Security Policy Papers
https://spp.nauss.edu.sa/index.php/spp
أوراق السياسات الأمنية
https://nauss.edu.sa/
جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
ورقة تحليل سياسات أمنية

سياسات التعاوُن الرقمي بين الأجهزة الأمنيَّة العربيَّة

Digital Cooperation Policies between Arab Security Agencies

عمار ياسر البابلي
باحث في أمن المعلومات
جمهورية مصر العربية

Amar Yaser Elbably
Researcher in Information Security
Arab Republic of Egypt

المخرجات الرئيسية:

- تبادُل المعلومات والبيانات داخل الأوعية المعلوماتيَّة المُستحدثة والمطلوب إنشاؤها عبر قنوات التعاون الدولي أمام الجرائم الدوليَّة، من خلال التطبيقات والبرامج التكنولوجيَّة المُؤَمَّنة.
- الفحص المبكِّر للمعلومات الدالَّة على وجود ارتباط خلايا إرهابيَّة أو مُنظَّمات إجراميَّة داخل الدول، من خلال التحقيقات المشتركة ودلائل المعلومات.
- توفير سُبل الاتصالات ونقل المعلومات بين أجهزة الشرطة العربيَّة بما يحقق السريَّة التامَّة.

المستخلص

يُسهِم التعاوُن الأمني الرقمي بين الدول إسهامًا كبيرًا في انحسار الجرائم المُنظَّمة والقضاء عليها، وبخاصَّةٍ الجرائم الإرهابيَّة، وهو ما يتطلَّب ضرورة تفاعُل الدول فيما بينها، وزيادة الجهود في سبيل تشجيع هذا التعاوُن وتفعيله، بإيجاد وسائل تعاونيَّة في المسائل الأمنيَّة الكفيلة بالوقاية من الجريمة وتَتَبُّع مرتكبيها حالَ وقوعها باستخدام شبكات مُؤَمَّنَة تسمح بنقل البيانات والمعلومات والتطبيقات بين الأجهزة المعنيَّة بأجهزة الشرطة العربيَّة، واستخدام التقنيات المؤَمَّنَة والسريعة التي تسمح بالتبادُل الرقمي للأجهزة الشرطيَّة، ما يحقِّق منع وقوع الجرائم والكشف عنها، وملاحقة المخطَّطات الإجراميَّة والإرهابيَّة بجميع أشكالها واستباق المعلومات بما يحافظ على الأمن الوطني للدول العربيَّة.

Abstract

Digital security cooperation between countries contributes significantly to the decline and elimination of organized crime, especially terrorist crimes, which requires the need for states to interact with each other and increase efforts to encourage and activate such cooperation, by creating cooperative means in security issues to prevent and track the perpetrators in the event of a crime using secure networks that allow the transfer of data, information and applications between the agencies concerned with the Arab police, and the use of secure and rapid technologies that allow the digital exchange of police agencies. In order to prevent and detect crimes, pursue criminal and terrorist schemes in all its forms and anticipate information in order to maintain the national security of Arab countries.

1- المُقدِّمة

يرتبط تاريخ المعلومة بتاريخ البشريَّة؛ حيث إن الإنسان الذي يملك المعلومة يصبح الأقوى، فالمعلومة مصدر القوة، وحجر الزاوية في مسيرة التطور، والتعاوُن الرقمي في مجال الأمن الجنائي الخارجي يهتم بالمعلومات التي لها علاقة بأي نشاط (إجرامي أو إرهابي) خارج الدولة، يمكن أن يهدد الأمن الداخلي للدولة (شفيق، 2019).

ولقد فرضت السياسات الرقميَّة وقضاياها بوضوح في الآونة الأخيرة - خصوصًا بعد أزمة فيروس «كورونا» - على العالم عمليَّة تحوُّل رقمي متسارع في قطاعات كثيرة، وبات التحوُّل الرقمي واقعًا تتعامل معه كل دول العالم مع التفاوت في القدرات والإمكانات، وجدير بالاعتبار الدور المهم الذي تؤدِّيه صناعة السياسات الرقميَّة وصياغاتها في عمليَّة صنع القرار الأمني وترشيده، ومن هنا تؤدِّي «الرقمنة» دورها المهم في عمليَّة ترشيد القرار وصناعته، في ظل عمليات التحوُّل التي يشهدها العالم في مجال الرقمنة (عبد الصادق، 2020).

وقد انتشرت تقنية المعلومات والاتصال عالميًّا بكثافة؛ حيث وصل عدد مستخدمي الإنترنت، بوصفه أحد المؤشرات، إلى نحو 4.57 مليار مستخدم، ما يمثِّل نحو 59% من سكان العالم. وبلغ عدد مستخدمي الهواتف نحو 5.15 مليار مستخدم، وعدد المستخدمين النشطين على الشبكات الاجتماعيَّة نحو 3.96 مليار مستخدم (عبد الصادق، 2020).

وتُعتبر تكنولوجيا الاتصالات والمعلومات Information & communication Technology (ICT) المحرِّك الرئيس للتغيير في المجتمعات في العصر الحاضر، وقد نقلت العالم من اقتصاد المعلومات إلى اقتصاد المعرفة؛ حيث إن تطوُّر تكنولوجيا الاتصالات والمعلومات وتعزيز استخدامها يعتبران حجر الزاوية للبنية الاقتصاديَّة؛ حيث إنَّ المعلومات هي المعنى الذي يُستخلص من البيانات، وتشمل مصادر المعلومات: الحاسبات الآليَّة ووسائل الاتصال وشبكة المعلومات والبيانات، التي يمكن تخزينها ومعالجتها واسترجاعها ونقلها بواسطة هذه الحاسبات، وجميع البرمجيَّات اللازمة لتشغيل هذه الأنظمة، أمَّا المعلوماتيَّة فهي التعامُل العقلاني، الذي يُدار بآلات أوتوماتيكيَّة، مع المعلومات باعتبارها دعامةً لقدرة الأجهزة الرقابيَّة، وأجهزة إنفاذ القانون، وسائر الأجهزة المختصَّة بمكافحة غسل الأموال والإرهاب والجريمة المُنظَّمة، أي: إن المعلومات هي بترول القرن (الجندي، 2014).

وتتمثَّل المشكلة البحثية في تعدُّد الجرائم وتطوُّرها من مجتمعٍ لآخر ومن دولةٍ لأخرى، مع التطوُّر السريع للتكنولوجيا واستخدام المحيط السيبراني في تنفيذ الجرائم والهجمات السيبرانيَّة، سواء على الجانب الإجرامي أو الإرهابي، ما أدَّى إلى عدم القدرة على مواجهة الإجرام الدولي بالوسائل الكفيلة لإحباط ذلك؛ لذلك فإنَّ الحاجة ماسة إلى تعزيز التبادُل الرقمي لمكافحة الجريمة، ومن هنا يلزم العمل على تأكيد تبادُل المعلومات بين سلطات الشرطة الجنائيَّة وتشجيعه، بالإضافة إلى سد الفجوة الرقميَّة بين الأجهزة الأمنيَّة العربيَّة؛ حيث إنَّ عمليَّة التعاوُن الرقمي بين الأجهزة والمؤسَّسات الأمنيَّة العربيَّة أمرٌ في

الشكل رقم (1): الخطوات الأولية للرقمنة الشرطية المتشتركة لرقمنة الشرطة[1]

غاية الصعوبة، وتقدِّم هذه الورقة حلولًا صائبة لزيادة حجم تبادُل المعلومات الأمني بهدف منع الجريمة (الموقع الرسمي لوزارة الاتصالات، 2016).

2- دواعي الاهتمام بالتعاوُن الدولي الأمني الرقمي في مكافحة الجرائم

يحقِّق التعاوُن الدولي في المجال الأمني، على ساحات مختلفة، عدَّة أهداف رئيسة تمثِّل في حقيقتها أوجهًا مستحدثة لهذا التعاوُن، وتزيد من قدر الحرص على ضرورة الوصول إليه، ويمكن القول: إن تلك الأهداف تمثل في حقيقتها غايات تسعى جميع المؤسَّسات الأمنيَّة في الدول العربيَّة إلى تحقيقها، وصولًا إلى أهداف مد جسور التعاوُن بين المؤسَّسات الأمنيَّة العربيَّة، وتحقيق الأمن العربي.

ولا يمكن لدولة بمفردها مكافحة الجريمة عبر الوطنيَّة بمعزِلٍ عن الآخرين؛ حيث يرتكز العمل الأساسي لجهاز الأمن على محور جوهري يتمثَّل في جمع المعلومات وتبادُلها مع أجهزة إنفاذ القانون الدوليَّة في المجالات المختلفة لمكافحة الجريمة العابرة للحدود الوطنيَّة؛ فهذا النوع من الجريمة يأخذ أبعادًا يتعدَّى نطاقها العمل التقليدي لأجهزة إنفاذ القانون، ولا بُدَّ من تطوير سياسات التعاون الرقمي بين الأجهزة الأمنيَّة العربيَّة للتصدِّي للتحديات المشتركة وتنسيق العمل فيما بينها لمطاردة التنظيمات الإرهابيَّة والإجراميَّة التي يتجاوز نشاطها حدود الدول.

بالإضافة إلى تنسيق الجهود لتبادُل المعلومات بين الدول والاستفادة من الأدوات الفنيَّة وتقنيات الذكاء الاصطناعي وسجلَّات المعلومات وأدوات تعقُّب خلايا الإرهاب التي تعمل من خلالها قبل وقوع الجريمة وبعدها، كما أنَّ تبادُل تطبيقات المعلومات الجنائيَّة من الأشياء المهمة التي تُعد مركزًا للمعلومات والتنسيق الدولي العربي الشرطي، ولا تستطيع أي دولة بمفردها القضاء على جريمة أو الحد منها، لا سيَّما إذا كانت عابرة للحدود يرتكبها أفراد أو جماعات مُنظَّمة في دولة معيَّنة ثم تنتقل إلى دولة أخرى، ما يقلِّل من فرص تعقُّبها وإلقاء القبض على مرتكبيها ومعاقبتهم.. ومن

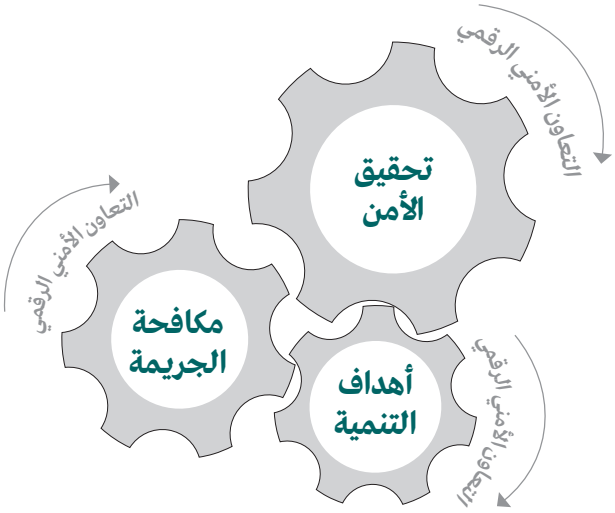
الشكل رقم «2»: تطور السياسات الرقمية بين الأجهزة الشرطية العربية

هنا تبرز أولويَّة الاهتمام بالتعاوُن الرقمي الأمني لتمكين أجهزة إنفاذ القانون في الدول من محاربة الجريمة بجميع سبلها والحفاظ على الأمن القومي العربي، في ظل استخدام التطوُّر التكنولوجي السريع وتقنيات الذكاء الاصطناعي (الامارات، 2020).

ويوضِّح الشكل التالي شكل رقم «1» الخطوات الأولوية نحو تطوير سياسات التعاون الرقمي بين الأجهزة الأمنية العربية.

كما يشير الشكل رقم «2»، الى تطوير السياسات الرقميَّة بين الأجهزة الشرطيَّة العربيَّة من خلال دمج التكنولوجيا وتبادُلها ونقل المعلومات المطلوبة وتبادُلها من خلال إستراتيجيَّة مشتركة، عن طريق نقل المعلومات عبر شبكات خاصَّة مُؤَمَّنَة وسريعة لحل ألغاز القضايا ومنع وقوع الجرائم بمختلف مستوياتها (الجنائيَّة أو الإرهابيَّة أو المُنظَّمة) وحماية الأمن العام بالدول؛ حيث إنَّ التحدي الذي يسود المنطقة العربيَّة والأفريقيَّة هو الإرهاب، فهو خطر يهدِّد العالم كله، وهو ليس فردًا أو فردين، بل تنظيمات تقف وراءها دولٌ تموِّلها لتحقيق مصالح وأهداف مشبوهة، وهناك علاقة طرديَّة بين الأمن والتنمية؛ حيث إنه لا يوجد تطوُّر وازدهار وتنمية دون تحقيق الأمن.

حيث إن العلاقة بين الأمن والاقتصاد تعد علاقة تواؤمية لا يمكن الفصل بينهما ولا يمكن لأحدهما البقاء دون الآخر فترة طويلة. غير أن الأمن يعد الأكثر أهمية فإذا انتكس الاقتصاد قد لا يؤدي إلى تدهور مباشر في الأمن، في حين إذا تدهور الأمن فسينتكس الاقتصاد كنتيجة مباشرة للتدهور الأمني. لهذا فإن الأولوية الأمنية لا يسبقها أولوية، وكلما زاد الاقتصاد نمواً وارتفع المستوى المعيشي للمواطن وزادت رفاهيته فإننا نصبح أكثر مديونية للقائمين على الأمن الذين



الشكل رقم «3»: دور التعاون الرقمي في تعزيز العلاقة بين الأمن واهداف التنمية المستدامة ومكافحة الجريمة (البابلي، 2021).

خلقوا لنا بيئة آمنة مستقرة مكنتنا من العطاء والإنتاج والإسهام في بناء الاقتصاد، كما يوضح الشكل رقم «3».

3- محاور تطوير سياسات التعاون الرقمي بين الأجهزة الأمنيَّة العربيَّة:

أولًا: جمع المعلومات المتعلِّقة بالإرهاب وتحليلها وتقييمها: ينبغي تحديد مستويات التهديد، وإصدار تحذيرات منها وتحليل المعلومات التي جُمِعت، والجمع بين خبرة الشرطة والإدارات والوكالات الحكوميَّة في مجال مكافحة الإرهاب، بحيث تُحلَّل المعلومات وتُعالَج على أساس مشترك، مع النظر إلى مشاركة الإنتربول واليوروبول بشأن تبادُل التطبيقات المستحدثة وتطبيقات البصمات الوراثيَّة (الأكاديمية الوطنية لمكافحة الفساد، 2019).

ثانيًا: تبادُل المعلومات الأمنيَّة: من المهم تعزيز تبادُل المعلومات التي تتعلَّق بأنشطة الجماعات الإرهابيَّة وجرائمها وقياداتها وعناصرها وأماكن تمركزها وتدريبها ووسائل تمويلها وتسليحها ومصادرهما ووسائل الاتصال والدعاية التي تستخدمها ووثائق السفر التي تستعملها، وتبادُل المعلومات والبيانات في مجالات الأمن المختلفة، وبخاصَّةٍ أنشطة الجماعات والمُنظَّمات الإرهابيَّة أو المعادية وجرائمها والجرائم المُنظَّمة وجرائم الاتِّجار والاستعمال غير المشروعين للمخدِّرات والمؤثِّرات العقليَّة ومرتكبيها (السعيد، 2013).

ثالثًا: إجراء التحريات: ينبغي تقديم المساعدة في مجال إجراءات التحرِّي والقبض على الهاربين من المتهمين أو المحكوم عليهم بجرائم إرهابيَّة.

رابعًا: تأمين سريَّة المعلومات وتطبيق سياسات تأمين المعلومات: ينبغي توفير الحماية الأمنيَّة لنقل البيانات والتطبيقات واستخدام نظم تشفير المعلومات وخدمات الجيل الخامس لنقل البيانات بسرعة فائقة.

الشكل رقم «4»: الجرائم في الفضاء السيبراني (البابلي، 2021)

4- أطر التعاوُن الأمني الرقمي المستهدف:

أ- نحو إستراتيجيَّة مشتركة لرقمنة الشرطة (Digital Policing)

لتبادُل المعلومات في التحقيقات المشتركة وجمع الاستدلالات، يتعيَّن على الدول العربيَّة النظر في إبرام اتفاقيَّات متعدِّدة الأطراف تُجيز للسلطات المختصَّة أن تنشئ هيئات تحقيق مشتركة، فيما يتعلَّق بالمسائل التي هي موضوع تحقيقات أو ملاحقات أو إجراءات قضائيَّة دوليَّة في دولة أو أكثر، وعلى الدول الأطراف المعنيَّة أن تكفل الاحترام التام لسيادة الدولة الطرف التي سيُجرى ذلك التحقيق داخل إقليمها، من خلال تبنِّي مختلف الأجهزة الشرطيَّة العربيَّة إستراتيجيَّةً مشتركةً للوصول إلى رؤية متقاربة حول المجالات التي ينبغي أن تسير فيها هذه المؤسَّسات الأمنيَّة على خطى متقاربة وتقديم المساعدة لتعميم إستراتيجيَّات إدارة الحدود وقدرات أجهزة مراقبة الحدود، وإنفاذ القانون، وإنشاء تطبيقات وبرمجيَّات وأنظمة لتبادُل المعلومات لمنع الاتجار بالمخدِّرات وسائر الجرائم ومكافحتها - مثل: الاتجار بالأسلحة الناريَّة وغير المشروعة، وغسل الأموال - وتعزيز قدرات أجهزة إنفاذ القانون والعدالة الجنائيَّة في علم الاستدلال الجنائي، المتعلِّقة بالمخدِّرات في جمع الأدلة الجنائيَّة وحفظها وعرضها، من أجل ملاحقة مرتكبي الجرائم المتعلقة بالمخدِّرات (خليفة، 2018).

ب- سُبل التعاوُن الرقمي (تبادُل المعلومات الرقميَّة)

إنَّ معظم الجرائم المستحدثة تقع في بحر الفضاء الإلكتروني، وتتبادل المُنظَّمات الإرهابيَّة والإجراميَّة التواصُلَ تحت غطاء المجال الإلكتروني، ما يصعِّب على الأجهزة الأمنيَّة تعقُّبها وتتبُّعها، كما يوضح الشكل رقم «4».

وفي حالة وجود تعاون رقمي أمني، فإنَّ سبل التحقيقات وتبادُل المعلومات وتتبُّع تلك العناصر واستيفاء المعلومات عنها.. ذلك كلّه سوف يُعزَّز.

وسيتناول الباحث سُبل التعاوُن الرقمي على النحو التالي:

رصد العناوين البريديَّة على الإنترنت	رصد أرقام حسابات البنوك الدوليَّة	حسابات شبكات التواصُل الاجتماعي
حساباتهم الخاصَّة على الإنترنت	الأقارب المشتبه بهم	الأسماء المستعارة والحركيَّة
التأشيرات السابقة وأماكن الإقامة	التنظيمات التي ينتمون إليها	علاقة المُنظَّمات بعضها ببعض ومصادر التمويل

جرائم الإرهاب وتمويل الجماعات الإرهابيَّة:

- تعزيز تبادُل المعلومات حول هُويَّة الأشخاص المشتبه بهم في تلك الجرائم وأماكن وجودهم وأنشطتهم السابقة، والوسائل والأساليب التي تُستخدم في ارتكاب تلك الجرائم، وحركة عائدات غسل الأموال وتمويل الإرهاب بالوسائل والتقنيات المستخدَمة في ارتكاب تلك الجرائم (Interpol, 2021).
- تبادُل المعلومات حول الأنشطة وجرائم الجماعات والمنُظَّمات الإرهابيَّة وعلاقتها المتبادَلة وقيادتها وعناصرها وهياكلها التنظيميَّة السريَّة وواجهتها العلنيَّة وأماكن تمركُزها ووسائل تمويلها وأساليب تدريبها والأسلحة التي تستخدمها، والمعلومات الرقميَّة بخصوص ما يلي:
- التعاوُن لتبادُل التحريات والمعلومات بشأن الجرائم التي حُدِّدت، للكشف عن هُويَّة الأشخاص الذين يُشتبه بتورطهم في هذه الجرائم وأماكن وجودهم وأنشطتهم، وحركة الأموال المتصلة بارتكاب هذه الجرائم.
- تبادُل تطبيقات وقواعد البيانات لجمع وتحليل المعلومات الخاصَّة بجرائم غسل الأموال وتمويل الإرهاب، بما في ذلك المعلومات المقدَّمة من الدول والمنُظَّمات الإقليميَّة والدوليَّة، ووضع قوائم متكاملة في هذا النطاق، والاحتفاظ بها وتحديثها، وتبادُل المعلومات مع الدول الأطراف في مجال جرائم غسل الأموال وتمويل الإرهاب (الأمم المتحدة، 2021).
- تطوير وتدعيم أساليب المراقبة وتبادُل المعلومات للكشف عن الخطط أو الأنشطة التي تهدف إلى نقل، أو استيراد، أو تصدير، أو تخزين، أو استخدام الأسلحة، أو الذخيرة، أو والمتفجرات وغيرها من المواد والوسائل الأخرى التي تساعد على ارتكاب الأعمال الإرهابيَّة عبر الحدود.

دور تبادُل المعلومات في مكافحة جريمة الفساد:

- التعاوُن بين سلطات إنفاذ القانون، وأن تتخذ كلُّ دولة طرف تدابير بتبادُل وتقديم معلومات مفيدة للسلطات المختصَّة لأغراض التحقيق والإثبات، وتبادُل السجلَّات الجنائيَّة لمرتكبي جرائم الفساد، بُغيةَ استخدام معلومات في إجراءات جنائيَّة تفيد في السيطرة على الدوائر الإجراميَّة والعصابات.
- التشاوُر مع الخبراء في تحليل اتجاهات الفساد السائدة، والظروف التي تُرتكب فيها جرائم الفساد، وتبادُل الإحصاءات والخبرة التحليليَّة بشأن الفساد، وكذلك التجارِب عن ممارسات منع الفساد ومكافحته (علي، 2020).
- تبادُل المعلومات عن الوسائل والأساليب التي تُستخدم لارتكاب جرائم فساد أو إخفائها، بما في ذلك الجرائم التي تُرتكب باستخدام التكنولوجيا الحديثة والكشف المبكر عنها، والتعاوُن على إجراء التحريات بشأن هُويَّة الأشخاص المشتبه بضلوعهم في جرائم فساد،

وأماكن وجودهم، وأنشطتهم، وحركات العائدات والممتلكات المتأتية من ارتكاب تلك الجرائم.

تبادُل المعلومات بين أجهزة إنفاذ القانون لضبط مرتكبي الجرائم

ينبغي تعزيز قنوات الاتصال من أجل تيسير تبادُل المعلومات عن الجرائم بأمان وبسرعة، بما فيها صلتها بالأنشطة الإجراميَّة الأخرى والجرائم ضد الأمن العام، وتبادُل المعلومات عن هُويَّة الأشخاص المشتبه بهم في تلك الجرائم وأماكن وجودهم وأنشطتهم أو أماكن الأشخاص المعنيين الآخرين، وحركة المُنظَّمات الإجراميَّة والأدوات المُستخدَمة في ارتكاب تلك الجرائم، وتوفير المواد لأغراض التحليل أو التحقيق، وتبادُل أدوات المساعدات الفنيَّة داخل أعمال التحقيقات والفيديوهات التوضيحيَّة داخل المعامل الجنائيَّة والفحص والتحليل (الوزان، 2014).

برنامج مراقبة الحاويات:

- أنشأ مكتبُ الأمم المتَّحدة المعنيّ بالمخدِّرات والجريمة ومنظَّمة الجمارك العالمية (United Nations Office on Drugs and crime) برنامج مراقبة الحاويات (CCP) سنة 2004، وقد ضمَّ أكثر من 30 وحدة لمراقبة الموانئ، ورفع كثيرًا من مستوى الكشف عن المخدِّرات وغيرها من السلع غير المشروعة ومصادرتها، وفي إطار برنامج مراقبة الحاويات بذل كلٌّ من مُنظَّمة الجمارك العالميَّة ومكتب الأمم المتَّحدة المعني بمكافحة المخدِّرات والجريمة جهودًا لإنشاء وحدات حديثة لمراقبة الموانئ واستخدام منصَّة التواصُل الخاصَّة بمُنظَّمة الجمارك العالميَّة (كونتيركوم) بوصفها أداةً لتبادُل المعلومات على الصعيد الدولي لجمع المعلومات من الوحدات التي أُنشِئت في إطار برنامج مراقبة الحاويات ومن خبراء آخرين في مراقبة الموانئ حول العالم (الحاويات، 2019).
- تبادُل وربط قواعد البيانات بالموانئ العربيَّة، من خلال منصَّات إلكترونيَّة سريعة ومُؤَمَّنة، ويجري تبادُل المعلومات المسجَّلة سابقًا بخصوص المخالفات والجرائم والأشخاص الذين ارتكبوا سابقًا جرائم تهريب متعدِّدة، سواء تهريب المخدِّرات أو الاتِّجار بالبشر أو المنوعات، إلى آخر الجرائم التي تضرُّ بالأمن

الحوادث الإرهابيَّة	القتل	الانتحار	الاغتصاب	دليل الإدانة أو البراءة في القضايا
التعرُّف إلى المفقودين	مسارح الجرائم	قضايا النسب	الجثث مجهولة الهُويَّة	

الفيروسات والبرامج الخبيثة	برمجيَّات انتزاع الفدية
برمجيَّات خبيثة لجمع البيانات	برمجيَّات البوتات الخبيثة
القرصنة لتعدين العملات المشفّرة	الشبكة الخفيَّة والإنترنت العميقة
الحوادث السيبرانيَّة السابقة	

القومي العربي، مع الإشارة إلى أهميَّة ربط قواعد البيانات تلك بالنظام الخاص للإنتربول واليوروبول؛ لأن طبيعة نقل الحاويات عبر الموانئ مسألة دوليَّة وليست مقتصرة على الدول العربيَّة.

الجرائم المُنظَّمة عبر الوطنيَّة

ينبغي تبادُل المعلومات والبيانات حول الجرائم المُنظَّمة عبر الوطنيَّة وقيادتها وعناصرها وهياكلها التنظيميَّة وأنشطتها وعلاقتها المتبادَلة، والخبرة المتعلِّقة بأساليب المكافحة ووسائلها، وكذا النُّظُم المتطوِّرة والمستحدثة لأجهزة المكافحة، واتخاذ الإجراءات المشتركة التي تكفل مواجهة مختلف الجرائم المُنظَّمة عبر الوطنيَّة، وبخاصَّةٍ جرائم الأموال وتهريبها وغسلها وتهريب القطع الأثريَّة والفنيَّة والاتجار غير المشروع في السيارات.

الإنتاج والاتِّجار والاستعمال غير المشروع للمخدِّرات والمواد المؤثِّرة في الحالة النفسيَّة:

- تبادُل المعلومات والبيانات بشأن جرائم الإنتاج والاتِّجار والاستعمال غير المشروع للمخدِّرات والمواد المؤثِّرة في الحالة النفسيَّة ومرتكبيها، وذلك طبقًا لقوانين كلِّ دولة، والخبرات المتعلِّقة بأساليب المكافحة ووسائلها، وكذا النُّظُم المتطوِّرة والمستحدثة لأجهزة المكافحة، وأحدث أساليب التحرِّي.
- إقامة أجهزة مراقبة والاحتفاظ بها في الموانئ الحرة والمطارات ونقاط التفتيش الواقعة على الحدود، مع تقديم المعلومات المفيدة لحكومات الدول المتورِّطة في تهريب المخدِّرات وزراعتها والاتجار بها (العربية، 2021).
- تبادُل المعلومات المتعلِّقة بالمخدِّرات عند الاقتضاء،

بين أجهزة إنفاذ القانون، ومراقبة الحدود، عبر قنواتٍ، منها: البوّابات الإلكترونيّة متعدِّدة الأطراف، ومراكز المعلومات، والشبكات الإقليميَّة التابعة لمكتب الأمم المتَّحدة المعني بالمخدِّرات والجريمة، وإجراء التحريات المشتركة، وتنسيق العمليات من أجل كشف وتعطيل وتفكيك الجماعات الإجراميَّة المُنظَّمة في إنتاج المخدِّرات والمؤثِّرات العقليَّة والتجارة غير المشروعة (عمران، 2021).

- تبادُل المعلومات والبيانات بشأن جرائم الإنتاج والاتِّجار والاستعمال غير المشروع للمخدِّرات والمؤثِّرات العقليَّة والأشخاص المتورطين فيها، والخبرات المتعلِّقة بأساليب ووسائل المكافحة وتطورها، وكذا النُّظُم المتطورة والمستخدمة لأجهزة المكافحة والمساعدات المتبادَلة في المسائل الميدانيَّة.
- تقديم المساعدات المتبادَلة في مجال إجراءات ضبط الأشخاص الهاربين المتهمين في قضايا أو المطلوبين في جرائم الاتِّجار بالمخدِّرات.

تبادُل قواعد بيانات سمات البصمة الوراثيَّة:

لتبادُل معلومات البصمات الوراثيَّة وسجلاتها دورٌ فعَّال في الكشف عن مرتكبي الجرائم؛ إذ يتيح تبادُلُ هذه المعلومات الربطَ بين سلاسل من الجرائم، أو تحديد وجود الشخص المشتبه به في مسرح الجريمة، كما أنَّ البصمة الوراثيَّة قد تساعد في إثبات براءة المشتبه به، وبخاصَّةٍ ملابسات ما يلي:

- أنشأت الشرطة الدوليَّة (الإنتربول) قاعدة معلومات وبيانات معروفة باسم «بوابة البصمة الوراثيَّة»، تضم هذه القاعدة أكثر من 150 ألف بصمة وراثيَّة من 73 بلدًا عضوًا، وبوسع أجهزة الشرطة تحليل قاعدة بيانات الإنتربول لاستخلاص مزيدٍ من المعلومات والدراسات والبحوث الجنائيَّة لتطوير آليَّات البحث وتحقيق النتائج السريعة في منظومة «DNA».
- البصمات الوراثيَّة هي مجرد قائمة أرقام تُحدَّد استنادًا إلى نماذج البصمة الوراثيَّة الخاصَّة بشخصٍ ما، وتعطي رمزًا رقميًّا يمكن استخدامه للتمييز بين الأشخاص، ولا تتضمَّن هذه البصمة أي معلومات عن البصمات البدنيَّة، أو النفسيَّة للشخص، أو أمراضه، أو قابليَّته لمرضٍ معيَّن.
- ربط قواعد البيانات تلك بأجهزة الشرطة بقواعد «DNA» بالنظام الخاص للإنتربول واليوروبول، وذلك فيما يتعلَّق بالقضايا الإرهابيَّة والاتجار بالبشر وتسلُّل المهرِّبين.

الجرائم السيبرانيَّة واختراق الأنظمة المعلوماتيَّة:

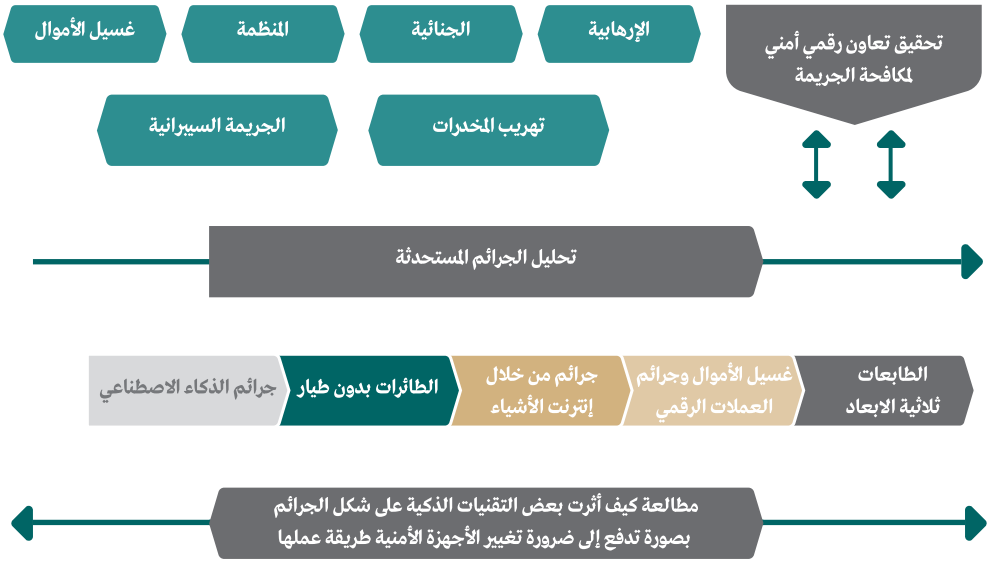
- في ضوء التطوُّر المستمر لظاهرة الجريمة السيبرانيَّة، يتعيَّن على أجهزة الشرطة العربيَّة تبادُل المعلومات والمعارف من أجل اتخاذ إجراءات آنية مستندة إلى المعلومات بشأن

تجميع الأدلَّة الجنائيَّة الرقميَّة وتبادُل بحوث التطوير.

- الاطلاع على سير البيانات من دولة لأخرى وبيانات تتبُّع بروتوكول الإنترنت (IP address).
- تبادل بيانات وسجلات الجريمة السيبرانيَّة بوصفها خدمة؛ إذ يستخدم المجرمون تقنيات جديدة لارتكاب هجمات سيبرانيَّة ضد الحكومات والشركات والأفراد، وهذه الجرائم لا تقف عند الحدود، سواء أكانت ماديَّة أم افتراضيَّة، وتسبِّب أضرارًا خطيرة وتشكِّل تهديدات ملموسة ضد الضحايا في جميع أنحاء العالم، ما يجعل تبادُل التكنولوجيا مهمًّا، وبخاصَّةٍ لأجهزة الشرطة المطلوب منها مكافحة الجرائم السيبرانيَّة، لفهم الإمكانات التي تتيحها للمجرمين وكيفيَّة استخدامها بوصفها أدواتٍ لمكافحة الجريمة السيبرانيَّة، وبخاصَّةٍ تغيُّر السلوكات والاتجاهات على الإنترنت واستغلالهما، في ظل وجود وباء «كوفيد - 19».
- تبادُل خبرات الأجهزة الأمنيَّة بسد الثغرات الأمنيَّة المرتبطة بإدارة المنظومات، التي قد يحاول المجرمون استغلالها؛ لجمع وتحليل المعلومات المتاحة عن الأنشطة الإجراميَّة المرتكَبة في الفضاء الرقمي، بهدف تزويد الدول بمعلومات استخباراتيَّة متسقة يمكن ترجمتها إلى تحرُّك عملي وتقني، وهنا يقع الهدف الأسمى من تبادُل المعلومات عبر أجهزة الشرطة العربيَّة، وهو:

حماية البنية التحتيَّة الإلكترونيَّة الحرجة من الاختراق الإلكتروني، وحماية المنشآت المهمَّة والحيويَّة من الهجمات السيبرانيَّة، وبخاصَّةٍ هجمات الحرمان من الخدمة Denial of Service (DoS).

- تبادُل المعارف المتصلة بالجريمة السيبرانيَّة بين أجهزة إنفاذ القانون والحكومات والمُنظَّمات الدوليَّة والخبراء من شركات الأمن السيبراني وتأمين المعلومات من أجل تبادُل معلومات ميدانيَّة غير شرطيَّة متعلِّقة بالجريمة السيبرانيَّة، من خلال التفاعُل المشترك لإتاحة الاتصالات والمشاركات للمستخدمين ليناقشوا مع زملاء مخوَّلين في الدول العربيَّة أحدث اتجاهات الجريمة السيبرانيَّة وإستراتيجيَّات الوقاية منها وتقنيات الكشف عنها وأساليب التحقيق فيها.
- تبادُل منصَّات الذكاء الاصطناعي للأمن السيبراني، حيث يُمكن للذكاء الاصطناعي معالجة أكثر من 100 تيرابايت من بيانات التهديد العالمي يوميًّا، بدءًا من المئات من استخبارات التهديد، لتحديد التهديدات الناشئة، ما يسمح للشرطة في الدول العربيَّة بمواءمة الدفاع ضدهم قبل أن يهاجموا.
- بوجود أكثر من 4,5 مليار نسمة على الإنترنت، يغدو أكثر من نصف البشريَّة مُعرَّضًا في كل لحظة لخطر الوقوع ضحيةً للجرائم السيبرانيَّة، الأمر الذي يستدعي التعاوُن الرقمي بين أجهزة الشرطة في الدول العربيَّة، مع إتاحة الشراكة والتعاوُن مع شركات الأمن



الشكل رقم «5»: التعاون الرقمي الأمني في مكافحة الجريمة (البابلي، 2021)

السيبراني؛ حيث تشكِّل الجرائم السيبرانيَّة أحد أكثر أشكال الجريمة الدوليَّة انتشارًا؛ إذ يُقدَّر أنها ستسبِّب للاقتصاد العالمي خسائر تبلغ 10,5 تريليون دولار أمريكي سنويًّا من الآن وحتى عام 2025 (Morgan, 2021).

- تعزيز الكفاءات والمعارف والقدرات التقنية في المجال السيبراني، من برامج تدريبيَّة ومشاريع وأدوات ومنصَّات بناء القدرات وأمن المعلومات والاتصالات، لتتيح للشرطة في الدول العربيَّة مكافحة الجريمة السيبرانيَّة بفعالية.
- تبادُل قواعد بيانات إدارة الأدلَّة الرقميَّة لأغراض التحقيقات والملاحقات القضائيَّة، لجمع القرائن الرقميَّة وَفقًا للقانون، وحفظ الأدلَّة وعرضها عرضًا مفهومًا ومقبولًا لدى المحاكم.
- تبادُل أدوات الربط بين المعلومات السيبرانيَّة والمعلومات الفعليَّة من خلال العثور على العلاقة القائمة بين الآثار الرقميَّة والمعلومات الفعليَّة؛ ليتسنَّى تحديد مكان مرتكبي الجرائم السيبرانيَّة.
- خدمات التعاوُن في مجال مكافحة الجريمة السيبرانيَّة بتفعيل دور التدريب المشترك بين الأجهزة الشرطيَّة العربيَّة على مستوى التحقيقات وطرق الفحص الفني وأدواته واستخراج الدليل الرقمي الإلكتروني وتبادُل المعلومات بشأن الهندسة الاجتماعيَّة وأخطارها وأضرارها على المواطنين والشركات

والبنوك (شفيق، 2019).

- تبادُل المعلومات المتوافرة عن أي جريمة من جرائم غسل الأموال، على أن يُوضَّح ما أحاط بالجريمة من ظروفٍ والجناة فيها، والمجني عليهم، وضحاياها، والآثار الناجمة عنها، والأساليب المستخدَمة في ارتكابها، التي تَستخدم الفضاء السيبراني والإنترنت والـ«ديب ويب» ستارًا لها؛ حيث تتمكَّن الأجهزة الأمنيَّة من تبادُل العناوين البريديَّة وتعقُّب «البروفايلات» و«الأكونتات» الخاصَّة بمرتكبي تلك الجرائم، مستخدمةً في ذلك أدوات الدليل الرقمي الإلكتروني وبرامج الفحص والتتبُّع عبر الشبكات، ومتابعة تحرُّكات الأثر الجنائي الرقمي داخل المجال السيبراني وتحديد أماكن الخطر والتجمُّعات والمُنظَّمات الإرهابيَّة وأنشطتهم على شبكات التواصل الاجتماعي.
- للتعاوُن الأمني الرقمي داخل مجال الفضاء السيبراني، تنبغي المشاركة بين شركات الاتصالات وشركات التكنولوجيا العملاقة والقطاعات المعنيَّة بالمجال السيبراني داخل أجهزة الشرطة العربيَّة والاتحاد الدولي للاتصالات؛ لتفعيل مجال البحث وتتبُّع مكافحة الجريمة التي يستخدم فيها المجرمون الفضاء السيبراني لارتكاب أفعالهم غير المشروعة (كامل، 2011).
- وضع معايير مشتركة لأدوات التحليل الجنائي الرقمي لجمع أدلَّة الإنترنت المظلمة على أجهزة الحاسبات الآليَّة.

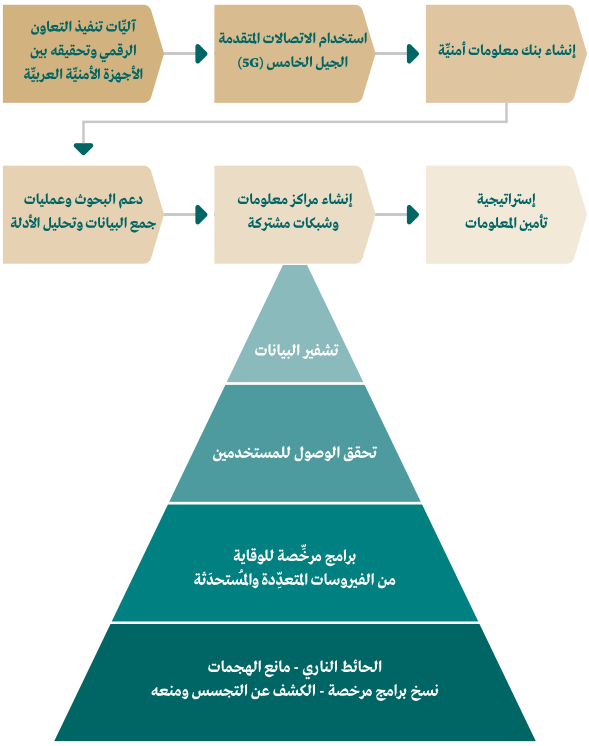
ويشير الشكل رقم «4» الى الأهمية الأمنية للتعاون الرقمي الأمني في مكافحة الجريمة:

5- آليَّات تنفيذ التعاوُن الرقمي وتحقيقه بين الأجهزة الأمنيَّة العربيَّة:

- إنشاء مركز معلومات دولي لمكافحة الإرهاب، لتطوير طرق تبادُل المعلومات، وجَمع البيانات الكاملة عن المنتمين إلى جماعات إرهابيَّة أو المشتبَه بهم، ووسائل تجنيد الإرهابيين، وأماكن تدريبهم، ومصادر التمويل، وأنواع الذخائر المستخدَمة، وتحليل المعلومات، والتنبُّؤ بأهداف العمليات، وتعزيز التعاوُن بين الأجهزة المتخصِّصة بالبيانات (السعد، 2020)، ويتبادل هذا المركز المعلومات من خلال ما يلي:
- إنشاء شبكة افتراضيَّة من أجل تبادُل المعلومات بهدف تقوية العمل الشرطي، لتعزيز مكافحة الإرهاب؛ حيث أصبح ضروريًّا أن تتواصل الأجهزة الأمنيَّة العربيَّة تواصلًا أكثر فاعليَّة.
- إنشاء بنك معلومات أمنيَّة لرصد جميع البيانات المتعلِّقة بالتنظيمات الإرهابيَّة الخطِرة ذات السِّمة الدوليَّة، ودعم الثقة باستدعاء المعلومة، وسرعة معرفة كل ما يتعلَّق بالأنشطة الإرهابيَّة، واعتماد بنك معلومات خاص بالمقاتلين الأجانب؛ حيث نتطلع إلى توسيع دائرة التعاوُن الرقمي ليصل إلى دول الاتحاد الأوروبي، وبخاصَّةٍ

الشرطة الأوروبيَّة (اليوروبول)، وما زال كثيرٌ من الشباب الأوروبي متأثِّرين بالفكر المتطرِّف، وربما يتحوَّلون إلى ذئاب منفردة تنفِّذ هجمات إرهابيَّة في أي وقت، ولا يمكن توقُّعها أو منعها.

- التنسيق والتعاوُن بين المؤسَّسات الأمنيَّة المتعدِّدة في الساحات الأمنيَّة العربيَّة بما يحقِّق في النهاية خفض معدلات الجريمة، مع استكمال نقص المعلومات الأمنيَّة، وذلك بالتعاوُن الدولي الرقمي لتجميع المعلومات الأمنيَّة وتبادُلها على المستوى العربي، والعمل دائمًا على استحداث قواعد المعلومات والبيانات لمكافحة الجرائم الدوليَّة، للكشف عن المخططات الإرهابيَّة والجريمة المُنظَّمة.
- إتاحة الفرصة لتدارُس الثغرات الأمنيَّة عبر الوطنيَّة، والعمل على توفير أفضل سُبل التصدِّي لها، منعًا للجريمة الإرهابيَّة ولضبط مرتكبيها.
- تشجيع التبادُل الفوري للمعلومات بين أجهزة إنفاذ القانون والنيابة العامة والوحدات الماليَّة ذات الصلة، وتوفير المعلومات الإحصائيَّة والتحليلات المتعلِّقة بزراعة المخدِّرات وإنتاجها وصنعها والاتِّجار بها بصورة غير مشروعة وغسل الأموال؛ لأغراضٍ، منها: تجسيد تلك المعلومات وتحليلها من أجل تعزيز التدابير التي تتخذها أجهزة العدالة الجنائيَّة في هذا الشأن.
- تعزيز تبادُل المعلومات الاستباقيَّة والتنسيق بين المؤسَّسات الماليَّة ووكالات إنفاذ القانون والاستخبارات والهيئات القضائيَّة من خلال منصَّة استخبارات عربيَّة، والتنسيق مع وكالة الشرطة الدوليَّة (الإنتربول)، بما في ذلك قاعدة لبيانات المعاملات المشبوهة.
- فرض إجراءات مشدَّدة واتباع شروط جديدة لاستخدام بطاقات الهاتف مدفوعة الثمن، بعد أن كان شراء هذه البطاقات دون أوراق رسميَّة، مع إدراجها بقواعد بيانات السجلَّات المدنيَّة والأحوال المدنيَّة، وإدراج بيانات الاستدلال الرقمي إلزاميًّا، مثل بصمة الأصابع، في بطاقات الهُويَّة الوطنيَّة.
- دعم البحوث وعمليات جمع البيانات وتحليل الأدلَّة وتبادُل المعلومات وتدعيم التدابير التي تتخذها أجهزة إنفاذ القانون والعدالة الجنائيَّة وسن القوانين، وذلك بتوطيد التعاوُن الدولي من أجل منع ومكافحة الأنشطة الإجراميَّة المتصلة بالمخدِّرات، التي تُستخدم فيها الإنترنت، بما يتوافق مع أحكام القانون المنطبقة ذات الصلة (السعد، 2020).
- استخدام الاتصالات المتقدمة - الجيل الخامس (G5) - فهي الثورة التكنولوجيَّة التالية في النطاق العريض النقَّال، التي ستُمكِّن تبادُلَ المعلومات بين أجهزة الشرطة في الدول العربيَّة من البحث السريع عن المعلومات، مع التمتُّع بسرعات تنزيل وتحميل أكبر كثيرًا، مع مستوى كمون منخفض، ما يعني تخفيض



الشكل رقم «6»: آليات تنفيذ التعاون الرقمي وتحقيقه (البابلي، 2021)

الوقت الذي تستغرقه الأجهزة للاتصال بالشبكات اللاسلكيَّة تخفيضًا كبيرًا، وتوفر شبكة G5 سرعات بيانات أكبر بشكل ملحوظ؛ حيث قد تصل معدلات ذروة البيانات إلى 20 جيجابت في الثانية (البابلي، 2018).

- تأمين شبكات المعلومات والاتصالات (الأمن السيبراني) والحفاظ على سرية المعلومات، من خلال تطبيق إستراتيجيَّة الأمن الإلكتروني وَفقًا لمعايير جودة أمن المعلومات طبقًا لجودة تأمين المعلومات لمعيار أيزو «آي إي سي 27001»؛ حيث إنها مجموعة القدرات المعلوماتيَّة التي تستخدمها المؤسَّسات للحماية من الهجمات السيبرانيَّة وصدِّها، وتُوصف بأنها مجموعة الوسائل الفنيَّة وغير الفنيَّة التي تسمح بالدفاع عن نُظُم المعلومات الحرجة في الفضاء الإلكتروني، وجميع الأدوات اللازمة لتحقيق الأمن الإلكتروني بكل السبل للمحافظة على البنية التحتيَّة المعلوماتيَّة، الأمر اللازم تطبيقه عند إنشاء وتفعيل الشبكات المعلوماتيَّة الناقلة للبيانات والتطبيقات والشبكات

الافتراضيَّة من أجل تبادُل المعلومات لحمايتها من الاختراقات الإلكترونيَّة وعمليات القرصنة، وفيما يلي يستعرض الباحث أهم النقاط الفنيَّة الأمنيَّة اللازمة لتحقيق الأمن السيبراني وتأمين الشبكات ونقل المعلومات بين أجهزة الشرطة العربيَّة:

أنظمة حماية الاختراقات:

توفِّر تقنية المعلومات وسائل متنوعة لحماية الشبكات، من أهمها: جدران الحماية (Firewalls)، التي لديها خصائص متعددة، وتتضمَّن تصفية البريد الإلكتروني الدعائي (Spam)، وإمكانات الحماية من الفيروسات، والكشف عن التجسُّس ومنعه (IDS/IPS)، وتصفية محتوى صفحات الويب، بالإضافة إلى مهام جدران الحماية التقليدية (البابلي، 2018(.

أجهزة إدارة التهديدات الموحدة (UTM): عُرِفت جدران الحماية التقليدية بالمصافي، ولقد تطوَّرت أخيرًا لتصبح أجهزة حماية متعددة الخصائص (UTM) (إدارة التهديدات الموحدة)، ومن المناسب تشغيل جدارين معًا، أحدهما رئيس والآخر احتياطي؛ فعند تعطُّل الأول يعمل الثاني مكانه، ويوجد في أنظمة تشغيل جدران الحماية تعليمات يجب إعدادها بعناية، لتحديد الوقت الذي يجب أن ينتظره الجدار الاحتياطي حتى يتسلَّم العمل.

أنظمة صلاحيات المستخدمين والهُويَّة:

التقنيات والتجهيزات، أو مزيج منهما، حتى تستخدمها المُنظَّمة للتأكُّد من صحَّة هُويَّة طالب الدخول (المستخدم) والسماح فقط للمسموح لهم بالدخول إلى موارد الشبكة.

تركيب أنظمة مراقبة تلفزيونيَّة ذكيَّة حديثة في جميع منشآت الحاسب الآلي، مع التركيز على غرفة الأجهزة والاتصالات مع أنظمة التعرُّف إلى الوجه.

تعزيز استخدام البصمات البارومترية داخل مراكز المعلومات والأنظمة الحساسة ولتسجيل المتعاملين مع شبكات الربط بين أجهزة الشرطة في الدول العربيَّة، للوصول المصرح به إلى الأجهزة والأنظمة وقواعد البيانات، لتجنُّب سرقة الهُويَّة أو فقدان بيانات حساسة أو سوء استخدامها.

أنظمة التشغيل وأمن الأجهزة:

- التحديثات (Updates): تحديث أنظمة التشغيل لأجهزة الخادم والحاسبات وأجهزة الشبكة كالموزِّعات والموجِّهات والنقاط اللاسلكيَّة والبرمجيَّات، لمنع استغلال مَواطن الضعف الناتجة عن عدم التحديث.
- ينبغي اتخاذ تدابير كثيرة لحماية أنظمة التشغيل والتطبيقات البرمجيَّة من أخطار التعطُّل الناتجة عن الثغرات الأمنيَّة والأخطاء التصنيعيَّة بتثبيت التحديثات التصحيحيَّة والأمنيَّة التي تُصدرها الشركات الصانعة، وذلك بتخصيص بيئة مشابهة لبيئة الإنتاج

لتجربة التحديثات قبل تثبيت تلك التحديثات في بيئة الإنتاج (الهيئة الوطنيَّة للأمن السيبراني، 2018).

أنظمة تشفير المعلومات:

- الغرض من تشفير المعلومات (encryption) هو حماية سريَّة المعلومات الرقميَّة، تُشفَّر البيانات أو النص العاديّ باستخدام خوارزميَّة تشفير ومفتاح تشفير، ينتج عن العمليَّة نصٌّ مشفَّر، يمكن عرضه فقط في شكله الأصلي، إذا فُكَّ تشفيره باستخدام المفتاح الصحيح.
- ينبغي اتخاذ تدابير عديدة لحماية أنظمة التشغيل والتطبيقات البرمجية من أخطار التعطل الناتجة عن الثغرات الأمنية والأخطاء التصنيعية بتثبيت التحديثات التصحيحية والأمنية التي تصدرها الشركات الصانعة، وذلك بتخصيص بيئة مشابهة لبيئة الإنتاج لتجربة التحديثات قبل القيام بتثبيت تلك التحديثات في بيئة الإنتاج (الأكاديمية الوطنية لمكافحة الفساد، 2019).

ويشير الشكل رقم «6»، الى آليات التعاون الرقمي بين الأجهزة الأمنية:

6- الخاتمة

- يكافح المجتمع الدولي من أجل تحوُّل التكنولوجيا التناظريَّة إلى رقميَّة بصورة أشمل وأقوى من أي وقت سابق، ما يعْقِد الأمل في ازدهار التكنولوجيا وتجنُّب أخطار ليس لها حد، قد تقع إذا لم تُتَّخَذ جميع التدابير والإجراءات التي من شأنها الوصول إلى الغاية المنشودة، فعلى الرغم من المميزات التي تنتج عن التقدُّم التكنولوجي الرقمي فإنَّه يشوبه بعض التحديات؛ نظرًا لاتساع الفجوات الرقميَّة والتهديدات الإلكترونيَّة وانتهاكات حقوق الإنسان على الإنترنت؛ لهذا كان لزامًا على الأمم المتَّحدة خلق نوع من أنواع التعاوُن الدولي الرقمي؛ ليصير المجتمعُ مجتمعًا دوليًّا رقميًّا أكثر سلامًا واستقرارًا، طريقه مضاء نحو مستقبل مشرق ومزدهر.
- ويكتسب التعاوُن الأمني الرقمي الدولي أهمية بالغة في مكافحة الجريمة المنُظَّمة العابرة للحدود؛ نظرًا لطبيعة هذه الجريمة وخصوصيَّتها، إضافةً إلى اعتبارها من أخطر النُّظُم الإجراميَّة الحديثة؛ لِما يترتَّب عليها من أضرار وخيمة تمسُّ جميع مناحي المجتمع الدولي والوطني على حدٍّ سواء، وفي ظلِّ المتغيرات التي يشهدها العالم، فإنه لا يمكن لأي دولة، مهما بلغ تقدُّمها وقوتها أن تواجه ظاهرة الإجرام بمفردها؛ وذلك لاتساع نطاق الجرائم وامتداده عبر الدول.
- كما يؤدِّي التعاوُن الأمني الرقمي الدولي إلى تبادُل الخبرات فيما بين الأجهزة الأمنيَّة العربيَّة، وذلك في أوسع نطاق، ما يؤدِّي إلى رفع كفاءة هذه الأجهزة لتكون قادرة على ردع الجماعات الإجراميَّة المنُظَّمة؛ لأن هذا التعاوُن

الرقمي يوفِّر معلومات وبيانات تعجز عن توفيرها الدولة الواحدة منفردة، ما يساعد على الكشف عن أعضاء الجماعات الإجراميَّة والإرهابيَّة والسيبرانيَّة، فالطابع العابر للحدود لهذه الجريمة يفرض وجود قنوات واسعة ومستمرة، وبخاصَّةٍ على مستوى جمع المعلومات والاستعلامات.

7- التوصيات:

- يمكن استخدام الذكاء الاصطناعي للكشف عن التهديدات وغيرها من الأنشطة الضارَّة المحتمَلة، ولا يمكن للأنظمة التقليديَّة مواكبة العدد الهائل من البرامج الضارَّة التي تُنشَأ، حيث يتدخَّل الذكاء الاصطناعي ويعالِج هذه المشكلة، وتعلِّم شركاتُ الأمن السيبراني أنظمةَ الذكاء الاصطناعي للكشف عن الفيروسات والبرامج الضارَّة باستخدام خوارزميَّات معقَّدة حتى يتمكَّن الذكاء الاصطناعي من تشغيل التعرُّف إلى الأنماط في البرامج، وتُدرِّب أنظمة الذكاء الاصطناعي على تحديد حتى أصغر سلوكات هجمات الفدية والبرمجيَّات الخبيثة قبل أن تدخل النظام، ثم تعزلها عن هذا النظام، ويمكنها أيضًا استخدام الوظائف التنبُّئِيَّة التي تتجاوز سرعة الأساليب التقليديَّة.
- تشجيع توفير المنافع الرقميَّة والاستثمار فيها، مثل: البرمجيَّات، والبيانات، ونماذج الذكاء الاصطناعي، والإسهام في تحقيق أهداف التنمية الأمنيَّة المستدامة.
- إضافة بصمة «DNA» وبصمة الوجه والعينين على قاعدة بيانات بطاقة الرقم القومي، بهدف سهولة التعرُّف إلى هُويَّة الأشخاص في أي مكان دون إيقافهم، وإبراز تحقيق شخصيَّتهم وسهولة تحديد أماكن الأشخاص المطلوبين أمنيًّا.
- الارتقاء بالمنافع العامَّة الرقميَّة من أجل تهيئة عالم أكثر إنصافًا، وكفالة الشمول الرقمي للجميع، بما في ذلك أكثر الفئات ضعفًا، وتعزيز بناء القدرات الرقميَّة، ودعم التعاوُن الدولي العالمي في مجال الذكاء الاصطناعي، مع الارتقاء بالثقة والأمن في البيئة.
- تنظيم اللقاءات والمؤتمرات العلميَّة المتخصِّصة لدعم هذا التعاوُن، لتعزيز العلاقات والتعاوُن الدولي وتبادُل الخبرات وأفضل الممارسات والمشورة في مجالات تعزيز الأمن والسِّلم العالميين.

المراجع العربية:

الأكاديميَّة الوطنيَّة لمكافحة الفساد. (2019). الإستراتيجيَّة المصرية الثانية لمكافحة الفساد (2018 - 2021). إستراتيجيَّات مكافحة الفساد، القاهرة.

الأمارات، ح. د. (2020). السلامة السيبرانية والأمن الرقمي. دبي: حكومة دولة الأمارات..https://u ae/ar-ae/information-and-services/ justice-safety-and-the-law/cyber-

safety-and-digital-security.

الأمم المتحدة، م.م. (نوفمبر، 2021). تبادل المعلومات. متاح على الرابط التالي: https://www.gcc-sg.org/ar-sa/CooperationAndAchievements/Achievements/SecurityCooperation/Achievements/Pages/Seventhcooperationinthefightag.aspx.

البابلي، عمار ياسر. (2018). الآليَّات الحديثة لحماية وتأمين نُظُم المعلومات وآثارها على المنظومة الأمنيَّة. رسالة دكتوراه. أكاديميَّة الشرطة، كليَّة الدراسات العليا. القاهرة. ص 204.

الجندي، م. (2014, ديسمبر). البيانات الضخمة بترول قرن ال 21. القاهرة: مجلة لغة العصر.

الحاويات، ب.م. (2019). مكتب الأمم المتحدة المعني بمكافحة المخدرات والجريمة.

خليفة، إيهاب. (2018). تنامي التهديدات السيبرانيَّة للمؤسَّسات العسكريَّة. اتجاهات الأحداث. مركز المستقبل للأبحاث والدراسات المتقدّمة، أبو ظبي، الإمارات العربيَّة المتُّحدة. العدد 22. متاح على: https://futureuae.com/ar/Activity/Item/.

السعد، صالح. (2020). محفِّزات التعاوُن الدَّولي في محاربة الإرهاب، التحالف الإسلامي العسكري لمحاربة الإرهاب، متاح على: https://www.imctc.org/ar/Pages/default.aspx.

السعيد، أحمد. (2013). تكنولوجيا المعلومات في المجال الأمني. دار النهضة العربيَّة. القاهرة.

شفيق، نوران. (2019). أشكال التهديدات الإلكترونيَّة ومصادرها. دراسات مكافحة الإرهاب. المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات. برلين، ألمانيا.

عبد الصادق عادل (2020). مُنظَّمة التعاوُن الرقمي: آليَّة جديدة نحو التنمية المستدامة. مركز الأهرام للدراسات السياسيَّة والإستراتيجيَّة. القاهرة. متاح على: https://acpss.ahram.org.eg/News/17017.aspx

العربية، 1. (2021). التعاون في مجال مكافحة المخدرات. متاح على الرابط التالي: https://www.gccsg.org/arsa/CooperationAndAchievements/Achievements/SecurityCooperation/Achievements/Pages/Seventhcooperationinthefightag.aspx

علي، معتز عبد الرحمن. (2020). دور التبادُل الدولي للمعلومات في الإثبات الجنائي: دراسة مقارنة. رسالة دكتوراه. أكاديميَّة الشرطة، كلية الدراسات العليا. القاهرة. ص 33.

عمران، أ. (2021). توصيات الجلسة الختامية للمؤتمر العربي 34 لرؤساء أجهزة مكافحة المخدرات. متاح على الرابط التالي: https://gate.ahram.org.eg

كامل، شريف سيد. (2011). الجريمة المُنظَّمة. دار النهضة العربيَّة. القاهرة.

الموقع الرسمي لوزارة الاتصالات. (2016). مركز

المعلومات. متاح على الرابط التالي: https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

الوزان، السيد حلمي. (2014). سلطة المعلومات: رؤية أمنيَّة معاصرة. دار النهضة العربيَّة. القاهرة.

الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبراني. متاح على: https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

المراجع الإنجليزية:

INTERPOL. (2021). report identifies top cyberthreats in Africa https://www.interpol.int/a. 33

Morgan, Steve. (2021). 2021 report: cyberwarfare in the C-suite. Cybersecurity Ventures. Available at: https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

Received 09 Sep. 2021; Accepted 20 Oct. 2021; Available Online 31 Dec. 2021.

الكلمات المفتاحية: دراسات أمنية، الأمن المعلوماتي، التعاون الرقمي، تبادل المعلومات، سياسات التعاون.

Keywords: Security Studies, Information Security, Digital Cooperation, Information Exchange, Cooperation Policies

Production and hosting by NAUSS

* Corresponding Author: Amar Yaser Elbably
Email: 3marelbably@gmail.com
doi: 10.26735/HJOO8882