تقرير وتوصيات الاجتماع الثالث لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات

الجمهورية التونسية

(١٢-٢٠٢٣/٧/١٣م)

إعداد:

الأمانة الفنية لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات

****

التقرير

تنفيذًا للتوصية سابعًا من توصيات الاجتماع الثاني لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات المنعقد بتاريخ ٢١-٢٢/١١/٢٠٢٢م في مقر جامعة الدول العربية (القاهرة)؛ التي نصت على " عقد الاجتماع القادم للفريق في مقر الأمانة العامة لمجلس وزراء الداخلية العرب – تونس- خلال الربع الثاني من عام ٢٠٢٣م، والطلب من الأمانة الفنية للفريق التنسيق في ذلك مع الجهات ذات الصلة" وبناءً عليه قامت الأمانة العامة للمجلس بالتنسيق وتوجيه الدعوة للدول الأعضاء ومؤسسات العمل العربي المشترك لحضور الاجتماع خلال الفترة (١٢-١٣/٧/٢٠٢٣م) بموجب التعميم رقم ٥١١ وتاريخ ٨/٥/٢٠٢٣م ، وتم عقد الاجتماع بحضور وفود تمثل الدول الأعضاء الآتية:

المملكة الأردنية الهاشمية، دولة الإمارات العربية المتحدة، مملكة البحرين، الجمهورية التونسية، الجمهورية الجزائرية الديمقراطية الشعبية، المملكة العربية السعودية، جمهورية العراق، سلطنة عمان، دولة فلسطين، دولة قطر، جمهورية القمر المتحدة، دولة الكويت، دولة ليبيا، جمهورية مصر العربية، المملكة المغربية، والجمهورية الاسلامية الموريتانية. كما حضر كذلك ممثلون عن الأمانة العامة لمجلس وزراء الداخلية العرب وجامعة نايف العربية للعلوم الأمنية، وعدد من مؤسسات العمل العربي المشترك **(مرفق قائمة بأسماء المشاركين).**

وقد تضمن جدول أعمال الاجتماع البنود الآتية:

١. نتائج تطبيق توصيات الاجتماع الثاني للفريق.
٢. تجارب الدول الأعضاء في مواجهة جرائم تقنية المعلومات.
٣. التحديات الناشئة في مجال جرائم تقنية المعلومات.
٤. مخاطر الابتزاز الإلكتروني.
٥. تصور مقترح لإعداد آلية دورية لاستعراض ومراجعة تنفيذ ما ورد بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
٦. ما يستجد من أعمال.

٧. توصيات الاجتماع.

وفي الساعة العاشرة من صباح يوم الأربعاء ٢٠٢٣/٧/١٢م، افتتح سعادة الأمين العام المساعد لمجلس وزراء الداخلية العرب د/ عبدالله بن أحمد الشعلان، أعمال الاجتماع الثالث لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات بكلمة رحّب في مستهلها بالسادة المشاركين وناقلًا تحيات معالي الأمين العام لمجلس وزراء الداخلية العرب معالي د/ محمد بن علي كومان، موضحًا أهمية هذا الفريق لما يترتب على التقنيات الحديثة والتحول الرقمي من أنماط وأساليب إجرامية مستجدة؛ الأمر الذي يتطلب توحيد الجهود ودعم العمل العربي المشترك لمواجهة تلك الأنماط والجرائم، والارتقاء بمنظومة العمل وتطوير الآليات والوسائل المعتمدة وتعزيز التعاون بين مختلف الهيئات والمنظمات الإقليمية والدولية والتركيز على حوكمة شاملة للمنظومة الأمنية وتكريس مقومات دولة القانون والمؤسسات واحترام حقوق الإنسان، معربًا عن أمله وتمنياته بنجاح أعمال هذا الاجتماع والخروج بتوصيات بنّاءة تصب في مصلحة تعزيز العمل الأمني العربي المشترك.

تلا ذلك كلمة لسعادة العقيد/ أكثم عبدالمجيد النمورة (رئيس وفد دولة فلسطين) نقل فيها تحيات معالي السيد وزير الداخلية الفلسطيني رئيس الدورة الأربعين لمجلس وزراء الداخلية العرب، متقدمًا بالشكر الجزيل إلى الجمهورية التونسية حكومةً وشعبًا على حسن الوفادة وكرم الضيافة، وإلى الأمانة العامة لمجلس وزراء الداخلية العرب، على جهودها الحثيثة والعمل الدؤوب في تطوير العمل الأمني العربي المشترك؛ مفتتحًا جلسات أعمال الاجتماع والمواضيع المدرجة ضمن بنوده.

البند الأول

نتائج تطبيق توصيات الاجتماع الثاني للفريق

تضمن هذا البند استعراضًا لتقرير تنفيذ توصيات الاجتماع الثاني للفريق على النحو الآتي:

التوصية أولًا/ ج:

نص التوصية" الطلب من الأمانة الفنية للفريق الاستمرار باستطلاع آراء الدول الأعضاء بشأن تعريف جرائم تقنية المعلومات، على أن تقوم في ضوئها بإعداد مشروع تعريف موحد وعرضه على أعمال اجتماع مقبل للفريق"

الإجراءات

قامت الأمانة الفنية للفريق المتمثلة في المكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات بمخاطبة شعب الاتصال في الدول الأعضاء بالخطاب رقم ١٠٠ وتاريخ ٢٠٢٣/٣/٢٨م، والخطاب الإلحاقي رقم ١٩٣ وتاريخ ٢٠٢٣/٦/٥م بشأن ما تضمنته التوصية تمهيدًا لوضع تعريف موحد لجرائم تقنية المعلومات.

النتائج

تلقى المكتب إجابات الدول الآتية: (المملكة الأردنية الهاشمية - المملكة العربية السعودية – جمهورية العراق - دولة فلسطين - دولة الكويت – الجمهورية اللبنانية)

الأردن: أفادت أن مفاهيم جرائم تقنية المعلومات تتناول الأنشطة غير القانونية التي تستهدف الأنظمة الحاسوبية والشبكات والبيانات وتشمل هذه الجرائم اختراق الأنظمة والاحتيال الإلكتروني وسرقة الهوية واستخدام البرمجيات الخبيثة والتجسس الإلكتروني والقرصنة وتوزيع المعلومات الضارة، حيث يسعى المجرمون إلى الوصول غير المشروع إلى المعلومات أو تعطيل الخدمات الحاسوبية أو الحصول على مكاسب غير قانونية من خلال استغلال التكنولوجيا. كما أفادت أن التعريف المعتمد لديهم في هذا الشأن هو نص قانون الجرائم الإلكترونية رقم ٢٧ لعام ٢٠١٥م، المعمول به في المملكة الأردنية الهاشمية.

السعودية: أفادت بأن الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من

بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو اســتخدام أو اســتغلال غير مشــروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.

كما أفادت أن الجريمة الإلكترونية: جريمة باســتخدام الحواســيب والشــبكات داخل أو خارج المملكة ترتكب ضد أفراد أو جماعات أو مؤسسات حكومية أو غير حكومية.

مع الأخذ بالاعتبار أن يكون التعريف الموحد لجرائم تقنية المعلومات يحتوي على مفردات أو مصــطلحات ثابتة وموحدة تســمح بالمرونة المســتمرة نظرًا لتطور جرائم تقنية المعلومات مثل: الأفعال الإجرامية-البيانات التقنية-السيبراني - الاتصالات.

العراق: أفادت أن اســتراتيجية الأمن الســيبراني العراقي عرّفت الأمن الســيبراني بأنه الاســتعداد الوطني لتوفير تدابير متماســكة وإجراءات اســتراتيجية لضــمان أمن وحماية الوجود العراقي في الفضاء السيبراني وحماية البنى التحتية الحيوية للمعلومات وبناء ورعاية مجتمع إنترنت موثوق. كما عرفته مســودة مكافحة الجريمة الإلكترونية في العراق على أنه كل فعل يرتكب باســتعمال الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل التقنية التي يعاقب عليها القانون.

فلسطين: أفادت بأن جرائم تقنية المعلومات: هي كل فعل أو امتناع غير مشروع يأتيه الشخص بواســطة نظام معلوماتي معين ينتج عنه اعتداء على حق أو مصــلحة مشــروعة أو بيانات معلوماتية أو نظم شبكات المعلومات التي يحميها القانون سواءً وقع الفعل داخل الدولة أو عابر للحدود.

الكويت: أفادت بأن تعريف جريمة تقنية المعلومات وفق قانون ٦٣ لســنة ٢٠١٥م بأنه قانون ينظم جرائم تقنية المعلومات في الكويت؛ وفقًا لهذا القانون يُعرّف جريمة تقنية المعلومات في الكويت على أنها فعل أو ســلوك يُعد انتهاكًا للأمن الرقمي للمعلومات أو النظام الآلي أو شــبكات الاتصــالات الســلكية أو اللاســلكية، ســواءً كان ذلك بغرض الاختراق أو التلاعب أو التدمير أو السرقة أو التشويش أو الاستيلاء على البيانات أو التلاعب بها أو تغييرها أو استخدامها بصورة غير قانونية أو اســتخدام الأجهزة أو البرمجيات أو أي وســائل أخرى للوصــول إلى المعلومات أو نظام آلي دون وجه حق أو بدون إذن قانوني.

ويشـــمل هذا التعريف مجموعة متنوعة من الأنشـــطة ذات الطابع الإلكتروني والتي تشـــمل الاختراقات الســيبرانية، والاعتداءات على الأنظمة الآلية وشــبكات الاتصــالات والاســتيلاء على البيانات والمعلومات الرقمية والتلاعب بالبيانات وتدمير البيانات والتشـــويش على الأنظمة الرقمية واستخدام الأجهزة والبرمجيات دون إذن قانوني أو الضار لتقنية المعلومات في الكويت.

كما أفادت بأن تعريف جرائم تقنية المعلومات هي الأفعال غير المشـــروعة التي ترتكب عبر الفضـاء الإلكتروني باسـتخدام الوسـائل غير التقليدية وهو بشـكل عام كل فعل مجرم قانونًا يصدر عبر الشبكة الإلكترونية.

لبنان: أفـادت أنـه لا يوجـد في القوانين اللبنـانيـة المرعيـة الإجرائيـة تعريف "لجرائم تقنيـة المعلومات" إنما بتاريخ ٢٠١٨/١٠/١٠م صـدر القانون رقم /٨١/ المتعلق بالمعاملات الإلكترونية والبيانات ذات الطابع الشـخصـي، حيث حدد في مواده (١١٠-١١١-١١٢-١١٣-١١٤-١١٥) الجرائم المتعلقة بالأنظمة والبيانات المعلوماتية والبطاقات المصـرفية بالإضـافة إلى العقوبات والقواعد الإجرائية المتعلقة بضبط الأدلة المعلوماتية وحفظها وفقًا للعناوين التالية:

- ❖ الولوج غير المشروع إلى نظام معلوماتي.
- ❖ التعدي على سلامة النظام.
- ❖ التعدي على سلامة البيانات الرقمية.
- ❖ إعاقة أو تشويش أو تعطيل.
- ❖ إساءة التصرف بالأجهزة والبرامج المعلوماتية.

كما اقترحت عند وضع تعريف موحّد لجرائم تقنية المعلومات من قبل الدول الأعضاء في مجلس وزراء الداخلية العرب أن يُصـار إلى الاسـترشـاد بما تضـمنه القانون رقم / ٨١/ وتاريخ ٢٠١٨/١٠/١٠م بهذا الشأن، وأرفقت نسخة منه.

التوصية: رابعًا/

نص التوصـــية" الطلب من الأمانة الفنية اتخاذ اللازم بشـــأن عرض عدد من البنود على جدول أعمال الاجتماع المقبل للفريق حسب الآتي:

❖ تجارب الدول الأعضاء في مواجهة جرائم تقنية المعلومات

❖ التحديات الناشئة في مجال جرائم تقنية المعلومات

أولًا: تجارب الدول الأعضاء في مواجهة جرائم تقنية المعلومات

الإجراءات

قامت الأمانة الفنية للفريق المتمثلة في المكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات بمخاطبة شعب الاتصال في الدول الأعضاء بالخطاب رقم ١٠٢ وتاريخ ٢٠٢٣/٣/٢٨م والخطاب الإلحاقي رقم ١٩٥ وتاريخ ٢٠٢/٦/٥م؛ المتضمن الطلب من الوزارات الموقرة موافاتها بما لديها في هذا الشأن.

النتائج

تلقى المكتب إجابات الدول الآتية: (المملكة الأردنية الهاشمية – دولة الإمارات العربية المتحدة- مملكة البحرين - جمهورية العراق) وكانت الإجابات على النحو التالي:

الأردن: أفادت أنها كغيرها من الدول حول العالم تقوم بسن ووضع التشريعات الرادعة واللجوء إلى التقنيات الحديثة واتخاذ التدابير الوقائية لمواجهة جرائم تقنية المعلومات وحيث أن الشبكات الرقمية والأنظمة الإلكترونية خلقت مجموعة متشابكة ومتداخلة من الأنظمة المرتبطة بعدد من المجالات الحيوية ونتيجة لزيادة الاعتماد على الشبكات الإلكترونية في مختلف المجالات أدى ذلك إلى ازدياد نسبة الجرائم الإلكترونية وزاد تبعًا لذلك حجم الانفاق على مجالات الأمن ومكافحة الجرائم الإلكترونية.

وفيما يتعلق بالتجربة الأردنية في مواجهة جرائم تقنية المعلومات؛ فقد أقرت المملكة الأردنية الهاشمية العديد من التشريعات ذات العلاقة بالأمن المعلوماتي والتقني وحماية أنظمة تكنولوجيا المعلومات والأمن السيبراني ومنها:

أولًا: قانون الجرائم الالكترونية:

سن المشرع الأردني قانون الجرائم الإلكترونية رقم ٢٧ لسنة ٢٠١٥ ومن قبله قانون جرائم أنظمة المعلومات لسنة ٢٠١٠ للجرائم الإلكترونية، وهو القانون المعني بتجريم الأفعال التي ترتكب على شبكة الإنترنت، كما أنه يوجد في الأردن العديد من التشريعات التي تجرّم الوصول غير المصرح به إلى الأجهزة الإلكترونية وشبكة الإنترنت والاعتداء على المعلومات والبيانات.

ونتيجة للتطورات المتسارعة في مجال جرائم تقنية المعلومات وبهدف حماية نظام المعلومات والبيانات والبنية التحتية الحرجة ومعالجة الأفعال الجرمية الجديدة للجريمة الإلكترونية ولموائمة التشريع مع المعايير الدولية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد تم وضع مسودة تعديل مشروع قانون الجرائم الإلكترونية لسنة ٢٠٢٣ وهو حاليًا معروض على مجلس الأمّة لغاية مناقشته وإقراره بحسب الأصول، ومن أبرز الملامح الذي تضمنها التعديل الجديد:

١. الدخول إلى أنظمة المعلومات الخاصة بمؤسسات الدولة وتجريمها بدون تصريح أو بما يخالف أو يجاوز التصريح.
٢. تجريم اصطناع مواقع أو حسابات أو منصات إلكترونية زائفة.
٣. تجريم اعتراض خط سير البيانات.
٤. تجريم حيازة برامج أو بيانات أو رموز بقصد ارتكاب الجرائم.
٥. تجريم التحايل على العنوان البروتوكولي.
٦. تجريم الأفعال المتعلقة باغتيال الشخصية والمساس بالوحدة الوطنية والحض على العنف والكراهية وازدراء الأديان.
٧. تجريم جمع التبرعات أو الصدقات دون ترخيص وتجريم التسول الإلكتروني.

ثانيًا: قانون الأمن السيبراني.

قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩ هو قانون يهدف لحماية الأنظمة والشبكات المعلوماتية من حوادث الأمن السيبراني والقدرة على استعادة واستمرارية عملها ضمن فضاء يشمل تفاعل الأشخاص والبيانات والمعلومات ونظم المعلومات وبرامجها وأنظمة الاتصالات والبنى التحتية المرتبطة بها في فضاء تقني عالمي مفتوح.

وقد أُنشئ المركز الوطني للأمن السيبراني عام ٢٠١٩ بموجب قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩ وفق نص المادة ٥/أ بقولها "أ- ينشأ في المملكة مركز يسمى (المركز الوطني للأمن السيبراني)

يتمتع بشخصية اعتبارية ذات استقلال مالي وإداري وله بهذه الصفة تملك الأموال المنقولة وغير المنقولة والقيام بجميع التصرفات القانونية اللازمة لتحقيق أهدافه بما في ذلك إبرام العقود وله حق التقاضي وينوب عنه في الاجراءات القضائية وكيل إدارة قضايا الدولة"، وبالتالي يعد المركز الوطني للأمن السيبراني كمؤسسة حكومية معني ببناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية الفضاء السيبراني للمملكة الأردنية الهاشمية من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الاشخاص والممتلكات والمعلومات.

وفي ظل تزايد أهمية الأمن السيبراني وتهديداته والقضايا المتعلقة به على المستوى الوطني والدولي، وبهدف حماية المملكة والفضاء الإلكتروني الخاص بها أصبح إيجاد مظلة تعنى بمهام الأمن السيبراني أهمية بالغة ودور محوري في صيانة مصالح الدولة وتعزيزها بالإضافة إلى تأمين سلامة عمل قطاعات الدولة المختلفة من أي اختراقات قد تحدث في ظل التطور الهائل، وما صاحبه من تنوع في وسائل الاتصالات والبرامج الحاسوبية وتطبيقاتها الأمر الذي زاد من حجم انتشار المعلومات وتبادل البيانات.

مهام وأهداف المركز الوطني للأمن السيبراني:

بموجب أحكام المادة ٦/ب من قانون الأمن السيبراني حدد القانون للمركز مجموعة من المهام والصلاحيات التي يمكن من خلالها القيام بعمله كمؤسسة وطنية معنية بالأمن السيبراني:

١. سياسات واستراتيجيات ومعايير الأمن السيبراني الوطني حيث يتم إعداد وتطوير معايير واستراتيجيات وسياسات الأمن السيبراني الوطني ومراقبة تطبيقها.
٢. التعاون المحلي والدولي للأمن السيبراني من خلال بناء برامج وآليات تعاون محلية ودولية مع الشركاء المحليين والحكومات الأجنبية والمنظمات الدولية لغايات التنسيق وتبادل المعلومات.
٣. بناء القدرات والتوعية بالأمن السيبراني بتطوير برامج لبناء الخبرات الوطنية في مجال الأمن السيبراني، وتعزيز الوعي بالأمن السيبراني على المستوى الوطني.
٤. حماية البنية التحتية الحرجة وتحديدها وتنسيق التعاون مع الجهات ذات العلاقة لبناء برامج وقدرات لحمايتها.

٥. إدارة عمليات الأمن والاستجابة لحوادث الأمن السيبراني من خلال الإشراف على بناء فرق الأمن السيبراني والاستجابة لحوادث الأمن السيبراني في القطاع العام والخاص وتطوير خطط وطنية لمواجهة الأزمات السيبرانية وتنسيق جهود الاستجابة لها والتدخل عند الحاجة.
٦. الإصلاح التنظيمي والقانوني بتطوير وتحديث التشريعات والأنظمة والتعليمات اللازمة لضمان الأمن السيبراني الوطني بالتعاون مع الجهات المعنية.
٧. منح التراخيص لمقدمي خدمات الأمن السيبراني.
٨. تقييم النواحي الأمنية لخدمات الحكومة الإلكترونية.
٩. تلقي الإخبارات والشكاوى المتعلقة بالأمن السيبراني وحوادث الأمن السيبراني واتخاذ الإجراءات المناسبة لمعالجتها ومنع حدوثها.

وهناك عدد من التشريعات التي يُعنى المركز الوطني للأمن السيبراني بتنظيمها والإشراف على مدى الالتزام بها منها نظام ترخيص مقدمي خدمات الأمن السيبراني لسنة ٢٠٢٣ وتعليمات معايير المخالفات والإجراءات المستحقة عليها لسنة ٢٠٢٣ وتعليمات تصنيف حوادث الأمن السيبراني لسنة ٢٠٢٣، بالإضافة إلى أن هناك سياسات متعلقة بالأمن السيبراني يعمل المركز الوطني للأمن السيبراني على إصدارها كسياسة خدمات الجيل الخامس وسياسة اعتماد منتجات الأمن السيبراني وسياسة إنترنت الأشياء.

وللمركز الوطني للأمن السيبراني دور أمني يتمثل بتلقي الشكاوى والإخبارات المتعلقة بالأمن السيبراني وحوادث الأمن السيبراني وله متابعتها واتخاذ الإجراء المناسب لمعالجتها ومنع حدوثها أو استمرارها وفق الصلاحيات الممنوحة له، وقد وضع المركز الوطني للأمن السيبراني نظام أمني متكامل من التقنيات والعمليات التي تستخدم لحماية الأنظمة والشبكات والبرامج والأجهزة والبيانات والمعلومات من الحوادث السيبرانية ولاكتشاف حوادث الأمن السيبراني والاستجابة لها تم تشكيل الفريق الوطني للاستجابة لحوادث الأمن السيبراني الأردني (JOCERT) Computer Emergency Response Team of Jordan هو فريق الاستجابة للحوادث مسؤول عن الاستجابة لحوادث أمن الكمبيوتر، وهو تابع للمركز الوطني للأمن السيبراني، حيث تتمثل الواجبات الرئيسية لهذا الفريق في منع الحوادث الأمنية السيبرانية وإدارتها والاستجابة لها وحفظ المعلومات والبيانات ومنع وقوع الضرر أو تخفيفه والتخفيف من الآثار المترتبة عليه، ويشمل بما في ذلك

البحث عن التهديدات وتطوير السياسات والإجراءات وتدريب الأفراد والمؤسسات على أفضل ممارسات الاستجابة لحوادث الأمن السيبراني.

ثالثًا: مشروع قانون حماية البيانات الشخصية لسنة ٢٠٢٣.

مسودة مشروع قانون حماية البيانات الشخصية والذي يقوم مجلس الأمة حاليًا بمناقشة مواده لغايات إقراره ورفعه لجلاله الملك للمصادقة عليه وفق احكام الدستور الأردني.

وقد نص القانون على إنشاء مجلس حماية البيانات الشخصية بموجبها يحق للمجلس صلاحية إقرار السياسات والإستراتيجيات والخطط والبرامج المتعلقة بحماية البيانات ومراقبة تنفيذها وأيضا اعتماد المعايير والتدابير الخاصة بحماية البيانات بما فيها مدونات السلوك الخاصة بحسن أداء المسؤول والمعالج والمراقب لأعمالها.

ويشمل قانون حماية البيانات الشخصية أمن المعلومات والبيانات على نوعيها سواءً كانت بيانات شخصية خاصة بالمستخدمين أو بيانات عامة متعلقة بالمؤسسات وهو يضمن حماية المعلومات والبيانات عن طريق ربطها مع ضوابط ومعايير الأمن السيبراني التي تقوم بدورها على حماية البيانات كافة من احتمالية وصول الأشخاص أو المؤسسات غير المصرح لهم ذلك بالاطلاع عليها أو محاولة تعديلها أو اتلافها مما يؤدي إلى انتهاك الخصوصية وتعرضها للسرقة والاستغلال ويعاقب القانون كل من يحاول أو يقوم بالإخلال بأمن وسلامة البيانات.

التحديات المتعلقة بجرائم تقنية المعلومات:

على الرغم من التطور الهائل فلا شك أن الجرائم الإلكترونية هي جرائم مستحدثة ومتطورة بشكل مستمر وأن هذا التطور قد أدى إلى ظهور جرائم إلكترونية وجرائم سيبرانية لم تعد المتطلبات التشريعية تفي بالغرض، ويعتبر من أكثر التحديات صعوبة هي:

١. إثبات الجريمة الإلكترونية: حيث أنها على الغالب لا تترك أثرًا إذا ما قام الفاعل بمحو بياناته أو سجلاته على نحو يتعذر معه استرجاع أي بيانات تستخدم ضده.
٢. بعض الجرائم قد يتم اكتشافها إما عن طريق الصدفة أو بعد وقت طويل من ارتكابها.
٣. جريمة عابرة للحدود كونها لا تعترف بالحدود الجغرافية التي تخترق كل زمان ومكان حيث قد ترتكب بواسطة جهاز كمبيوتر في دولة معينة ويتحقق الفعل الإجرامي في دولة أخرى.
٤. الاستخدام السلبي لوسائل التواصل الاجتماعي، وانتشار جرائم خطاب الكراهية، وانتهاك الخصوصية، والأخبار الكاذبة أو المزيفة.

التعاون العربي في مجال جرائم تقنية المعلومات:

تدرك المملكة الأردنية الهاشمية أهمية التعاون والتنسيق المشترك بين الدول العربية والإقليمية والدولية في تتبع الجرائم المتعلقة بتقنية المعلومات وأهمية التبادل والتعاون المشترك للمعلومات الاستخبارية ذات العلاقة وذلك بموجب الاتفاقيات والمعاهدات الدولية المنضمة لها.

دور الأجهزة الأمنية الأردنية في مكافحة الجريمة الإلكترونية وبناء وتطوير القدرات لمكافحتها:

أولًا: وحدة مكافحة الجرائم الإلكترونية

تضم هذه الوحدة مجموعة من الضباط الأمنيين المدربين والمؤهلين من مديرية الأمن العام لملاحقة المجرمين الذين يرتكبون جرائم إلكترونية سواءً كانت تلك الجرائم ترتكب على نظام تقنية المعلومات بحد ذاتها أو على إحدى مكوناتها أو أن ترتكب الجرائم عبر شبكة الإنترنت أي بواسطتها، وقد بين قانون الجرائم الإلكترونية عددًا من الجرائم الإلكترونية التي أوردها ضمن نصوصه.

ثانيًا: المركز الوطني للأمن السيبراني

تضمن نص المادة ٦ / ب/٢ والبند ١٣ من ذات النص من قانون الأمن السيبراني "ب- يتولى المركز في سبيل تحقيق أهدافه المهام والصلاحيات التالية (٢. تطوير عمليات الأمن السيبراني وتنفيذها وتقديم الدعم والاستشارة اللازمين لبناء فرق عمليات الأمن السيبراني في القطاعين العام والخاص وتنسيق جهود الاستجابة لها والتدخل عند الحاجة"، "١٣. تقييم وتطوير فرق الاستجابة لحوادث الأمن السيبراني").

مكافحة الحوادث السيبرانية أو ما تعرف عالميًا بالاستجابة للحوادث Incident Responses هي مجموعة من السياسات والإجراءات الخاصة بأمن المعلومات التي يتم استخدامها لتحديد الهجمات الإلكترونية واحتوائها والقضاء عليها والتعافي منها، ويكون الهدف من الاستجابة للحوادث هو تمكين المركز الوطني للأمن السيبراني وغيره من المؤسسات والدوائر الحكومية والقطاع الخاص من اكتشاف الهجمات والحوادث السيبرانية وإيقافها بسرعة، وتقليل الضرر ومنع الهجمات المستقبلية من نفس النوع للهجمات السيبرانية.

كما تتولى هيئة تنظيم قطاع الاتصالات ووزارة الاقتصاد الرقمي والريادة القيام بالمتطلبات الأمنية والإجراءات القضائية للتعامل مع مزودي الخدمات ومعالجة شكاوى متقي الخدمة المتعلقة بالحسابات الوهمية وحظرها والتصدي لها.

الإمارات: استعرضت دولة الإمارات العربية المتحدة تجربتها في مجال مكافحة جرائم تقنية المعلومات (حسب ما يتضح في الملف المرفق).

البحرين: أفادت بأن مملكة البحرين بذلت جهودًا مبكرة لمواكبة التطورات العلمية في تكنولوجيا الاتصالات والمعلومات، إذ حرصت على إدارة وتنظيم عملية التحول الرقمي داخل المملكة وفق رؤية استراتيجية تحقق التوازن بين الاستفادة الوطنية من تطبيقات التكنولوجيا الحديثة في التفاعلات الإنسانية والاجتماعية والمعاملات الاقتصادية والتجارية وبين المسؤولية الوطنية لحفظ الأمن البحريني من المخاطر الأمنية المستحدثة، بما يحقق أهداف النمو والتنمية المستدامة داخل مملكة البحرين.

١. الإطار التشريعي والتنظيمي

- أصدر المشرع البحريني حزمة من التشريعات والقوانين المتطورة لإدارة وتنظيم عملية التحول الرقمي في مملكة البحرين، كان أبرزها التشريعات المتعلقة بهيئة المعلومات والحكومة الإلكترونية: وحماية البيانات الشخصية؛ والتعاملات والتوقيعات الإلكترونية؛ وحقوق الملكية الفكرية: والتشغيل البيني للبيانات.
- وضعت مملكة البحرين اللبنة الأساسية التي تحفظ هذه المكتسبات وتعزز البيئة الاقتصادية الآمنة لتدفع عجلة التنمية والنهضة، حيث صدر في تاريخ ٢٨ نوفمبر لعام ٢٠١١م عن عاهل البلاد حضرة صاحب الجلالة الملك حمد بن عيسى آل خليفة مرسوم رقم (١٠٩) للعام ٢٠١١م بتعديل بعض أحكام المرسوم رقم (٦٩) للعام ٢٠٤٤م بإعادة تنظيم وزارة الداخلية حيث جاء فيه بإنشاء الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني والتي يندرج تحت مظلتها عددًا من الإدارات الأمنية تهدف لحفظ دعائم الاقتصاد الوطني، من ضمنها إدارة مكافحة الجرائم الإلكترونية.
- وفي أعقاب التحولات الكبيرة في أنماط الجرائم المستحدثة وارتفاع مستويات المخاطر الأمنية التي شهدها العالم نتيجة التطور الشبكي، انضم التشريع البحريني لركب الدول ذات التشريعات المواكبة للتطور في الجرائم المرتكبة عبر تقنية المعلومات وتكنولوجيا

الاتصالات ومكافحة الأنشطة الإجرامية المتصلة بها، حيث تم إصدار القانون رقم (٦٠) لسنة (٢٠١٤م) بشأن جرائم تقنية المعلومات.

- وعلى مستوى التشريع العربي، صادقت مملكة البحرين على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وذلك بموجب قانون رقم (٢) لسنة ٢٠١٧م.

٢. الإدارة الأمنية الحديثة ومكافحة الجريمة

- منذ إصدار المرسوم رقم (١٠٩) لسنة ٢٠١١م، والمتضمن إنشاء إدارة مكافحة الجرائم الإلكترونية، باشرت الإدارة اختصاصاتها القانونية بشأن الجرائم والممارسات غير القانونية المرتكبة عبر مجال العالم الافتراضي.
- ومنذ إصدار القانون رقم (٦٠) لسنة (٢٠١٤م) بشأن جرائم تقنية المعلومات، توسعت مسؤوليات إدارة مكافحة الجرائم الإلكترونية لتغطي الاتجاهات الحديثة في الأنشطة الإجرامية كالاختراق الإلكتروني وإحداث التلف والتلاعب بالبيانات وحجب الخدمات الرقمية والاستيلاء على الأموال بطرق احتيالية والمحتوى الإلكتروني غير القانوني وإساءة استعمال تكنولوجيا المعلومات والاتصالات، بالإضافة إلى ملاحقة الأنشطة والممارسات الإجرامية الأخرى في الجرائم المرتكبة باستخدام وسائل تقنية المعلومات.
- ومنذ عام ٢٠١٨م انتهجت إدارة مكافحة الجرائم الإلكترونية نظم أمنية مستحدثة في مكافحة الجرائم التي تقع تحت طائلة قانون رقم (٦٠) لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات، من خلال تكوين فرق عمل احترافية على المستويات الإدارية والفنية والشرطية من الكفاءات البشرية، وفق مخططات ومسارات عمل نستند لعلوم الإدارة الأمنية المعاصرة.
- استحدثت الإدارة آليات سريعة ومتطورة لحث المواطنين والمقيمين على تقديم البلاغات والإبلاغ الفوري عن الأنشطة الإجرامية والممارسات غير المشروعة، من خلال الإبلاغ الإلكتروني عن طريق موقع الويب الخاص بالإدارة، وتخصيص رقم للاتصال بالخط الساخن، وعبر مواقع التواصل الاجتماعي أيضًا، بالإضافة إلى البلاغات المستلمة من

مراكز الشـرطة: مما حقق عنصـر السـرعة في الاسـتجابة الأمنية في التعامل مع الجرائم الإلكترونية والجرائم المرتكبة عبر تكنولوجيا المعلومات والاتصالات.

- تمكنت إدارة مكافحة الجرائم الإلكترونية بوزارة الداخلية من رفع الجاهزية الأمنية للشعب والأقسام التابعة للإدارة في الرصد والتتبع للتعامل مع المستجدات الطارئة في بيئة المخاطر الأمنية: وهو ما انعكس بالإيجاب على أداء الإدارة في ظل انعكاسات جائحة فيروس كورونا على أنماط ومعدلات الجرائم المرتكبة عبر الإنترنت والاتصالات والرسائل الهاتفية.
- أدى دعم وزارة الداخلية المتواصل في تزويد إدارة مكافحة الجرائم الإلكترونية بالمعامل والأجهزة التقنية والمعدات الفنية الحديثة المستخدمة في عمليات الفحص الفني للأدلة الرقمية إلى رفع الكفاءة الفنية والقدرة التشغيلية لمختبرات فحص الأدلة الرقمية.
- كما أولت الإدارة الأمنية أولوية استراتيجية في الاستثمار في الكوادر البشرية من خلال التأهيل والتدريب الأمني المتقدم في المعاهد والأكاديميات المتخصصة وبيوت الخبرة العالمية في مجالات الرصد والفحص والتتبع الإلكتروني.
- كما استهدفت الإدارة برامج عمل ومشاريع تطوير تهدف إلى تعزيز القدرات الوطنية في مكافحة الجرائم الإلكترونية وتحسين كفاءة تقديم الخدمات الأمنية وذلك من خلال:
  - ✓ برامج البلاغات الإلكترونية وتلقي البلاغات الرقمية.
  - ✓ برامج إدارة وتطوير عمليات فحص الأدلة الرقمية.
  - ✓ برامج إدارة وتطوير الربط الإلكتروني لقضايا جرائم الإنترنت ونظم المعلومات.

٣. المجتمع والتوعية من الجريمة الإلكترونية

- يشكل عامل التوعية الأمنية للمستخدمين حجر الزاوية في استراتيجية إدارة مكافحة الجرائم الإلكترونية، انطلاقًا مبدأ أن «المستخدم هو الحلقة الأضعف في الجريمة الإلكترونية».
- تعتمد الإدارة على وسائل الإعلام التقليدية (الصحافة والإذاعة والتليفزيون) بجانب وسائل الإعلام الحديث (مواقع التواصل الاجتماعي ومنصات الاجتماعات الرقمية)،

وذلك من أجل نشـر البرامج التوعوية لطرق الاسـتخدام الآمن لتكنولوجيا الاتصـالات والمعلومات والحماية من الأنشطة الإجرامية المتصلة بها.

- تتعاون الإدارة في هذا الشأن مع مراكز الفكر والدراسات والأبحاث والمعاهد والجامعات والمؤسسات الوطنية من أجل عقد ورش العمل والندوات والمحاضرات التثقيفية، بهدف إيصـال رسـالة النوعية إلى الشـرائح المسـتهدفة من المواطنين والمقيمين داخل المجتمع البحريني.
- كما تسـتهدف برامج التوعية الأمنية الأطفال والطلاب في المدارس والجامعات من أجل التوعية من الاتجاهات الإجرامية الحديثة والمخاطر المرتبطة بها مثل التنمر الإلكتروني واسـتغلال الأطفال عبر الإنترنت والابتزاز على مواقع التواصـل الاجتماعي وغيرها من الأنشطة الإجرامية التي تستهدف بشكل خاص فئة النشء والشباب.
- تتبنى الإدارة سـياسـة الالتزام بخصـوصـية البيانات والمعلومات الخاصـة بالمبلغين من النشـر الصـحفي والإعلامي، كما تحظر مشـاركة المعلومات مع عائلة المبلغ؛ مما كان له مردود كبير في تشـجيع كثير من فئات المجتمع وعدم ترددها في الإبلاغ عن الجرائم التي قد تعرضوا لها.
- تتيح الإدارة قنوات لتلقي الاسـتجابة العكسـية من المواطنين والمقيمين من خلال حثهم على إرسـال الاقتراحات والشـكاوى عبر آليات التواصـل المختلفة مع الإدارة؛ مما يتيح فرص معرفية لتحسين وتطوير العمل الأمني بشكل مستمر.
- اعتمدت إدارة مكافحة الجرائم الإلكترونية على نهج مؤسـسـي من أجل رسـم مسـار اسـتراتيجي لكيفية مواجهة التحديات الطارئة والتغلب عليها، وفق رؤية اسـتراتيجية معاصـرة وبرامج عمل متطورة، تسـتهدف تحسـين بيئات العمل الأمني والسـلامة العامة والتحول الرقمي، والشراكة المجتمعية.

٤. التعاون الأمني

- يمثل التعاون الأمني مرتكزًا رئيسـيًا في الاسـتراتيجية الأمنية لمكافحة الجرائم الإلكترونية، مسـتندًا في ذلك على تشـييد جسـور التعاون الأمني وتبادل المعلومات والخبرات بين إدارة

مكافحة الجرائم الإلكترونية والجهات الفاعلة ذات العلاقة والارتباط على مختلف الأصعدة.

- بشكل منهجي، تتعاون الإدارة على المستوى الوطني مع الوحدات الأمنية والمؤسسات الوطنية داخل مملكة البحرين، وعلى المستوى الإقليمي يتكامل التعاون الأمني بين الدول الأعضاء في مجلس التعاون لدول الخليج العربية ومجلس وزراء الداخلية العرب، وذلك إضافةً إلى المستوى الدولي للتعاون مع المنظمات الحكومية الدولية وهيئات المجتمع الدولي.
- يسهم فريق التحليل والدراسات الأمنية التابع للإدارة في دراسة الأنشطة الإجرامية المتصلة بمنظومة الأمن الإلكتروني، وتحليل بيئة المخاطر الأمنية ورصد مؤشرات الجريمة والاتجاهات الناشئة في ارتكابها، واستراتيجيات مواجهتها، حيث يضطلع باحثي الإدارة بإصدار البحوث والدراسات والتقارير والنشرات الأمنية في هذا الشأن.
- تشارك الإدارة بأوراق العمل والمقترحات والتوصيات والمرئيات الأمنية في المجالات المتعلقة بمنظومة الأمن الإلكتروني ومكافحة الجرائم الإلكترونية والأنشطة الإجرامية المتصلة بها، على الصعيدين الإقليمي والدولي: والتي من أبرزها:
  - ✓ لجنة الخبراء الدولية المكلفة بوضع اتفاقية دولية شاملة بشأن مكافحة استخدام المعلومات وتكنولوجيا الاتصالات للأغراض الإجرامية، وذلك بالتعاون مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة.
  - ✓ اجتماعات فريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات.
  - ✓ اللجنة المتخصصة بالجرائم المستجدة، والمعتمدة من قبل مجلس وزراء الداخلية العرب.
  - ✓ مؤتمر التفاعل وتدابير بناء الثقة في أسيا (CICA) ومشروع التعاون في مجال أمن تكنولوجيا المعلومات والاتصالات واستخدامها.
  - ✓ الاتفاقيات الثنائية ومذكرات التعاون المشترك بين مملكة البحرين وبلدان العالم في المجالات الأمنية وتعزيز قدرات مكافحة الجرائم الإلكترونية، عبر القنوات الدبلوماسية ووزارة الخارجية البحرينية.

- ✓ اللجنة الدائمة للأمن السيبراني بدول مجلس التعاون لدول الخليج العربية.
- ✓ متابعة تنفيذ بنود الخطة المرحلية لتنفيذ الاستراتيجية العربية لمواجهة جرائم تقنية المعلومات.

- كما تتعاون إدارة مكافحة الجرائم الإلكترونية مع الجهات الأمنية الدولية، من خلال عدد من قنوات الاتصال وآليات التعاون الأمني فيما يتعلق بتبادل المعلومات الجنائية، وتعميم النشرات الأمنية عن الحوادث والجرائم والمطلوبين للعدالة في ارتكاب الجرائم الإلكترونية، عبر أنظمة الربط الرقمي وشعب الاتصال والمكاتب المتخصصة في نطاق الشرطة الجنائية الدولية (الإنتربول). والأمانة العامة لمجلس وزراء الداخلية العرب، والأمانة العامة لمجلس التعاون، والشرطة الخليجية.

العراق: أفادت أن التطور السريع الذي شهده العراق في استخدام التكنولوجيا الحديثة والانتشار الواسع لاستخدام مواقع التواصل حيث أصبحت هذه المواقع من الأمور الحياتية المهمة وأداة مساعدة وفاعلة في تطوير وتنمية المؤسسات العامة وتمكنهم من التقدم وتقديم الخدمات وقد كانت الدول المتقدمة سباقة في استخدامها، ومواكبتها، وأصبح من الصعوبة الاستغناء عنها، لكن في المقابل أفرزت أنواعًا جديدة من الجرائم تصيب المجتمع بالأزمات السياسية والاقتصادية والاجتماعية، والثقافية. إن الثورة التكنولوجية والمعلوماتية أفرزت مجموعة من الجرائم وأصبحت هاجسًا وتحدٍ أساسي للأجهزة الأمنية، ويمكن أن تتمثل الجرائم الإلكترونية فيما يلي:

١. الابتزاز الإلكتروني.

٢. الإرهاب الإلكتروني.

٣. الاخبار الكاذبة والإشاعات.

<u>أولًا" الابتزاز الإلكتروني</u>

هناك دوافع مشتركة لدى غالبية المجرمين الإلكترونيين من حيث دوافع الابتزاز (الدافع المادي - دافع الانتقام - دافع سياسي - دوافع ذهنية - دافع التسلية) حيث سجل العراق خلال العام الماضي وفق إحصائية بوزارة الداخلية، عن ٢٤٠٠ حالة ابتزاز معظم ضحاياها من

النساء بينهن فتيات في سن المراهقة وأطفال دون سن (الـ١٤). ورغم المعدلات المتصاعدة لا يوجد في العراق أي قانون يخص جرائم الابتزاز الإلكتروني"، ويجري التعامل معها وفق قانون العقوبات رقم ١١١ لسنة ١٩٦٩ م، وبحسب القانون وضمن المادة ٢٦ من القانون، أولًا تكون عقوبة الابتزاز بمضمونه العام الحبس الشديد، أو البسيط من (٣ أشهر إلى ٥ سنوات) أو الغرامة التي تحدد من الخبير القضائي وفقًا للضرر، وفي ما يلي تجارب وزارة الداخلية العراقية في محاربة الابتزاز.

- ❖ وجهت بتكليف عدد من الدوائر المختصة من بينها مكافحة الإجرام والشرطة المجتمعية ووكالة الاستخبارات وبعض التشكيلات السائدة لمتابعة جرائم الابتزاز الإلكتروني بالإضافة إلى استحداث شعبة خاصة بذلك وتحديد قاضٍ مختص للنظر بهذه الجرائم فضلًا عن عقد ندوات تثقيفية استهدفت جامعات ومدارس ومؤسسات عدة للتنبيه بمخاطر - الابتزاز وكيفية التعامل السليم مع العالم السيبراني"، حيث تم العمل على تجسير الثقة بين السلطات الأمنية والمواطنين بما يطمئن ضحايا الابتزاز خاصة الذين يخشون الإفصاح عن تعرضهم لتلك الجرائم خوفًا من الفضيحة وشيوع ذلك بين ذويهم ومعارفهم".
- ❖ اشراك العنصر النسوي

قامت وزارة الداخلية بضم عناصر نسائية ضمن المفاصل التي تتعامل مع جرائم الابتزاز الإلكتروني وإدخال المنتسبين دورات تطويرية وتقنية لكسب خبرات أكبر في مواجهة جرائم الابتزاز والوصول إلى الفاعلين"

- ❖ الخط الساخن: تم انشاء خط ساخن لغرض الإبلاغ عن حالات الابتزاز الإلكترونية والتعامل معها بكل جدية وسرعة وفق الإجراءات القانونية.
- ❖ إقامة ندوات تثقيفية: قامت وزارة الداخلية العراقية بعمل ندوات تثقيفية وعرض أساليب ومخاطر الابتزاز الالكتروني وكيفية محاربته.

<u>ثانيًا: الجرائم المتعلقة بالإرهاب والمرتبكة بواسطة تقنيات المعلومات</u>

هي الجرائم التي تشكل تحدي للعاملين في مجال مكافحة الإرهاب حيث يقومون الإرهابيين بنشر أفكار ومبادئ جماعات إرهابية والدعوة اليها، وتمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، ونشر طرق صناعة المتفجرات، حيث يتم إجراء

ندوات تثقيفية لغرض محاربة الأفكار الإرهابية وتتبع الجماعات المسلحة ومتابعة تمويلهم واتصالاتهم لغرض إلقاء القبض عليهم. وفيما يلي تجارب بلادهم فيما يتعلق بجرائم الإرهاب:

١. مكافحة التجنيد الإلكتروني

عملت الكوادر المختصة في مجال مكافحة الإرهاب الإلكتروني على استهداف الحسابات والمواقع التي تعمل على نشر الفكر الإرهابي وتجنيد الشباب من المراهقين والمتعاطفين من خلال غلق المواقع والوصول إلى معلوماتهم الشخصية باستخدام طرق فنيه واستخبارية وإلقاء القبض عليهم.

٢. محاربة الإرهاب الإلكتروني بنفس الأسلوب

استخدام نفس الأساليب التي تعتمدها التنظيمات الإرهابية في هذا المجال، مثل التجسس والقرصنة واختراق المواقع واستخدام العملاء.

٣. متابعة منصات التواصل الاجتماعي.

من خلال رصد قنواتهم الإعلامية وصفحاتهم وتجمعاتهم على منصات التواصل الاجتماعية واغلاقها.

٤. عقد ندوات وورش عمل خاصة بمكافحة الإرهاب الإلكتروني

من خلال عمل ندوات وورش عمل تثقيفية مختصة بمكافحة الإرهاب الإلكتروني للمناطق التي كانت تحت سيطرة العصابات الارهابية.

<u>ثالثًا: الأخبار الكاذبة و البروباغندا ، والجيوش الإلكترونية في مو اقع التواصل الاجتماعي</u>

مع انتشار شبكات التواصل الاجتماعي وزيادة أعداد مستخدميه، وتقدمها في الأهمية على الصحافة التقليدية، ظهرت وسائل جديدة تهدف لإرباك المتابعين ورواد هذه المواقع وللوصول إلى وهم السيطرة على الرأي العام، ويقصد به تلك الحسابات الوهمية أو الحقيقية على مواقع التواصل الاجتماعي الموجهة من جهات معينة لشن حملات إعلامية ممنهجة ضد أشخاص أو كيانات أو دول، وغالبًا ما يكون أصحابها مجهولين، وأسلحتهم الحواسيب، وساحتهم منصات التواصل الاجتماعي، وهؤلاء العناصر ليسوا مدربين بل مبرمجين بهدف إنشاء عدد لا نهائي من المقاتلين الأوفياء لجهة ما بأسماء وهمية وحسابات غير حقيقية، وظيفتهم إعادة نشر آراء

محددة وتبني مواقف معينة في وسائل التواصل الاجتماعي، كي تبدو وكأنها رأي عام لعـــدد كبير من المستخدمين وكأنهم يجمعون على رأي واحد أو يغردون بصوت واحد.

وما يلي تجاربهم في مكافحة الإشاعة.

١. استحداث قسم مكافحة الشائعات في وزارة الداخلية العر اقية

تقوم الوزارة برصـد الشـائعات وخاصـة في المنصـات الإلكترونية باعتبار أن مواقع التواصـل الاجتماعي أرض خصبة لانتشار الشائعات ورفعها إلى الجهات المختصة ذات العلاقة.

٢. محاسبة مطلقي الإشاعات وفق القانون

إلقاء القبض بحق مطلق الإشـــاعة وفق القانون من المادة ٧٩ التي تؤكد على عقوبة السـجن لمطلقي الشائعات بمدة تصل الى ١٠ سنوات.

٣. إطلاق ندوات وحملات تثقيفية

حملات التثقيف في الجامعات والمعاهد والمدارس للتعرف على كيفية التعامل مع الأخبار المظللة وضرورة استسقاء الأخبار من مصادرها.

٤. احتضان الشباب من خلال اللقاء المباشر بهم

يتم عبر آلية جديدة يتبعها قسم الشائعات للخروج إلى الشارع والالتقاء بالمواطن بشكل مباشر من خلال استهداف فئـة الشـباب لأنه وفق الاحصائيات فإن أكثر الأخبار المتداولة من الشباب عن طريق مواقع التواصل الاجتماعي.

ثانيًا: التحديات الناشئة في مجال جرائم تقنية المعلومات

الإجراءات

قامت الأمانة الفنية متمثلة في المكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات بمخاطبة شعب الاتصال في الدول الأعضاء بالخطاب رقم ١٠٢ وتاريخ ٢٠٢٣/٣/٢٨م، والخطاب الإلحاقي رقم ١٩٥ وتاريخ ٢٠٢٣/٦/٥م، المتضمن موافاتها بأبرز التحديات الحديثة في هذا المجال والسبل المثلى لمواجهتها.

النتائج

تلقى المكتب إجابات الدول الآتية: (المملكة الأردنية الهاشمية - مملكة البحرين - المملكة العربية السعودية - جمهورية العراق - دولة الكويت)

ويستعرض البند الرابع من هذا التقرير تلك الإجابات بالتفصيل.

التوصية/ خامسًا:

نص التوصية " تعميم ورقة العمل التي أعدتها الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري على الدول الأعضاء للاستفادة منها ".

الإجراءات والنتائج

قامت الأمانة الفنية للفريق ممثلةً بالمكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات بتعميم ورقة العمل التي أعدتها الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري الموسومة بـ "وضع إطار عربي موحد لمواجهة القرصنة الإلكترونية وحماية الشبكات" على الدول الأعضاء للاستفادة منها بالخطاب رقم ١٠٥ وتاريخ ٢٠٢٣/٣/٢٨م.

التوصية سادسا/أ:

نص التوصية " دعوة الدول الأعضاء إلى اتخاذ موقف عربي موحد إزاء تطورات بلورة اتفاقية دولية بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، يأخذ في الحسبان ما ورد بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات".

الإجراءات

قامت الأمانة الفنية للفريق متمثلةً بالمكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات بمخاطبة شعب الاتصال في الدول الأعضاء بالخطاب رقم ١٠٦ وتاريخ ٢٠٢٣/٣/٢٨م، والخطاب الإلحاقي رقم ١٩٦ وتاريخ ٢٠٢٣/٦/٥م من أجل موافاته بما تم في هذا الشأن.

النتائج

تلقى المكتب إجابات الدول الآتية: (المملكة الأردنية الهاشمية - مملكة البحرين - المملكة العربية السعودية - جمهورية العراق - دولة الكويت) وكانت الإجابات على النحو الآتي:

الأردن: أوصت بما يلي:

- ❖ وضع سياسة عربية موحدة بين دول الأعضاء للتعامل مع الشركات العالمية المزودة لمنصات التواصل الاجتماعي وإلزامها على التعاون مع مؤسسات إنفاذ القانون بهذه الدول.
- ❖ إنشاء مجلس تعاون عربي لمكافحة جرائم تقنية المعلومات.
- ❖ وضع ضباط ارتباط بين دول الأعضاء والمشاركة بإنشاء منصة لتبادل المعلومات والخبرات.

البحرين: أفادت بما يلي:

١) شارك وفد مملكة البحرين في أعمال لجنة الخبراء الدولية المعنية بوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، والتي تم تشكيلها بموجب قرار الجمعية العامة للأمم المتحدة رقم (٢٤٧/٤٧).

٢) عقدت اللجنة حتى هذا التاريخ - خمس دورات خلال عامي (٢٠٢٢ و٢٠٢٣) بمشاركة واسعة من الوفود الممثلة للدول الأطراف بما في ذلك وفد مملكة البحرين والوفود العربية بجانب مشاركة

الوفود من غير الدول الممثلة للهيئات الدولية والأكاديمية وأصحاب المصلحة ومنظمات المجتمع المدني المتعلقة بمجالات: الأمن والجريمة والتكنولوجيا.

٣) شارك وفد مملكة البحرين في الجهود المبذولة لإعداد "وثيقة التفاوض الموحدة" والتي تعبر عن مرئيات الدول الأطراف في الاتفاقية الدولية.

٤) اشتملت مقترحات إدارة مكافحة الجرائم الإلكترونية بوزارة الداخلية في مملكة البحرين المقدمة إلى أمانة اللجنة الدولية خلال الدورتين الرابعة والخامسة مقترحات (بالتعديل والحذف والإضافة) للمواد والبنود والفقرات الفرعية من وثيقة التفاوض الموحدة، علاوة على مقترحات متعلقة بالنصوص والصياغة والمصطلحات المستخدمة تناولت الموضوعات الأساسية لمسودة الاتفاقية وفق الآتي:

أ- الديباجة
ب- الأحكام العامة
ت- الأحكام المتعلقة بالتجريم
ث- التدابير الإجرائية وإنفاذ القانون
ج- الأحكام المتعلقة بالتعاون الدولي
ح- المساعدة التقنية بما في ذلك تبادل المعلومات
خ- الأحكام المتعلقة بالتدابير الوقائية
د- آلية التنفيذ
ذ- الأحكام الختامية.

٥) أدمجت المقترحات المقدمة من إدارة مكافحة الجرائم الإلكترونية بوزارة الداخلية بمملكة البحرين مع المقترحات المدخلة على النسخة الختامية لوثيقة التفاوض الموحدة للاتفاقية.

وبناء على ذلك، توصي الجهات المختصة لديهم بالإيعاز لممثل الدول العربية في اللجنة الدولية المعنية بوضع الاتفاقية الدولية بتعميم البيانات والمقترحات التي سوف تصدر عن ممثل الدول العربية في اللجنة الدولية حتى يتسنى للدول الأعضاء دراستها ومراجعتها وإبداء مرئياتها قبل انعقاد الدورة السادسة في نيويورك في ٢١ أغسطس ٢٠٢٣.

السعودية: ترى مناسبة ما ورد في التوصية مع الأخذ بالاعتبار أن يتم عقد اجتماعات تشاورية بين الدول الأعضاء بهدف التنسيق حول الاتفاقية.

العراق: تؤيد ما جاء في التوصية بما لا يتعارض مع القوانين والتشريعات الوطنية، وتؤكد على تفعيل بنود الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

الكويت: أفادت أن جهاتهم المختصة تؤيد هذا المقترح بضرورة أن تصبح هناك اتفاقية دولية موحدة كما هو معمول في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث رغبت في تعزيز التعاون فيما بينهما لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعًا منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذًا بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها بشرطة ألا تتعارض هذه الاتفاقية الدولية مع قوانين دولة الكويت ودستورها.

كما أفادت أن دولة الكويت متمثلة بإدارة مكافحة الجرائم الالكترونية قد شاركت بشكل فعال في الاجتماعات التي نظمتها الأمم المتحدة بشأن بلورة اتفاقية دولية لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية وقد قامت بالإجابة على كافة الأسئلة المطروحة من قبلهم والتي يسر لها مشاركتها مع الأمانة العامة الموقرة حسبما جاء بالتوصية سالفة الذكر مع العلم بأن جهاتهم المختصة ترى مشاركة بيانات الأشخاص المعنيين بحضور الاجتماعات الافتراضية من قبل دول المجلس وذلك لتتمكن من توحيد الصفوف وتنسيق الآراء والانتهاء إلى رأي موحد بهذا الشأن.

البند الثاني

تجارب الدول الأعضاء في مواجهة جرائم تقنية المعلومات

في هذا البند استعرضت كل من الدول الآتية: (المملكة الأردنية الهاشمية – دولة الإمارات العربية المتحدة – مملكة البحرين) تجاربها وممارساتها المتميزة في مكافحة جرائم تقنية المعلومات على الصعيد الوطني لتحقيق الاستفادة المتبادلة وتقييم المخاطر ورصد التهديدات المشتركة.

كما تم التعليق على تلك التجارب، وأشاد الجميع بالجهود المبذولة لمواجهة جرائم تقنية المعلومات.

البند الثالث

التحديات الناشئة في مجال جرائم تقنية المعلومات

تناول هذا البند استعراضًا للمعالجة التي قدمتها الأمانة الفنية للفريق من خلال مرئيات الدول التي أجابت على ذلك، والتي تعد جزءًا من التوصيات الواردة في البند الأول حسب الآتي:

فقد قامت الأمانة الفنية متمثلة في المكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات بمخاطبة شعب الاتصال في الدول الأعضاء بالخطاب رقم ١٠٢ وتاريخ ٢٠٢٣/٣/٢٨م، والخطاب الإلحاقي رقم ١٩٥ وتاريخ ٢٠٢٣/٦/٥م، المتضمن موافاتها بأبرز التحديات الحديثة في هذا المجال والسبل المثلى لمواجهتها.

وبناءً على ذلك تلقى المكتب إجابات الدول الآتية: (المملكة الأردنية الهاشمية - مملكة البحرين - المملكة العربية السعودية - جمهورية العراق - دولة الكويت)؛ **يمكن عرضها في الآتي:**

الأردن: أفادت بأن أبرز القضايا التي يتم التعامل معها هي:

- قضايا الابتزاز والاحتيال الإلكتروني وقضايا برامج الفدية وتتلخص صعوبة التعامل مع هذه القضايا في قيام مرتكبيها باستخدام تقنية (VPN) وإخفاء الهوية الرقمية بالإضافة إلى اعتمادهم على العملات الرقمية لصعوبة تتبعها وتحديد مستخدميها.
- تقنية الذكاء الاصطناعي التي قد يستخدمها المجرمون لارتكاب الجرائم الإلكترونية.
- ضعف التواصل المباشر بين وحدات مكافحة الجرائم الإلكترونية والتعاون المشترك بينها.
- تفاوت آليات تعاون الشركات العالمية مع الدول على أسس سياسات خاصة بهم.
- عدم وجود برامج تدريبية دولية وإقليمية مشتركة في الأساليب الجرمية المستحدثة وآلية التعامل معها ومكافحتها.
- التعاون المشترك مع الدول الأعضاء والشقيقة في تبادل المعلومات على مستوى سلطات إنفاذ القانون.

البحرين: استعرضت موجزًا لأبرز التحديات الأمنية الناشئة التي تعترض مجال تقنية المعلومات، متضمنة المعطيات وآليات مواجهتها من منظور إدارة مكافحة الجرائم الإلكترونية بوزارة الداخلية في مملكة البحرين، وفق الآتي:

١- التكنولوجيا المالية وجرائم الاحتيال الإلكتروني

المعطيات: تشهد المجتمعات العربية تقدمًا ملحوظًا في عملية التحول الرقمي والاستفادة من تطبيقات التكنولوجيا الحديثة في الارتقاء بجودة تقديم الخدمات في مختلف القطاعات، وفي مقدمتها قطاع التكنولوجيا المالية، حيث توفر المصارف والمؤسسات المالية أنظمة دفع إلكترونية عبر شبكة الإنترنت والهواتف الذكية، فضلًا عن دمج أنظمة الدفع الإلكترونية بقطاع التجارة الإلكترونية وتجارة التجزئة والدعاية والإعلان واستضافة مواقع البيع وترويج السلع والمنتجات وخدمات شحن البضائع عبر الحدود.

وعلى الجانب الآخر، تؤشر التقديرات الأمنية على ارتفاع معدل جرائم الاحتيال الإلكتروني المرتبطة بقطاع التكنولوجيا المالية، التي تستهدف سرقة الأرصدة البنكية من حسابات الضحايا، حيث يعتمد المحتالون على أساليب مختلفة يأتي في مقدمتها الاحتيال عبر المكالمات الهاتفية والرسائل النصية، ورسائل البريد الإلكتروني من خلال إنشاء روابط الدفع الوهمية.

الاقتراح: إصدار توصية إلى الجهات المعنية في البلدان العربية بشأن تفعيل نظام "تعريف جهة الاتصال" عند استلام المكالمات والرسائل النصية على الهواتف الذكية، وبشكل خاص تعريف جهة الاتصال الخاصة بالبنوك والمؤسسات المالية وشركات الشحن والشركات التجارية المسجلة محليًا داخل كل بلد، بحيث تكون المكالمات والرسائل المستلمة موثوقة باسم الجهة المتصلة على هاتف الشخص المتلقي للمكالمة الهاتفية أو الرسالة النصية؛ مما يضعف من قدرة المحتالون من الاحتيال على الضحايا باسم البنك أو المؤسسة المالية أو الشركة التجارية أو شركة الشحن.

كما تم اقتراح إصدار نشرة فصلية تحت مظلة مجلس وزراء الداخلية العرب، تحتوي على تحديث لاتجاهات الجرائم الإلكترونية ذات الطبيعة المالية والأنماط والأساليب المستحدثة في ارتكابها، بهدف تعميمها على مؤسسات الأعمال الحيوية (الحكومية والأهلية) ولاسيما التي تنتمي لقطاعات المال والأعمال والمصارف والتجارة الإلكترونية وتقنية المعلومات.

٢. هجمات الفدية ومؤسسات الأعمال

المعطيات: تتواتر العديد من النشرات والتقارير الأمنية الدولية بشأن وجود سلالات متطورة من برمجيات الفدية، والتي تستهدف منظمات الأعمال الكبيرة والمتوسطة بشكل خاص، نظرًا لجدوى

استهدافها وقدرتها على دفع وتحويل المبالغ المالية المطلوبة لإزالة الأضرار التي يتمكن الجناة من إلحاقها بالمؤسسات المستهدفة، والتي تصبح هدفًا ثمينًا بالمقارنة باستهداف وإصابة أجهزة وحواسيب الأفراد.

الاقتراح: إصدار دليل استرشادي عربي، وقائي، لمساعدة منظمات الأعمال على اتباع الإجراءات الوقائية اللازمة لتأمين وحماية أنظمة التشغيل والخوادم والشبكات والأجهزة والحواسيب الخاصة بها من هجمات الفدية وكيفية التعامل معها في حالة الإصابة بها مع الجهات والسلطات المحلية.

كما تم اقتراح: إنشاء منصة عربية رقمية للإبلاغ السريع ومساعدة ضحايا هجمات الفدية، لمجلس وزراء الداخلية العرب. ويمكن الاستفادة في هذا الشأن بالمبادرة الأوروبية الخاصة بالشرطة الأوروبية اليوروبول No More Ransomware حيث قامت إدارة مكافحة الجرائم الإلكترونية في وزارة الداخلية بدعم المبادرة داخل مملكة البحرين.

٣- مو اقع التواصل الاجتماعي والألعاب الإلكترونية واستغلال الأطفال عبر الإنترنت

المعطيات: في الوقت التي تتزايد فيه أعداد مستخدمي وسائل التواصل الاجتماعي من فئة الشباب والنشء والفئات العمرية الأقل سنًا، وتتسارع أيضًا بالتوازي وتيرة صناعة الألعاب الإلكترونية وتجذب الكثيرين من كل الفئات العمرية حول العالم، تشهد منصات التواصل الاجتماعي والألعاب الإلكترونية اتجاهًا ناشئًا في الجرائم المتعلقة باستغلال الأطفال عبر الإنترنت، سواءً فيما يتعلق بجرائم الاستغلال الجنسي أو نشر وتداول المحتوى الجنسي أو جرائم التنمر والابتزاز الإلكتروني أو بث الأفكار المتطرفة أو ازدراء الأديان.

الاقتراح: دعم التوصية الصادرة عن فريق الخبراء العرب المعني بمكافحة الإرهاب التابع لمجلس وزراء الداخلية العرب، بشأن إنشاء منصة عربية رقمية لتصنيف الألعاب الإلكترونية، علما بأن إدارة مكافحة الجرائم الإلكترونية في وزارة الداخلية بمملكة البحرين قد تقدمت بتقرير تحليلي يتضمن مرئياتها إلى الجهات المعنية بشأن التصور المبدئي للمنصة.

٤. التوعية الأمنية واختراق وسرقة الحسابات الإلكترونية

المعطيات: لا يزال الوعي الأمني لمستخدمي تقنية المعلومات هو الحلقة الأضعف في تعزيز قدرات الأمن الإلكتروني على مواجهة التحديات والمخاطر المتصلة بتقنية المعلومات، إذ تشير العديد من الاستخلاصات المستندة إلى التحليلات الأمنية على انخفاض مؤشر الوعي الأمني للمستخدمين، وهو ما يظهر جليًا في الارتفاع النسبي للحالات المبلغ عنها لاختراق وسرقة الحسابات الإلكترونية.

الاقتراح: مناقشة فكرة إطلاق يوم عربي للتوعية الأمنية من مخاطر الجريمة الإلكترونية والاستخدام الآمن لتقنية المعلومات، وهو مقترح تقدمت به إدارة مكافحة الجرائم الإلكترونية في وزارة الداخلية بمملكة البحرين في أكثر من مناسبة وسياق أمني (خليجي وعربي)، بحيث يتم تسليط الضوء وتكثيف الجهود والحملات والبرامج التوعوية بشكل ممنهج في يوم محدد من كل عام، بما يؤدي إلى رفع الوعي الأمني لمستخدمي تقنية المعلومات في البلدان العربية.

السعودية: أفادت بأنه يمكن ايجاز التحديات الناشئة في مجال تقنية المعلومات بالآتي:

- ❖ التشفير.
- ❖ التحديات المتعلقة بحوكمة الإنترنت والعملات الرقمية وتتبعها.
- ❖ الاتجاهات الحديثة مثل المستوى المتزايد لإساءة الاستخدام الاجرامي للإنترنت المظلم (Tor,12p,free Intranet).
- ❖ التحديات المرتبطة بالأطر القانونية.
- ❖ تحديات الاستجابة للهجمات الإلكترونية واسعة النطاق.
- ❖ معوقات التعاون الدولي.
- ❖ تحديات الشراكات بين القطاعين العام والخاص.
- ❖ ارتفاع عمليات التصيد الالكتروني.
- ❖ استخدام العملات الرقمية لأغراض غير مشروعة.

العراق: أفادت بأن أهم التحديات التي تواجههم في مجال جرائم تقنية المعلومات ما يلي:

١. **الاحتيال الإلكتروني:**

من أهم التحديات الحديثة التي تواجه أجهزة إنفاذ القانون في مجال مكافحة جرائم تقنية المعلومات هو عمليات الاحتيال المالي الإلكتروني حيث تأشرت لديهم العديد من حالات الاحتيال الإلكتروني من خلال تلقي اتصالات وهمية وينتحل صفة عميل في أحد الشركات أو إرسال روابط وهمية يتم من خلالها إيهام الضحية وتعبئة بيانات البطاقة البنكية لتمكن المحتال من الحصول على بيانات الحساب البنكي ورمز الأمان (OTP) للضحية والاستيلاء على الأموال، بالإضافة إلى منصات تداول وهمية.

٢. **العملات الرقيمة (cryptocurrency)**

- استخدام العملات الرقيمة في تهريب العملة الصعبة خارج البلد وغسل الأموال بعيدًا عن سياقات التحويل المالي المتعارف عليها وخارج الضوابط من خلال شرائها لعدد كبير من المحافظ الإلكترونية واستلام المبالغ في دول أخرى.
- من خلال الاحتيال بتقديم عروض وخدمات للاستثمار والتداول بالعملات الافتراضية ومشاركة كلمات السر للحسابات مع المحتال بحجة إدارة الحساب وزيادة الأرباح، ويتم من خلالها الاستيلاء على أمواله.

٣. **المقترحات:**

أ- وضع مناهج تدريبية وإقامة ورش عمل مشتركة لتطوير عمل ضباط إنفاذ القانون العاملين في مجال مكافحة جرائم تقنية المعلومات في التعامل مع جرائم الاحتيال المعالي والعملات المشفرة وإصدار كراسات تعليمية في هذا المجال.

ب- عرض تجارب الدول الأعضاء تجاربها والتعليمات التنظيمية والتشريعية التي تخص التعامل مع العملات المشفرة على المستوى الوطني.

الكويت: أفادت بأن التحول الإلكتروني يشير إلى النقلة النوعية التي تحدث في العالم الرقمي وتضمن التقدم التقني والتحولات في التعامل مع البيانات والمعلومات والتواصل الإلكتروني، ومع ذلك فإن هذا التحول يأتي بتحديات أمنية واضحة فعندما يتم تحويل العمليات الأساسية والبيانات إلى شكل إلكتروني تزداد نسبة تعرضها للاختراق من قبل مجاميع التهديد، حيث إن أبرز

التحديات الناشئة والمخاطر التي تواجه المؤسسات والأفراد في مجال جرائم الفضاء السيبراني وتقنية المعلومات هي:

١. **الهجمات السيبرانية لأغراض تجسسية:** حيث يتم اختراق أنظمة المعلومات والشبكات السحابية لسرقة البيانات والمعلومات الحساسة الخاصة بالدولة بغرض التجسس وجمع المعلومات.
٢. **الهجمات السيبرانية لأغراض مالية:** حيث تقام عن طريق شن هجمات برامج الفدية (RANSOMWARE) على المؤسسات الحكومية أو الأفراد العاملين فيها ويتم أخذ نسخة من بيانات الضحية وتشفيرها لمنع الضحية من الوصول إليها حتى يتم دفع مبلغ مالي يحدده المخترق.
٣. **الهجمات السيبرانية لأغراض تخريبية:** مثل هجمات حرمان الخدمة (DDOS ATTACK) حيث يقوم المخترق باستغلال العديد من الأجهزة المخترقة (Botnet) لإغراق خوادم المواقع بطلبات وبيانات عديدة التي تؤدي إلى انهيار الشبكة وتعطيل المؤسسة من أداء عملها.
٤. **استخدام الاتصالات الوهمية عن طريق أجهزة الحاسب الآلي** (voip) والتي تمكن من استغلال هوية رقم هاتف لشخص آخر وإيهام الشخص مستقبل الاتصال بأنه يتم التواصل معه من قبل هاتف محلي على سبيل المثال " يرد للمجني عليه اتصال من رقم هاتف كويتي ويتبين بأن صاحب الخط لم يقم بإجراء ذلك الاتصال " وتسمى هذه البرمجة (الاتصال المخادع spoof calling) وطرق مواجهتها تكون عن طريق طلب كشوفات الحركة من المرسل والمستقبل ومقارنة الكشوف ووقت الاتصال حيث يتضح بأن هوية المتصل لا تظهر عند المستقبل.
٥. **الهجمات الإلكترونية مدفوعة الأجر من الإنترنت الداكن** (DDOS Attack) على شركات الدفع الإلكتروني بغية خلق نوع من المنافسة وحث تلك الشركات على دفع مبالغ مالية ضخمة لمفهوم التأمين السيبراني من الهجمات.
٦. **إشاعة الأخبار الكاذبة ونشر المعلومات غير الدقيقة ونسبها إلى السلطات الرسمية** باستخدام وسائل التواصل الاجتماعي حيث تعتبر أحد أهم الجرائم الإلكترونية التي تهدد

سير الحفاظ على أمن واستقرار البلاد لما تثيرها من هلع في نفوس المواطنين والمقيمين، ويجب على الدول العمل على تسخير كافة الجهود وما يتوفر من إمكانيات ومعلومات بشأن تلك الحسابات والتحذير منها عن طريق قنوات وسائل التواصل الاجتماعية الرسمية الخاصة بالدول.

٧. **الأسواق التجارية متناهية الصغر في مواقع التواصل الاجتماعي وبيع المنتجات الوهمية** أو غير المتوفرة والمتاجرة بأموال الغير (opm) وفي هذا الشأن يتم توعية المواطنين والمقيمين بخصوص تلك الأسواق والتأكيد على عدم دفع مبالغ مالية نظير شراء المنتجات إلا بعد استلام تلك المنتجات.

٨. **عدم تعاون شركات مواقع التواصل الاجتماعي** بتزويد الجهات الأمنية المختصة بالبيانات والمعلومات المتوفرة لديهم تحت ذريعة حماية خصوصية مستخدمي وسائل التواصل الاجتماعي.

٩. **التحويلات المالية:** عدم القدرة والسيطرة على التحويلات المالية بين بنوك دول الخليج والتي غالبًا يكون سببها روابط الدفع الإلكتروني من خلال التعامل مع حسابات وهمية تقوم بعمليات النصب والاحتيال المالي.

البند الرابع

مخاطر الابتزاز الإلكتروني

خلال هذا البند قدمت الأمانة الفنية لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات ورقة عمل تناولت فيه الابتزاز الإلكتروني من خلال عدة محاور تمثلت بالآتي:

- ❖ تعريف جرائم الابتزاز الإلكتروني
- ❖ دور وسائل التواصل الاجتماعي في التغيير الاجتماعي
- ❖ أركان وظروف جريمة الابتزاز الإلكتروني
- ❖ أنواع الابتزاز الإلكتروني
- ❖ إحصاءات متعلقة بجرائم بالابتزاز الإلكتروني
- ❖ أسباب الابتزاز الإلكتروني
- ❖ وسائل مكافحة الابتزاز الإلكتروني.
- ❖ التوصيات.

البند الرابع

تصـــور لإعداد آلية دورية لاســـتعراض ومراجعـة تنفيـذ مـا جـاء في الاتفـاقيـة العربية لمكافحة جرائم تقنية المعلومات

خلال هذا البند استعرضت الأمانة الفنية للفريق التصور المقترح حول إعداد آلية دورية يتم من خلالها استعراض ومراجعة تنفيذ ما جاء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على النحو الآتي:

مقدمة:

تنفيذًا للتوصية (سادسًا/ب) من توصيات الاجتماع الثاني لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات المنعقد بمقر جامعة الدول العربية – القاهرة- بتاريخ ٢١-٢٢/١١/٢٠٢٢م التي نصت على " الطلب من الأمانة الفنية للفريق التنسيق مع الأمانة الفنية لمجلس وزراء العدل العرب والأمانة الفنية لمجلس وزراء الاتصالات العرب، من أجل وضع تصور لإعداد آلية دورية يتم من خلالها استعراض ومراجعة ما جاء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وعرضها على اجتماع مقبل للفريق" وفقًا للمقترح الذي قدمته جمهورية مصر العربية، وبناءً عليه قامت الأمانة الفنية للفريق بالتنسيق لاستضافة أعمال اجتماع يعنى بهذا الشأن في مقرها بالرياض (المكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات) ووجهت الدعوات لكل من: الأمانة الفنية لمجلس وزراء العدل العرب، والأمانة الفنية لمجلس وزراء الاتصالات العرب، وجامعة نايف العربية للعلوم الأمنية لحضور الاجتماع بتاريخ ٩/٥/٢٠٢٣م لبحث الآلية المناسبة لمراجعة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من كافة الجوانب العدلية والأمنية والفنية للخروج بتصور شامل بهذا الشأن.

الهدف من مراجعة الاتفاقية:

تطوير الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من أجل تعزيز التعاون المتكامل بين الدول العربية في مجال مكافحة كافة أشكال الجرائم المستجدة في مجال تقنية المعلومات؛ لدرء أخطار تلك الجرائم حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

المبررات:

يظهر جليًا الدور الذي يفرضه التحول الرقمي وتطوراته المتتالية على الساحة العالمية؛ فقد وفرت تلك التقنيات الناشئة مزايا وخدمات متعددة؛ إلا أنها أظهرت مجموعة من التحديات والثغرات التي قد تشكل هاجسًا أمنيًا متزايدًا؛ ما يستلزم مواجهتها ومكافحتها للحد من خطورتها من خلال منظومة متكاملة من الاتفاقيات والمعاهدات والقوانين والتشريعات والسياسات والاستراتيجيات والبرامج والأنشطة على المستويات الوطنية والإقليمية والعالمية؛ لذلك فإن فكرة" تطوير آلية دورية لاستعراض ومراجعة تنفيذ ما جاء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" يُعدّ مطلبًا مهمًا؛ لمواكبة التطور المتسارع والتحولات التي يشهدها العالم في مجال الفضاء الافتراضي، والاعتماد عليه باعتباره واقعًا متّسع النطاق ويتعاظم باستمرار؛ ما يتطلب الحاجة الماسّة إلى تطوير منظومة الأمن السيبراني لحماية المجال السيبراني وسد ثغراته، لدعم منظومة الأمن العربي المشترك للامتثال إلى أفضل السبل والممارسات للتعامل مع الأخطار والمهددات ومعالجتها.

التصور المقترح:

يرى الفريق المشكّل من الأمانة الفنية للفريق، والأمانة الفنية لمجلس وزراء العدل العرب، والأمانة الفنية لمجلس وزراء الاتصالات العرب، وجامعة نايف العربية للعلوم الأمنية مناسبة الآتي:

- تتم مراجعة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال وزارات (الداخلية والعدل والاتصالات) العرب لمرة واحدة كل خمسة أعوام.
- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب بمتابعة مراجعات وزارات الداخلية العرب من خلال التركيز على المجال الأمني الوارد بالاتفاقية، والأمانة الفنية لمجلس وزراء العدل العرب بمتابعة مراجعات وزارات العدل العرب للمجال القانوني في الاتفاقية، وتقوم الأمانة الفنية لمجلس وزراء الاتصالات العرب بمتابعة مراجعة وزارات الاتصالات وتقنية المعلومات فيما يتعلق بالجوانب الفنية المضمنة بالاتفاقية.

- تقوم كل من: الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب والأمانة الفنية لمجلس وزراء الاتصالات العرب بإعداد تقرير يتضمن كافة الاجابات الواردة إليها وموافاة الأمانة الفنية لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات بذلك؛ ليتسنى لها إعداد تقرير شامل للمراجعة الدورية للاتفاقية العربية لمكافحة جرائم تقنية المعلومات من المنظورات الثلاث.
- عقد اجتماع لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات؛ للنظر في التقرير المعد من الأمانة الفنية للفريق بشأن المراجعة الدورية للاتفاقية العربية لمكافحة جرائم تقنية المعلومات وإجراء التعديلات اللازمة بشأنها، والتوصية برفع المشروع المحدّث من الاتفاقية على الاجتماع المشترك لمجلسي وزراء الداخلية والعدل العرب للنظر فيه.

مراحل المراجعة المقترحة:

١- إعداد خطة المراجعة للاتفاقية: بحيث تتضمن مجالات التركيز، وتحديد فريق المراجعة الفنية والصياغة التطويرية، والمخطط الزمني، والأدوار المطلوبة من جميع الجهات ذات العلاقة في المراجعة.

٢- ارسال تلك التحسينات المطلوبة على الاتفاقية للدول الأعضاء؛ من أجل المراجعة والتأكد من توافر متطلبات التنفيذ الوطنية، والاتساق مع الأنظمة والقوانين والتشريعات الوطنية، وبحث فرص التنفيذ الممكنة؛ من أجل إجازتها أو الرفع بالتعديلات المطلوبة خلال المدى الزمني المخطط في خطة المرجعة.

٣- استقبال المرئيات والردود التي ترد من الدول، وقيام الفريق الفني المشكّل للمراجعة بتطوير نموذج يأخذ بالاعتبار جميع تلك التحسينات المطلوبة من الدول الأعضاء، وفي حال وجود التعارضات فإنه يتم إعداد خيارات متعددة ومبرراتها؛ ووضع سيناريوهات لكل تعارض محتمل.

٤- قيام الفريق الفني المشكل لمراجعة الاتفاقية بعرض النموذج المطور وتعارضاته على اجتماع لاحق لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات خلال البند يتم

تخصيصه لأجل ذلك مع منح الفرصة الكافية لنقاشات الدول للخروج برأي توافقي حيالها أو الطلب بإعادتها للدول من أجل المراجعة اللاحقة والتأكد من مواءمة مكوناته مع السياق الوطني للدول الأعضاء.

٥- توثيق مشروع النسخة المطورة من الاتفاقية، ورفعها في اجتماع فريق الخبراء العرب المعني بمواجهة جرائم تقني المعلومات من خلال التوصيات التي يتم رفعها للمجالس المتخصصة واللجنة التنسيقية العليا من النظر فيها واتخاذ ما تراه في هذا السياق.

٦- تطوير الاستراتيجية العربية لمكافحة جرائم تقنية المعلومات وخطتها التنفيذية؛ بما يتماشى مع النسخة المعتمدة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المطورة؛ بحيث تشمل تطويرًا شاملًا يستوعب جميع المنظورات العدلية والتشريعية والفنية والأمنية المتخصصة.

٧- إعداد مخطط زمني من أجل التقييم المستمر لمحتويات الاتفاقية ومكوناتها.

البند الخامس

ما يستجد من أعمال

في هذا البند تم مناقشـــة التعاون مع الهيئات والمنظمات الإقليمية والدولية باعتباره من أهم الآليات لبناء وتطوير القدرات ،فمن خلال المشـــاركة العربية الفاعلة في اللقاءات والمنتديات الإقليمية والدولية المعنية بمواجهة جرائم تقنية المعلومات، يمكن معرفة إلى ماذا انتهى إليه الآخرون والاستفادة من التقارير الدولية المتخصصة بهذا الشأن، كما أنه ومن خلال التعاون مع هذه المنظمات والهيئات يمكن عقد المنتديات وتنظيم ورش العمل المتخصصة والتي سيكون من شأنها تطوير قدرات الفريق من خلال إيجاد شركاء إقليميين ودوليين يمتلكون الخبرة والرغبة لتحقيق الاستفادة المتبادلة في مواجهة جرائم تقنية المعلومات.

كما تم في هذا البند تقديم عرضين لجامعة نايف العربية للعلوم الأمنية عن الموضوعين الآتيين:
أولًا: جرائم الفدية: باعتبارها نوع خطير جدًا من الهجمات الإلكترونية في جميع أنحاء العالم.

وتضمنت المحاور الآتية:

- ❖ أبرز النتائج والاحصائيات في هذا الجانب:
- ❖ البلدان الأكثر عرضة لضحايا الفدية في الفترة الزمنية ما بين عامي (٢٠٢٠-٢٠٢٢م)
- ❖ أنواع منظمات الضحايا.
- ❖ خطوات صناعة الضحية.
- ❖ أهم ثلاث عصابات لبرامج الفدية خلال عام ٢٠٢٣م.
- ❖ ورش العمل الفنية التي ستعقدها الجتمعة في هذا الجانب.

ثانيًا: التهديدات السيبرانية: وتضمن المحاور الآتية:

- ❖ ذكاء التهديدات الإلكترونية على أساس جمع البيانات الحقيقية وتحليلها.
- ❖ الإجراءات الاستباقية والوقائية.
- ❖ الوعي بالتهديد.
- ❖ تقييم المخاطر والتخفيف من حدتها.
- ❖ تحسين صنع القرار.
- ❖ التعاون وتبادل المعلومات بين جميع الجهات ذات العلاقة.

البند السادس

التوصيات

وفي نهاية الاجتماع أوصى الفريق بالآتي:

أولًا: نتائج تطبيق توصيات الاجتماع الثاني للفريق

أ. تقديم الشكر للدول الأعضاء التي أجابت على مراسلات الأمانة الفنية للفريق، بشأن تنفيذ توصيات الاجتماع الثاني للفريق.

ب. الطلب من الأمانة الفنية للفريق إعداد مشروع تعريف موحد لجرائم تقنية المعلومات في ضوء المعطيات الواردة من الدول الأعضاء وعرضه على أعمال الاجتماع القادم للفريق بالتعاون مع جامعة نايف العربية للعلوم الأمنية.

ثانيا: تجارب الدول الأعضاء في مواجهة جرائم تقنية المعلومات

أ. تقديم الشكر للدول الأعضاء التي وافت الأمانة الفنية للفريق بتجاربها في مواجهة جرائم تقنية المعلومات، والطلب إلى الأمانة الفنية للفريق تعميم تلك التجارب على الدول الأعضاء للاستفادة منها.

ب. دعوة الدول الأعضاء الآتية: (الجمهورية التونسية – الجمهورية الجزائرية الديمقراطية الشعبية – جمهورية جيبوتي – المملكة العربية السعودية) لموافاة الأمانة الفنية للفريق بتجاربها في مجال مواجهة جرائم تقنية المعلومات لعرضها على أعمال الاجتماع الرابع للفريق والتركيز في هذا الجانب على موضوع (التحديات التي تواجه أجهزة إنفاذ القانون في مجال جرائم تقنية المعلومات).

ج. الطلب إلى جامعة نايف العربية إجراء دراسة وعقد ورشة عمل عن "الأساليب والاتجاهات الحديثة في جرائم تقنية المعلومات، وكيفية الوقاية منها، ومعالجتها عند حدوثها".

د. الطلب إلى جامعة نايف العربية تعميم التقرير الخاص بجرائم الفدية على الدول الأعضاء للاستفادة بما تضمنه التقرير من معطيات.

ثالثًا: التحديات الناشئة في مجال جرائم تقنية المعلومات

أ. تقديم الشكر للدول الأعضاء التي قامت بموافاة الأمانة العامة للفريق بالتحديات التي تواجهها في مجال جرائم تقنية المعلومات والطلب من الأمانة الفنية للفريق تعميمها للدول الأعضاء للاستفادة منها.

ب. الطلب من الأمانة الفنية للفريق تعميم الورقة التي أعدتها بعنوان "الابتزاز الإلكتروني ومخاطره" على الدول الأعضاء للاستفادة منها.

رابعًا: التصور المتعلق بإعداد آلية دورية لاستعراض ومراجعة تنفيذ ما ورد بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات

- الطلب من الأمانة الفنية للفريق تعميم التصور المقترح الذي أعدته حول "إعداد آلية دورية لاستعراض ومراجعة تنفيذ ما ورد بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات" على وزارات الداخلية والعدل العربية لإبداء مرئياتها حياله، وعرض النتائج على اجتماع مقبل للفريق.

خامسًا: ما يستجد من أعمال

أ. الطلب من الأمانة الفنية للفريق تخصيص بند على جدول أعمال الاجتماع المقبل الفريق يتعلق بالتعاون مع الهيئات والمنظمات الإقليمية والدولية المعنية بمواجهة جرائم تقنية المعلومات، على أن تقوم الأمانة الفنية للفريق بدعوة ممثلين عن تلك المنظمات المتخصصة للمشاركة في اجتماع الفريق بصفة مراقب، وذلك لبحث سبل التعاون وآليات عقد الأنشطة المشتركة.

ب. الطلب من الأمانة العامة لمجلس وزراء الداخلية العرب تقديم عرض عن نظام الشيخ زايد للاتصالات العصري بين أجهزة مجلس وزراء الداخلية العرب على أعمال الاجتماع المقبل للفريق.

سادسًا: الاجتماع القادم للفريق:

عقد الاجتماع القادم للفريق في مقر جامعة الدول العربية (القاهرة) في الربع الأخير من العام ٢٠٢٣م، والطلب من الأمانة الفنية لمجلس وزراء العدل العرب والأمانة الفنية لمجلس وزراء الاتصالات العرب

إجراء التنسيق اللازم حيال ذلك، وإشعار الأمانة الفنية للفريق بالتواريخ المحددة بوقت كافٍ؛ لإكمال اللازم فيما يخصها.

وفي ختام الاجتماع تقدم أعضاء الفريق بتقديم أسمى آيات الشكر والتقدير لسعادة العقيد/ أكثم عبدالمجيد النمورة رئيس الاجتماع الحالي لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات على حسن إدارته لجلسات الاجتماع، وتقديم جزيل الشكر للأمانة الفنية للفريق على التنظيم المتميز والتنسيق المتكامل لأعمال الاجتماع.

أسماء المشاركين في الاجتماع الثالث لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات
تونس- الجمهورية التونسية
١٢-١٣/٧/٢٠٢٣م

المملكـة الأردنيـة الهـاشميـــة

الاســـم	الجهة/الصفـــــة
١. النقيب/ سجى جسار عيـوش	وزارة الداخلية
٢. م١/ صالح رشاد سعيد	وزارة الداخلية
٣. السيد/ محمد الجوهـري	المركز الوطني للأمن السيبراني
٤. م/ ليليان رياض العميان	المركز الوطني للأمن السيبراني

دولـة الامـارات العربيـة المتحـدة

الاســـم	الجهة/الصفـــــة
١. عقيد.د/ ابراهيم حميد المياحي	وزارة الداخلية
٢. السيد مبارك سعيد الهاملي	وزارة الداخلية
٣. المستشار/خالد مبارك المدحاني	وزارة العدل

مملكـة البحـريـــن

الاســـم	الجهة/الصفـــــة
الرائد/ محمد يوسف بوعلي	وزارة الداخلية

الجمهـوريـة التـونسيـــة

الاســـم	الجهة/الصفـــــة
١. السيدة/ ولاء تركي	وزارة تكنولوجيا الاتصال
٢. السيد/ ياسين جميل	وزارة تكنولوجيا الاتصال
٣. السيد/ حيدر الهراغي	وزارة تكنولوجيا الاتصال
٤. عقيد/ مهدي حسن هويشي	وزارة الداخليـة
٥. محافظ شرطة أعلى/ جيهان المليتي	وزارة الداخلية
٦. محافظ شرطة عام صنف ثاني/ رياض السليطي	وزارة الداخلية
٧. محافظ شرطة أول/ فوزي يوسف الرياحي	وزارة الداخلية
٨. عقيد/ الناصر ثابوتي	وزارة الداخلية

٩. الرائد/عصام الريحاني	وزارة الداخلية

الجمهورية الجزائرية الديمقراطية الشعبية

الاســـم	الجهة/الصفـــــة
١. محافظ الشرطة/ كرفاح مصطفى	وزارة الداخلية

المملكة العربية السعوديـــة

الاســـم	الجهة/الصفـــــة
١. لواء/ ملوح بن فلاح أبو جلبة	وزارة الداخلية
٢. فضيلة الشيخ/ سليمان بن عبد الكريم العليان	وزارة العدل
٣. عقيد.م/ عبدالرحمن بن عنيت الله المطيري	رئاسة أمن الدولة
٤. مهندس/ المثني بن فريح العقلاء	وزارة الاتصالات
٥. مهندس/ عبدالله الربيعان	الهيئة الوطنية للأمن السيبراني
٦. نقيب/عبدالإله سعد العريفي	وزارة الداخلية
٧. م١/ عبدالرحمن بن حمد الباتلي	وزارة الداخلية
٨. السيد/ عبد العزيز بن صالح الشعيبي	وزارة الداخلية

جمهوريـــة العـــراق

الاســـم	الجهة/الصفـــــة
١. الرائد/ أحمد علي حسين جاسم	وزارة الداخلية
٢. السيدة /شيماء مزهر ثعبان	وزارة الاتصالات
٣. السيدة/ انتصار سليمان محمد	وزارة الاتصالات

سلطنـة عُمـــان

الاســـم	الجهة/الصفـــــة
١. المقدم/ يحيى الصوافي	وزارة الداخلية

٢. النقيب/ مطر الكلباني	وزارة الداخلية

دولة فلسطيـــن

الاســـم	الجهة/الصفـــــة
١. عقيد/ أكثم عبدالمجيد موسى النمورة	وزارة الداخلية
٢. المقدم د. رهام سائد أحمد جبر ناصر	وزارة الداخلية

دولـة قطـــر

الاســـم	الجهة/الصفـــــة
١. النقيب/ جاسم محمد الكواري	وزارة الداخلية
٢. النقيب/ عبدالرحمن عبدالله البوعينين	وزارة الداخلية
٣. السيد/ محمد مرشد المناعي	الوكالة الوطنية للامن السيبراني
٤. الأستاذ/ محمد المري	وزارة العدل

جمهورية القمر المتحدة

الاســـم	الجهة/الصفـــــة
السيد/ موسى آدم	وزارة الداخلية

دولة الكويـــت

الاســـم	الجهة/الصفـــــة
١. عقيد/ حمد محمد الحمود	وزارة الداخلية
٢. نقيب/ عيسى صلاح الدين الشهاب	وزارة الداخلية

دولـــة ليبيـــا

الاســـم	الجهة/الصفـــــة
١. عميد/ حسين امحمد سالم سويسي	وزارة الداخلية
٢. مهندس/ مهند علي منصور طلحة	وزارة الداخلية
٣. موظف/ أحمد جمعة سالم غومة	وزارة الداخلية

جمهورية مصر العربيـــة

الاســـم	الجهة/الصفـــــة
عميد/ محمد علي البرنس	وزارة الداخلية

المملكة المغربيـــة

الاســـم	الجهة/الصفـــــة
١. عميد شرطة ممتاز/ المهدي بوعبادي	وزارة الداخلية
٢. القاضي/ محمد أمين الجردانى	وزارة العدل

الجمهورية الإسلامية الموريتانيـة

الاســـم	الجهة/الصفـــــة
١. السيد/ محمد انتليت	وزارة الداخلية
٢. السيد/ ديدي الحسين	وزارة التحول الرقمي

مجلس التعاون لدول الخليج العربية

الاســـم	الصـفـــــة
أ/ مشعل صقر السعدون	إدارة التواصل الأمني الدولي

جامعة الدول العربية (الأمانة الفنية لمجلس وزراء العدل العرب)

الاســـم	الصـفـــــة
مستشار/ الحسين الاكحل	إدارة الشؤون القانونية

جامعة نايف العربية للعلوم الأمنيـة

الاســـم	الصـفـــــة
د. عبدالرزاق المرجـان	مدير مركز الجرائم السيبرانية والأدلة الرقمية

مجلس وزراء الداخلية العــرب

الاســـم	الصـفـــــة
١. د/ عبدالله بن أحمد الشعلان	الأمين العام المساعد
٢. العقيد. د/ نايف بن سليمان المطلق	مـدير المكتـب العربي لمكـافحـة الارهـاب وجرائم تقنية المعلومات
٣. المهندس/ خالد بن بندر الشلهوب	المكتـب العربي لمكـافحـة الارهـاب وجرائم تقنية المعلومات
٤. الرائد/ فيصل بن حسن القحطاني	المكتب العربي لمكافحة الارهاب وجرائم تقنية المعلومات
٥. الأستاذ/ عبد ربه العساف	مكتب الأمين العام