنسين)، والثامن (العمل اللائق ونمو الاقتصاد)، والتاسع (الصناعة والابتكار والهياكل الأساسية)، والسادس عشر (السلام والعدل والمؤسسات القوية)، والسابع عشر (عقد الشراكات لتحقيق الأهداف).

التحول في الأصول

شَهِدَ العالمُ تسارعًا غير مسبوق في التحول الرقمي، مدفوعًا بأهداف التنمية المستدامة وأزمة كوفيد19-. فقد أصبحت الأصول المعلوماتية والتقنية حجر الزاوية في بناء مجتمعات واقتصادات قائمة على المعرفة. ومع تزايد الاعتماد على التقنيات الرقمية، مثل: الخوادم والحاسوب المحمول والأجهزة المحمولة والبرمجيات، ازدادت أيضًا قيمة هذه الأصول، وأصبحت هدفًا جذابًا للهجمات السيبرانية. فمن البيانات الحساسة إلى البنية التحتية الحيوية، فإن أي خلل في الأنظمة الرقمية يمكن أن يعرض تحقيق أهداف التنمية المستدامة للخطر.

التطور الكبير في التقنيات الحديثة

شَهِدَ العالمُ تسارعًا هائلًا في تطوير وتبني التقنيات الحديثة، مثل: الذكاء الاصطناعي وإنترنت الأشياء والميتافيرس. ومع أن هذه التقنيات توفر فرصًا هائلةً للتقدم والنمو، إلا أنها تفتح الباب أمام تحديات أمنية جديدة. ففي الوقت الذي تسعى فيه الدول إلى الاستفادة القصوى من هذه التقنيات، فإنها تواجه خطر استغلالها من قبل الجهات الساعية إلى زعزعة الاستقرار وتنفيذ أعمال إجرامية.

قدرات سيبرانية مدعومة من الدول

باتت الدول تستخدم قدرات سيبرانية لتحقيق أهداف إستراتيجية، مثل: التجسس الاقتصادي، والتأثير في الرأي العام، وتعطيل البنية التحتية الحيوية. وهذه الهجمات تتميز بتخطيطها الدقيق واستخدامها لأحدث التقنيات، وهو ما يجعلها صعبة الكشف والتصدي. وتشير التقارير إلى أن عدد هذه الهجمات آخذ في الازدياد، وهو ما يدل على تزايد اعتماد الدول على الأدوات السيبرانية لتحقيق أهدافها؛ حيث أكد تقرير شركة كراود ستريك أنهم رصدوا في عام 2023م ازديادًا لقائمة الجهات المهددة للأمن السيبراني المدعومة من الدول في حدود 34 جهة، وهو ما زاد عدد الهجمات إلى أكثر من 200 هجمة سيبرانية.

التحديات الجيوسياسية

تشكل التطورات الجيوسياسية عاملًا حاسمًا في تشكيل مشهد التهديدات السيبرانية. فالتنافس بين الدول، والصراعات الإقليمية، والتغيرات في التوازن بين القوى الدولية، كلها عوامل تسهم في زيادة حدة الهجمات السيبرانية وتنوعها. وقد أظهر استطلاع لمنتدى الاقتصاد العالمي أن 70% من قادة الأمن السيبراني يرون أن التحديات الجيوسياسية هي المحرك الرئيس وراء تطور التهديدات السيبرانية، وهو ما يؤدي إلى زيادة الهجمات على البنية التحتية الحيوية وسلاسل الإمداد العالمية.

وكشفت مايكروسوفت عن تورط 7 نطاقات روسية في شن هجمات سيبرانية تستهدف المؤسسات الأوكرانية ومراكز الفكر في الغرب. وتهدف هذه الهجمات إلى اختراق الأنظمة الحيوية وتسريب المعلومات الحساسة لدعم العمليات العسكرية الروسية وتقويض جهود الدول الداعمة لأوكرانيا. كما استهدفت هذه الهجمات أكثر من 128 منظمة أمريكية وحليفة، وهو ما يؤكد الدور المتزايد للاستخبارات الروسية في شن حروب سيبرانية بهدف تحقيق أهداف جيوسياسية.

البيانات الشخصية

شهدت السنوات الأخيرة استغلالًا واسعًا للبيانات الشخصية لأغراض تجارية؛ حيث تقوم الشركات الكبرى بجمع وتحليل كميات هائلة من البيانات دون الحصول على موافقة واضحة من المستخدمين. وقد أدت هذه الممارسات إلى غرامات باهظة، على سبيل المثال:

- في عام 2022، غرَّمت إيرلندا شركة ميتا 390 مليون يورو لاستهدافهم المستخدمين بإعلانات بناءً على ما يقومون به من أنشطة في الإنترنت.
- في عام 2022، وافقت شركة تويتر على دفع غرامة للحكومة الأمريكية بعد تضليلها المستخدمين بكيفية حماية بياناتهم الشخصية؛ حيث كانت تستخدم بيانات الاتصال الخاصة بهم لمساعدة المسوقين على استهداف المستخدمين بالإعلانات.
- في عام 2020، فرضت محكمة فرنسية غرامة مالية بقيمة 50 مليون يورو على شركة جوجل؛ لافتقارها إلى الشفافية والوضوح في الطريقة التي يُبَلَّغ بها المستخدمون عن تعاملها مع البيانات الشخصية، ولا تحصل بطريقة ملائمة على موافقتهم على الإعلانات الشخصية.

المنهجية

تعتمد هذه الورقة على بيانات موثوقة وتقارير رسمية صادرة عن جهات دولية معترف بها؛ للوقوف على التحديات الناشئة في مجال تقنية المعلومات.

جمع البيانات من التقارير الدولية والإقليمية

استندت هذه الورقة إلى تحليل مجموعة واسعة من التقارير والأبحاث، التي أصدرتها أبرز المنظمات الدولية المتخصصة في مكافحة الجريمة، مثل: الإنتربول (Interpol) واليوروبول (Europol) ومكتب التحقيقات الفيدرالي (FBI) والمركز الأوروبي للكفاءة في الأمن السيبراني (ECCC). كما شملت الورقة تقارير من مؤسسات أكاديمية متخصصة في الجرائم السيبرانية، كمركز الجرائم السيبرانية والأدلة الرقمية (CoECDF) بجامعة نايف العربية للعلوم الأمنية. بالإضافة إلى ذلك، تمت الاستعانة بتقارير صادرة عن مؤسسات دولية ذات صلة، مثل: البنك الدولي ومنظمة الصحة العالمية (WHO)؛ لتغطية الجوانب الاقتصادية والصحية المرتبطة بالتقنيات الناشئة.

تصنيف البيانات

من خلال تصنيف البيانات وفقًا لنوع التقنية والتحدي المرتبط بها، تمكن الباحثون من تحديد طبيعة التهديدات المحددة لكل تقنية. وقد أظهر هذا التحليل أن التزييف العميق يُشَكِّل تهديدًا متزايدًا للمصداقية المعلوماتية، ويمكن استغلاله في العديد من الجرائم، بما في ذلك الاحتيال المالي. كما كشفت الورقة عن أن هجمات الفدية تمثل تهديدًا مباشرًا للبنية التحتية الحيوية، وهو ما يؤثر في الاقتصاد والمجتمع بشكل عام.

أهم التحديات الناشئة الرئيسة التي أبرزتها التقارير

منتدى الاقتصاد العالمي

أكد قادة الأمن السيبراني في الاستطلاع أن الذكاء الاصطناعي يشكل تهديدًا متزايدًا على الأمن المعلوماتي والاجتماعي. فمن خلال إنشاء وتوزيع المعلومات المضللة والأخبار الزائفة، وتزييف المحتوى المرئي والصوتي، واستهداف الناخبين بإعلانات مضللة، والتلاعب بالخوارزميات على وسائل التواصل الاجتماعي، يمكن للذكاء الاصطناعي التأثير في الرأي العام، وتقويض الثقة في المؤسسات، والتدخل في الانتخابات.

أكد قادة الأمن السيبراني في الاستطلاع أن الذكاء الاصطناعي قد يخلق 6 تحديات، وهي كالآتي:

- **المعلومات المضللة والأخبار الزائفة:** وتشكل المعلومات المضللة والأخبار الزائفة تهديدًا كبيرًا للرأي العام؛ حيث يمكن أن تؤثر في نتائج الانتخابات وتقوض الثقة في المؤسسات.
- **الفيديوهات والمقاطع الصوتية المزيفة:** ويمكن استخدام مقاطع الفيديو أو التسجيلات الصوتية المزيفة، التي تم إنشاؤها بواسطة الذكاء الاصطناعي في هذا النوع المحدد من المعلومات المضللة؛ لنشر معلومات كاذبة عن المرشحين أو التلاعب بالرأي العام.
- **التضليل الآلي:** ويمكن استخدام خوارزميات الذكاء الاصطناعي لإنشاء ونشر كميات كبيرة من المعلومات المضللة، وهو ما يجعل من الصعب اكتشافها ومكافحتها.
- **الإعلانات الموجهة:** يمكن استخدام الاستهداف المباشر، الذي يقوده الذكاء الاصطناعي للمعلومات المضللة أو الخاطئة للناخبين، من خلال الإعلانات الشخصية للتلاعب بالآراء أو تقليل إقبال الناخبين.

- **مخاوف الخصوصية:** وعندما يتم استقاء معلومات التصويت من الهوية الوطنية أو من طرق أخرى مرتبطة بالمعلومات الشخصية، قد تؤدي المعالجة الآلية للبيانات إلى خلق فرصٍ لتسرب البيانات الشخصية.
- **التلاعب الخوارزمي بوسائل التواصل الاجتماعي:** ويمكن التلاعب بخوارزميات الذكاء الاصطناعي على منصات التواصل الاجتماعي؛ لتضخيم بعض الرسائل السياسية أو تحجيم بعض الرسائل، وهو ما يؤثر في الرأي العام.

يوروبول (Europol)

تقرير حديث صادر عن اليوروبول تحت عنوان «التزييف العميق»:

- يكشف التحديات أمام إنفاذ القانون و"تقييم تهديدات المنظمة عبر الإنترنت 2024" (IOCTA) النقاب عن استخدام التزييف العميق في الاحتيال والتضليل الإعلامي. ويسلط الضوء على التهديدات المتزايدة التي تشكلها هجمات الفدية على البنية التحتية الحرجة.
- إضافة إلى ذلك، يحذر التقرير من التحيزات الخوارزمية والمخاوف المتعلقة بحقوق الإنسان عند استخدام الذكاء الاصطناعي في إنفاذ القانون. فالعملات المشفرة تمثل تحديًا آخر؛ حيث تُستخدم في غسل الأموال وتمويل الإرهاب، في حين أن التكنولوجيا البيومترية تواجه أخطار التلاعب بالبيانات وأمانها. كما يشير التقرير إلى تصاعد الأنشطة غير القانونية، التي تُنفذ باستخدام المركبات ذاتية القيادة، مثل: تهريب المخدرات.

الإنتربول (Interpol)

- يكشف تقرير الإنتربول «التقييم العالمي للجرائم المالية والسيبرانية» عن أن التزييف العميق يستخدم بشكل متزايد في الاحتيال والتضليل الإعلامي، وهو ما يشكل تهديدًا كبيرًا لأمن المعلومات.
- وتستهدف هجمات الفدية البنية التحتية الحرجة، وهو ما يسبب خسائر مالية فادحة، ويهدد استقرار الأنظمة الحيوية.
- كما يعبر التقرير عن قلقه من التحيزات الخوارزمية ومخاوف حقوق الإنسان التي تنشأ عند استخدام الذكاء الاصطناعي في إنفاذ القانون.
- وتمثل العملات المشفرة تحديًا أمنيًّا رئيسًا بسبب استخدامها في غسل الأموال وتمويل الإرهاب،

بينما تواجه التكنولوجيا البيومترية تحديات تتعلق بالتلاعب بالبيانات ومخاطر الأمان.

- التقرير يشير أيضًا إلى التهديدات الناشئة عن استخدام المركبات ذاتية القيادة في الأنشطة غير القانونية، مثل: تهريب المخدرات، مؤكدًا الحاجة إلى تعزيز التعاون الدولي لمكافحة هذه التهديدات.
- وكشف منتدى الإنتربول المتعلق بالتكنولوجيا الجديدة، الذي عقد في 2022م، عن أن جهات إنفاذ القانون تواجه تحديات متزايدة في مواكبة التطورات التكنولوجية المتسارعة، خاصة مع ظهور بيئات رقمية جديدة، مثل الميتافيرس. فطبيعة الميتافيرس اللامركزية، التي توفر مساحات افتراضية واسعة للتفاعل والتعاملات المالية، تجعل من الصعب على الأجهزة الأمنية تتبع الجرائم المرتكبة فيها.
- كما أن استخدام الرموز غير القابلة للاستبدال (NFTs) في مخططات غسل الأموال والأنشطة الإجرامية الأخرى، ووجودها على منصات لامركزية، مثل: البلوكتشين، يزيد من تعقيد مهمة مكافحة الجرائم السيبرانية. هذه التطورات تتطلب من أجهزة إنفاذ القانون تطوير أدوات جديدة وتعديل القوانين القائمة لضمان قدرتها على مواجهة هذه التحديات.

المركز الأوروبي للكفاءة في الأمن السيبراني (ECCC)

- تضمن تقرير المركز الأوروبي للكفاءة في الأمن السيبراني (European Cybersecurity Competence Centre - ECCC) أمن الحوسبة السحابية وتطوير معايير أمان لحماية البيانات في البيئات السحابية.
- وأكد التقرير أهمية التشفير المتقدم وحماية البيانات الحساسة من خلال تقنيات التشفير المتطورة، وتعزيز التعاون بين الدول الأوروبية لحماية البنية التحتية الحيوية.

مركز الجرائم السيبرانية والأدلة الرقمية بجامعة نايف العربية للعلوم الأمنية (CoECDF)

- تناول تقرير لمركز الجرائم السيبرانية والأدلة الرقمية بجامعة نايف العربية للعلوم الأمنية التزييفَ العميقَ وتأثيره في المجتمعات العربية، واستخدامه في الاحتيال والابتزاز.
- تحدث تقرير آخر للمركز عن هجمات الفدية وزيادة انتشارها في القطاعات الحيوية بالدول العربية، والذكاء الاصطناعي ودوره في تعزيز الجرائم السيبرانية واستخدامه في التهديدات المعقدة.

مكتب التحقيقات الفيدرالي (FBI)

- سلطت تقارير متعددة صادرة عن مكتب التحقيقات الفيدرالي (FBI) الضوء على التحديات المرتبطة بالتكنولوجيا البيومترية، مثل: التلاعب بالبيانات ومخاطر الأمان التي تهدد خصوصية المستخدمين وأمن المؤسسات.
- بالإضافة إلى ذلك، يشير التقرير إلى التهديدات المتزايدة، التي تستهدف البنية التحتية الحرجة من خلال هجمات الفدية، والتي تهدف إلى تعطيل الأنظمة الحيوية وسرقة البيانات الحساسة.
- كما يركز التقرير على أهمية تعزيز الأمن المعرفي لمواجهة التضليل المعلوماتي والتأثير في العقول البشرية من خلال استخدام تقنيات التزييف العميق والذكاء الاصطناعي.

منظمة الصحة العالمية (WHO)

- سلط تقرير صادر عن منظمة الصحة العالمية (WHO) الضوء على التحديات الأخلاقية والخصوصية المتعلقة باستخدام الذكاء الاصطناعي في الطب.
- يركز التقرير على كيفية تطبيق تقنيات الذكاء الاصطناعي لتحسين الرعاية الصحية مع الحفاظ على أخلاقيات المهنة وحماية خصوصية المرضى.
- يشير التقرير إلى أن هذه التحديات تتطلب اهتمامًا خاصًّا؛ لضمان أن الابتكارات التقنية لا تأتي على حساب حقوق الإنسان.

البنك الدولي

- ناقش تقرير صادر عن البنك الدولي التحديات المرتبطة بإدارة المخاطر في النظام المالي اللامركزي (DeFi) باستخدام العملات المشفرة.
- ويشير التقرير إلى أن العملات المشفرة تمثل فرصة لتوسيع الوصول المالي، ولكنها في الوقت نفسه تفرض تحديات كبيرة تتعلق بغسل الأموال وتمويل الإرهاب.
- ويوصي البنك الدولي بتطوير أطر تنظيمية دولية لإدارة هذه المخاطر، وتعزيز الأمان في النظام المالي العالمي.

ويوضح الشكل (1) ارتباط التحديات الناشئة بالتقنيات.

الشكل 1

ارتباط التحديات الناشئة بالتقنيات

الخاتمة

يشكل التزايد الهائل في الجرائم السيبرانية تهديدًا وجوديًّا للأمن والاستقرار في العالم الرقمي. ولقد تجاوزت هذه الجرائم حدود الدول والمؤسسات؛ لتصل إلى الأفراد وتؤثر في حياتهم اليومية. إن التعامل مع هذه التحديات يتطلب تضافر الجهود على المستوى العالمي والإقليمي والوطني.

وتُظهر الدراسات والبحوث أن التقنيات الناشئة، مثل: الذكاء الاصطناعي وإنترنت الأشياء تزيد من تعقيد المشهد السيبراني، وتفتح أبوابًا جديدةً لجرائم تقنية المعلومات. ومع ذلك، فإن هذه التقنيات

نفسها تحمل في طياتها الحلول لمواجهة هذه التحديات. ومن خلال الاستثمار في البحث والتطوير وبناء القدرات البشرية، يمكننا تطوير أدوات وأنظمة أكثر فعالية للكشف عن الجرائم السيبرانية والتصدي لها.

التوصيات

1. بناء منظومة دفاعية شاملة ضد الجرائم السيبرانية، تشمل:
   - تطوير إستراتيجيات وطنية وإقليمية لمكافحة الجرائم السيبرانية.
   - تعزيز التعاون الدولي وتبادل المعلومات الاستخباراتية.
   - بناء القدرات البشرية في مجال الوقاية من الجرائم السيبرانية.
   - تطوير التشريعات والقوانين اللازمة لمواجهة الجرائم السيبرانية.
2. الاستثمار في أحدث التقنيات والأدوات لمكافحة الجرائم السيبرانية، مثل: الذكاء الاصطناعي وأنظمة الكشف عن التهديدات المتقدمة.
3. توعية المجتمع بأهمية الأمن السيبراني، وكيفية حماية أنفسهم من الهجمات السيبرانية.
4. حماية البنية التحتية الحيوية من الهجمات السيبرانية؛ حيث تعتبر هذه البنية شريان الحياة للاقتصاد والمجتمع.
5. تشجيع الشراكة بين القطاع العام والخاص لتعزيز الأمن السيبراني.
6. تطوير آليات للاستجابة السريعة على الهجمات السيبرانية، بما في ذلك فرق الاستجابة لحوادث الأمن السيبراني.
7. بناء ثقافة أمنية قوية في جميع المؤسسات، تشجع على تبادل المعلومات والتعاون في مجال الأمن السيبراني.
8. تقارير متخصصة: الاستفادة من تقارير مركز الجرائم السيبرانية والأدلة الرقمية بجامعة نايف العربية للعلوم الأمنية.
9. تدريب سيبراني: الطلب من مركز الجرائم السيبرانية والأدلة الرقمية بجامعة نايف العربية للعلوم الأمنية، القيام بتنفيذ تدريب سيبراني للدول العربية؛ لقياس جاهزية الجهات على التعامل مع الجرائم السيبرانية.

المصادر

الإنتربول. (2020). إطار الإنتربول لمواجهة حوادث الطائرات المسيَّرة. تم الاسترداد بتاريخ 24/6/2023، من: https://www.interpol.int/ar/content/download/15298/file/DFL_DroneIncident_Final_AR.pdf?inLanguage=ara-SA&version=5

إنتر ريجونال للتحليلات الإستراتيجية. (2023). اللاعبون الجدد: ما أهداف الدول الصاعدة في إنتاج الدرونز؟". تقديرات إنتر ريجونال. تم الاسترداد بتاريخ 22/6/ 2023، من: https://www.interregional.com/app/uploads/2023/03/1678201230_508_3485635_171.pdf

الحرة. (2020). أمريكا تسمح للطائرات دون طيار بتوصيل الطلبات للمنازل. تم الاسترداد بتاريخ 19/12/2023، من: https://www.alhurra.com/usa/2020/12/29/

خرفاتي، زينب. (2020). اختراق "الطائرات دون طيار" أكبر التهديدات الأمنية لـ 2017. العربية. نت. تم الاسترداد بتاريخ 24/6/2023، من: https://www.alarabiya.net/arab-and-world/2016/11/30/

ماركس، باول. (2017). جرائم طائرات الدرون.. من التجسس إلى حمل المتفجرات. BBC NEWS عربي. تم الاسترداد بتاريخ 27/6/2023، من: https://www.bbc.com/arabic/vert-fut-41090353

Europol. (2023). Facing reality? Law enforcement and the challenge of deepfakes. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes

Europol. (2024). Internet organised crime threat assessment (IOCTA) 2024. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

INTERPOL. (n.d.). Cybercrime. https://www.interpol.int/en/Crimes/Cybercrime

Federal Bureau of Investigation. (n.d.). Biometrics and security. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics

INTERPOL. (n.d.). Emerging crimes. https://www.interpol.int/en/Crimes/Emerging-crimes

World Health Organization. (2023). Artificial intelligence in healthcare. https://www.who.int/news-room/fact-sheets/detail/artificial-intelligence-in-healthcare

World Bank. (n.d.). Decentralized finance. https://www.worldbank.org/en/topic/decentralized-finance

Europol. (2023). Emerging technologies and cognitive security. https://www.europol.europa.eu/publications-events/main-reports/emerging-technologies-and-cognitive-security

Federal Bureau of Investigation. (n.d.). Cyber crime. https://www.fbi.gov/services/cjis/cyber-crime

Center of Excellence for Cybercrime and Digital Forensics. (2023). Ransomware trend report 2023. Naif Arab University for Security Sciences.

Center of Excellence for Cybercrime and Digital Forensics. (2023). Deepfake incidents and their implications.

Naif Arab University for Security Sciences.

CrowdStrike. (2024). 2024 Global threat report.

https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

Egyptian Center for Strategic Studies. (2023). Reading the cyber conflict between Russia and Ukraine.

https://ecss.com.eg/19881/

INTERPOL. (2022). Modern technology at the center of the INTERPOL forum.

https://www.interpol.int/ar/1/1/2022/60

Naif Arab University for Security Sciences. (2023). Ransomware trends in Arab countries, 2020-2022.

https://nup.nauss.edu.sa/index.php/sr/catalog/book/250

Naif Arab University for Security Sciences. (2023). First forum on the uses of artificial intelligence in security fields: 2023 Forum report.

https://nup.nauss.edu.sa/index.php/sr/catalog/book/272

July 2026 يوليو 2026

Centre for Cybercrime and Economic Crime **مركز الجرائم السيبرانية والاقتصادية**

Naif Arab University for Security Sciences جامعة نايف العربية للعلوم الأمنية

Riyadh, Saudi Arabia الرياض، المملكة العربية السعودية

Keywords: cybercrime, emerging technologies, cybersecurity

الكلمات المفتاحية: الجرائم السيبرانية، التقنيات الناشئة، الأمن السيبراني

Production and hosting by NAUSS

Email:coecdf@nauss.edu.sa

doi: 10.26735/EEOZ9233