تقرير وتوصيات

الاجتماع الثاني لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات

الأمانة العامة لجامعة الدول العربية – القاهرة

في تاريخ (٢١-٢٢/١١/٢٠٢٢م)

إعداد:

الأمانة الفنية لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات

****

التقرير

تنفيذًا للتوصية سابعًا من توصيات الاجتماع الأول لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات المنعقد بتاريخ ٢٠٢٢/٥/١٨م في مقر جامعة نايف العربية للعلوم الأمنية بالرياض الذي نصت على "عقد الاجتماع القادم للفريق في مقر جامعة الدول العربية بالقاهرة في الربع الأخير من هذا العام، والطلب من الأمانة الفنية للفريق التنسيق في ذلك مع الجهات ذات الصلة"؛ وبناءً عليه قامت الأمانة العامة للمجلس بالتنسيق مع الأمانة العامة لجامعة الدول العربية لاستضافة أعمال هذا الاجتماع بمقرها في مدينة القاهرة بجمهورية مصر العربية، وتوجيه الدعوة للدول الأعضاء ومؤسسات العمل العربي المشترك لحضور الاجتماع في الفترة (٢١-٢٢/١١/٢٠٢٢م) بموجب التعميم رقم ١١٣٢ وتاريخ ٢٠٢٢/٩/١٣م ، وتم عقد الاجتماع بحضور وفود تمثل الدول الأعضاء الآتية:

المملكة الأردنية الهاشمية، دولة الإمارات العربية المتحدة، مملكة البحرين، الجمهورية التونسية، الجمهورية الجزائرية الديموقراطية الشعبية، المملكة العربية السعودية، جمهورية السودان، جمهورية العراق، سلطنة عمان، دولة فلسطين، دولة قطر، دولة ليبيا، المملكة المغربية، جمهورية مصر العربية، والجمهورية الإسلامية الموريتانية. كما حضر كذلك الاجتماع ممثلون عن الأمانة العامة لمجلس وزراء الداخلية العرب وجامعة نايف العربية للعلوم الأمنية، والأمانة الفنية لمجلس وزراء العدل، والأمانة الفنية لمجلس وزراء الاتصالات، وعدد من مؤسسات العمل العربي المشترك.

وقد تضمن جدول أعمال الاجتماع البنود التالية:

١. نتائج تطبيقات توصيات الاجتماع الأول للفريق.
٢. تجارب الدول الأعضاء في مواجهة جرائم تقنية المعلومات.
٣. التحديات الناشئة في مجال جرائم تقنية المعلومات.
٤. تحديد الأولويات بشأن بنود اجتماعات الفريق.
٥. استعراض الإطار العربي الموحد لمواجهة القرصنة الإلكترونية وحماية الشبكات.
٦. ما يستجد من أعمال.

وفي الساعة العاشرة من صباح يوم الاثنين ٢٠٢٢/١١/٢١م، افتتح سعادة العقيد مهندس/ عبدالرحمن بن مبارك الشطي أعمال الاجتماع الثاني لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات بكلمة رحّب فيها بالسادة المشاركين في أعمال الاجتماع الثاني، متمنيًا للفرق العربية المشاركة في بطولة كأس العالم لكرة القدم كل التوفيق في مشوارها الكروي باستضافة كريمة من دولة قطر، معربًا عن أمله وتمنياته بنجاح أعمال هذا الاجتماع.

البند الأول

نتائج تطبيق توصيات الاجتماع الأول للفريق

التوصية رابعًا/ أ:

الموافقة على البنود المقترحة، والطلب من الأمانة الفنية للفريق التنسيق مع مؤسسات العمل العربي المتخصصة لإعداد ما يلزم بشأن هذه البنود وعرض النتائج على الاجتماع القادم للفريق.

وقد اشتملت البنود على 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

قام المكتب العربي لمكافحة التطرف والإرهاب بمخاطبة شعب الاتصال في الدول الأعضاء بخطابة رقم ٤٩٠ وتاريخ ٢٠٢٢/٩/١٥م المتضمن أن الطلب من الوزارات الراغبة في عرض تجاربها بهذا الشأن على أعمال الاجتماع الثاني.

النتائج

تلقى المكتب إجابات الدول الآتية: (مملكة البحرين - الجمهورية الجزائرية الديموقراطية الشعبية - جمهورية العراق – الجمهورية اللبنانية) وكانت الإجابات على النحو الآتي:

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 المشرّع 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 الشرطة: مما حقق عنصر السرعة في الاستجابة 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.

٣. المجتمع والتوعية من الجريمة الإلكترونية

- يشكل عامل التوعية الأمنية للمستخدمين حجر الزاوية في استراتيجية إدارة مكافحة الجرائم الإلكترونية، انطلاقًا من 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 نشر البرامج التوعوية لطرق الاستخدام الآمن لتكنولوجيا الاتصالات 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 إيصال رسالة التوعية إلى الشرائح المستهدفة من المواطنين والمقيمين داخل المجتمع البحريني.
- كما تستهدف برامج التوعية الأمنية الأطفال والطلاب في المدارس والجامعات من أجل التوعية من الاتجاهات الإجرامية الحديثة والمخاطر المرتبطة بها مثل التنمر الإلكتروني واستغلال الأطفال عبر الإنترنت والابتزاز على مواقع التواصل الاجتماعي وغيرها من الأنشطة الإجرامية التي تستهدف بشكل خاص فئة النشء والشباب.
- تتبنى الإدارة سياسة الالتزام بخصوصية البيانات والمعلومات الخاصة بالمبلغين من النشر الصحفي والإعلامي، كما تحظر مشاركة 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.

٤. التعاون الأمني

- يمثل التعاون الأمني مرتكزًا رئيسيًا في الاستراتيجية الأمنية لمكافحة الجرائم الإلكترونية، مستندًا في ذلك على تشـييد جسـور التعاون الأمني وتبادل المعلومات والخبرات بين إدارة مكافحـة الجرائم الإلكترونيـة والجهـات الفـاعلـة ذات العلاقـة والارتبـاط على مختلف الأصعدة.
- بشـكل منهجي، تتعاون الإدارة على المسـتوى الوطني مع الوحدات الأمنية والمؤسـسـات الوطنية داخل مملكة البحرين، وعلى المستوى الإقليمي يتكامل التعاون الأمني بين الدول الأعضـاء في مجلس التعاون لدول الخليج العربية ومجلس وزراء الداخلية العرب، وذلك إضـافة إلى المسـتوى الدولي للتعاون مع المنظمات الحكومية الدولية وهيئات المجتمع الدولي.
- يسـهم فريق التحليل والدراسـات الأمنية التابع للإدارة في دراسـة الأنشـطة الإجرامية المتصـلة بمنظومة الأمن الإلكتروني، وتحليل بيئة المخاطر الأمنية ورصـد مؤشـرات الجريمة والاتجاهات الناشئة في ارتكابها، واستراتيجيات مواجهتها، حيث يضطلع باحثو الإدارة بإصدار البحوث والدراسات والتقارير والنشرات الأمنية في هذا الشأن.
- تشـارك الإدارة بأوراق العمل والمقترحات والتوصـيات والمرئيات الأمنية في المجالات المتعلقة بمنظومة الأمن الإلكتروني ومكافحة الجرائم الإلكترونية والأنشـطة الإجرامية المتصلة بها، على الصعيدين الإقليمي والدولي: والتي من أبرزها:

❖ أعمال الدورة التنظيمية للجنة الحكومية الدولية المفتوحة العضوية المكلفة بوضع

- ❖ اتفاقية دولية شـــاملة بشـــأن مكافحة اســـتخدام المعلومات وتكنولوجيا الاتصـــالات للأغراض الإجرامية، وذلك بالتعاون مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة.
- ❖ اجتماعات فريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات.
- ❖ اللجنة المتخصـــصـــة بالجرائم المســـتجدة، والمعتمدة من قبل مجلس وزراء الداخلية العرب.
- ❖ مؤتمر التفاعل وتدابير بناء الثقة في أســـيا (CICA) ومشـــروع التعاون في مجال أمن تكنولوجيا المعلومات والاتصالات واستخدامها.
- ❖ الاتفاقيات الثنائية ومذكرات التعاون المشـــترك بين مملكة البحرين وبلدان العالم في المجالات الأمنية وتعزيز قدرات مكافحة الجرائم الإلكترونية، عبر القنوات الدبلوماسـية ووزارة الخارجية البحرينية.
- ❖ اللجنة الدائمة للأمن السيبراني بدول مجلس التعاون لدول الخليج العربية.
- ❖ متابعة تنفيذ بنود الخطة المرحلية لتنفيذ الاســـتراتيجية العربية لمواجهة جرائم تقنية المعلومات.

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

الجزائر: أفادت بأنها اعتمدت مجموعة من الآليات لمواجهة جرائم تقنية المعلومات، منها الوقائية والردعية، حيث تم بهذا الخصـــوص ســـن ترســـانة من القوانين لمجابهة هذا النوع من الإجرام، مواكبةً للتطورات الحاصلة في هذا المجال، حيث أصدر المشروع قانون ٠٩-٠٤ المتعلق بالقواعد الخاصـة بالوقاية من الجرائم المتصـلة بتكنولوجيات الإعلام و الاتصـال ومكافحتها، بالإضـافة إلى ما جاء في قانون العقوبات الجزائري بخصـوص المسـاس بأنظمة المعالجة الآلية للمعطيات ضـمن المواد القانونية من ٣٩٤ مكرر إلى ٣٩٤ مكرر ٧، كما تم اسـتحداث المادة ٨٧

مكرر ١١ و ٨٧ مكرر ١٢ المتضمنتان استخدام تكنولوجيات الإعلام والاتصال لأغراض إرهابية، بالإضـــافة إلى القانون ٠٥-١٨ المؤرخ في ١٠ مايو ٢٠١٨م الذي ينظم التجارة الإلكترونية و كذا قانون ١٨-٠٧ المتعلق بحماية الأشـخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

كما تم استحداث لدى المصالح الأمنية أجهزة مكلفة بمتابعة و مكافحة جرائم تقنية المعلومات، على غرار المصـلحة المركزية لمكافحة الجرائم السـيبرانية، بالإضـافة إلى الفرق التابعة لها المتواجـدة على مسـتوى ٥٨ أمن ولايـة التي تعنى بمكـافحـة هـذا النوع من الإجرام، كمـا تم اسـتحداث الهيئة الوطنية لمكافحة الجرائم المتصـلة بتكنولوجيات الإعلام و الاتصـال، والتي تقوم باقتراح عناصـر الاسـتراتيجية الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيات الإعلام والاتصـال ومكافحتها، ومسـاعدة السـلطات القضـائية ومصـالح الشـرطة القضـائية في مجال مكافحـة هـذه الجرائم من خلال جمع المعلومـات والتزويـد بهـا من خلال الخبرات القضـــائيـة، بالإضـافة إلى تجميع وتسـجيل وحفظ المعطيات الرقمية وتحديد مصـدرها ومسـارها من أجل استعمالها في الإجراءات القضائية.

بالإضـافة إلى توفر أقسـام خاصـة بالأدلة الرقمية، بمخابر الشـرطة العلمية والتقنية والذي يحوز على عتاد وتطبيقات في هذا المجال للكشـف والتعامل مع الأدلة الرقمية، كما تتوفر المخابر الجهوية التابعة لها.

عقد دورات تكونية في مجال مكافحة جرائم تقنية المعلومات لفائدة محققي الجرائم السيبرانية، بالإضـــافة إلى تكوين ضـباط دول عربية وتبادل الخبرات لتطوير قدرتها والاطلاع على كافة المستجدات في مجال الأمن المعلوماتي.

العراق: أفادت أن التطور السـريع الذي شـهده العراق في اسـتخدام التكنولوجيا الحديثة والانتشار الواسع لاستخدام مواقع التواصـل حيـث أصبحت هذه المواقـع مـن الأمور الحياتية المهمة وأداة مساعدة وفاعلة في تطوير وتنميـة المؤسسات العامـة وتمكنهم من التقدم وتقديم الخدمات وقد كانت الدول المتقدمة سـباقة في اسـتخدامها، ومواكبتها، وأصـبح من الصـعوبة الاسـتغناء عنها، لكن في المقابل أفرزت أنواعًا جديدة من الجرائم يطال كل المجمعات البشـرية 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 الالكتروني.

٢. الإرهاب الالكتروني.

٣. الاخبار الكاذبة والإشاعات.

أولًا" الابتزاز الالكتروني

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.

ثانيًا: الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنيات المعلومات

هي الجرائم التي تشكل تحدي للعاملين في مجال مكافحة الإرهاب حيث يقوم الإرهابيون 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 الالكتروني

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 فنية 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.

ثالثًا: الأخبار الكاذبة و البروباغندا، والجيوش الإلكترونية في مو اقع التواصل الاجتماعي

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 لعدد 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 برصد الشائعات وخاصة في المنصات الإلكترونية باعتبار أن مواقع التواصل الاجتماعي أرض خصبة لانتشار الشائعات ورفعها إلى الجهات المختصة ذات العلاقة.

٢. محاسبة مطلقي الاشاعات وفق القانون

إلقاء القبض بحق مطلق الإشاعة وفق القانون من المادة ٧٩ التي تؤكد على عقوبة السجن 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 فئة الشباب لأنه وفق الاحصائيات فإن أكثر الأخبار المتداولة من الشباب عن طريق مواقع التواصل الاجتماعي.

لبنان: أفادت أنه لا يوجد لديها تجارب حول مواجهة جرائم تقنية المعلومات.

ثانيًا: التحديات الناشئة في مجال جرائم تقنية المعلومات

الإجراءات

قام المكتب العربي لمكافحة التطرف والإرهاب بمخاطبة شعب الاتصال في الدول الأعضاء بخطابة رقم ٤٩١ وتاريخ ٢٠٢٢/٩/١٥م المتضمن موافاته بأبرز التحديات الحديثة في هذا المجال والسبل المثلى لمواجهتها.

النتائج

تلقى المكتب إجابات الدول الآتية: (مملكة البحرين - الجمهورية الجزائرية الديموقراطية الشعبية - جمهورية العراق - دولة قطر- دولة الكويت - الجمهورية اللبنانية) وكانت الإجابات على النحو الآتي:

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: تشـهد المجتمعات العربية تقدمًا ملحوظًا في عملية التحول الرقمي والاسـتفادة من تطبيقات التكنولوجيا الحديثة في الارتقاء بجودة تقديم الخدمات في مختلف القطاعات، وفي مقدمتها قطاع التكنولوجيا المالية، حيث توفر المصـارف والمؤسـسـات المالية أنظمة دفع إلكترونية عبر شـبكة الإنترنت والهواتف الذكية، فضـلًا عن دمج أنظمة الدفع الإلكترونية بقطاع التجارة الإلكترونية وتجارة التجزئة والدعاية والإعلان واسـتضـافة مواقع البيع وترويج السلع والمنتجات وخدمات شحن البضائع عبر الحدود.

وعلى الجانب الآخر، تؤشـر التقديرات الأمنية على ارتفاع معدل جرائم الاحتيال الإلكتروني المرتبطة بقطاع التكنولوجيا المالية، التي تسـتهدف سـرقة الأرصـدة البنكية من حسـابات الضـحايا، حيث يعتمد المحتالون على أسـاليب 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 الاتصـال الخاصـة بالبنوك والمؤسـسـات المالية وشـركات الشـحن والشـركات التجارية المسـجلة محليًا داخل كل بلد، بحيث تكون المكالمات والرسـائل المسـتلمة موثوقة باسـم الجهة المتصلة على هاتف الشخص المتلقي للمكالمة الهاتفية أو الرسالة النصية؛ مما يضعف من قدرة المحتالون من الاحتيال على الضـحايا باسـم البنك أو المؤسـسـة المالية أو الشـركة التجارية أو شركة الشحن.

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

٢. جمات الفدية ومؤسسات الأعمال

المعطيات: تتواتر العديد من النشـرات والتقارير الأمنية الدولية بشـأن وجود سـلالات متطورة من برمجيات الفدية، والتي تسـتهدف منظمات الأعمال الكبيرة والمتوسـطة بشـكل خاص، نظرًا لجدوى اسـتهدافها وقدرتها على دفع وتحويل المبالغ المالية المطلوبة لإزالة الأضـرار التي يتمكن الجناة من إلحاقها بالمؤسسات المستهدفة، والتي تصبح هدفًا ثمينًا بالمقارنة باستهداف وإصابة أجهزة وحواسيب الأفراد.

الاقتراح: إصـدار دليل اسـترشـادي عربي، وقائي، لمسـاعدة منظمات الأعمال على اتباع الإجراءات الوقائية اللازمة لتأمين وحماية أنظمة التشـغيل والخوادم والشـبكات والأجهزة والحواسـيب الخاصـة بها من هجمات الفدية وكيفية التعامل معها في حالة الإصـابة بها مع الجهات والسلطات المحلية.

كما تم اقتراح: إنشاء منصة عربية رقمية للإبلاغ السريع ومساعدة ضحايا هجمات الفدية، لمجلس وزراء الداخلية العرب. ويمكن الاسـتفادة في هذا الشـأن بالمبادرة الأوروبية الخاصـة بالشـرطة 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 مسـتخدمي وسـائل التواصـل الاجتماعي من فئة الشـباب والنشء والفئات العمرية الأقل سـنًا، وتتسـارع أيضًـا بالتوازي وتيرة صـناعة الألعاب الإلكترونية وتجذب الكثيرين من كل الفئات العمرية حول العالم، تشـهد منصـات التواصـل الاجتماعي والألعاب الإلكترونية اتجاهًا ناشـئًا في الجرائم المتعلقة باسـتغلال الأطفال عبر الإنترنت، سـواءً فيما يتعلق بجرائم الاسـتغلال الجنسـي أو نشـر وتداول المحتوى الجنسـي أو جرائم التنمر والابتزاز الإلكتروني أو بث الأفكار المتطرفة أو ازدراء الأديان.

الاقتراح: دعم التوصـية الصـادرة 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 الأمن 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.

الجزائر: أفادت أن التطور السريع لتكنولوجيات الإعلام والاتصال ساهم بشكل كبير في تطور الجريمة المعلوماتية وتعقيده لاسيما في عمليات التحقيق والتحري، وبالأخص ما يتعلق بهجمات فيروسات الفدية " Ransomware ، والتصيد الاحتيالي " Phishing " ... إلخ.

كما أفادت أيضًا بالآتي:

- تداول العملات الرقمية المشفرة، ساهم في تفاقم نشاطات إجرامية عبر شبكة الإنترنت وبالأخص في الإنترنت المظلم.
- تواجد معظم خوادم مقدمي خدمات الإنترنت، في دول أجنبية تخضع لقوانين تلك الدول مما يصعب عملية استرجاع الأدلة الإلكترونية نظرًا لعدم وجود قانون دولي موحد يسهل هذه العملية.

- نشـاط القراصـنة ضـمن مجموعات تضـم أعضـاء من مختلف البلدان، يصـعب عملية تحديد هويتهم عندما يتم استهداف المعلومات الحساسة لمختلف الدول.
- نشـــاط بعض الأشـخاص في مجموعات مغلقة عبر تطبيقات المســـنجر والواتس آب في نشر محتويات خاصة بإباحة الأطفال يصّعب عملية رصد هذه المجموعات.

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

١. التشريع القانوني

التحدي الأكبر الذي يواجه جهود مكافحة الجرائم التقنية في العراق هو عدم امتلاك العراق لقانون جرائم إلكترونية مستقل ينص ويعالج الجرائم الإلكترونية ويعرف المصطلحات التقنية ويضيفها للقانون العراقي المعمـــول به في العراق، علمًا أن الأجهـــزة الأمنية والمختصين والبرلمان العراقي ومنظمات المجتمع المدني والناشطين أعدوا مسودة قانون للجرائم المعلوماتية توازن بين ضـــمان حرية الرأي وبين مكافحة الجرائم الإلكترونية. كما أن بلادهم تعالج بعض الجرائم الإلكترونية بصعوبة وفق قانون العقوبات العراقي.

٢. صعوبة التعامل مع الجرائم التقنية و انباتها والتوصل إلى مرتكبيها

تتميز الجريمة المعلوماتية بصـــعوبة اكتشـــافها من الناحية الفنية لوجود العديد من المحددات على مســـتوى الجريمة وظروفها وعلى مســـتوى البنى التحتية للبلد، ويمكن إدراج أهم الأســـباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى ما يلي:

- عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية.
- الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى فهي جريمة عابرة للوطنية.
- صـــعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذا يســـتطيع المجرم المعلوماتي في أقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكمبيوتر.
- صعوبة العلم بوقوع الجريمة:

في الجرائم غير الرقمية يعلم المجني عليه بوقوع الجريمة التي وقعت عليه في الغالب وقت وقوعهـــا، ولكن في الجرائم الرقمية قد لا يعلم المجني عليه بوقوع الجريمة ضده أو الاعتداء

عليه بالتشـهير أو التجسـس من خلال جهاز أو اختراق أجهزته أو سـحب أموال عن طريق سرقة أرقام بطاقته الائتمانية، إلا بعد مدة وذلك بالطبع يصعب من عملية تطبيق القوانين الجنائية المتعلقة بهذه الجرائم إما لضـياع أدلة أو أن هذه المدة أتاحت للمجرم من مسـح آثاره في اعتداءه.

- صعوبة تعيين الجاني

اتخـاذ الجنـاة أسـمـاء مسـتعـارة يرتكبون بهـا جرائمهم أو أن يرتكـب جريمتـه عن طريق اسـتخدام أماكن عامة كالمقاهي المنتشـرة في البلاد والمكتبات العامة وخصـوصًـا تلك التي لا تطلب توثيق لشـخصـيـة المسـتخدم يصـعـب من عملية فرض وتطبيق القوانين الجنائية المتعلقة بالجرائم الإلكترونية بحيث يصعب تحديد مكان الجاني ومعرفة هويته.

- صعوبة القبض على الجاني

إذا تم ارتكاب جريمة رقمية بواسطة شخص أو أشخاص خارج الوطن فإن عملية القبض علـى الجـانـي تكون صعبة وتتطلـب تدخل الإنتربول الدولي وذلك لحدوث تضاد في القوانين اللازم تطبيقها في مثل هذه الحالات بين دولة الجاني دولة المجني عليه.

- التطور الإلكتروني والتكنولوجي السريع

التطور التكنولوجي أدى إلى ظهور أنواع وأشـكال جديدة من أشـكال التعدي الإلكتروني ممـا جـعـل القـانون الجنائي المتعلـق بالجرائم الإلكترونية عاجز عن معاقبة الجاني لعدم وجود ما بدينه، وانطلاقًا من هذه النقطة يجب ايجاد جهات مختصـة تقـوم بتجديد القانون الجنائي الإلكتروني تبعًا لتطور التكنولوجيا والأخذ بعين الاعتبار الجرائم الإلكترونية المستجدة.

- تفاوت أعمار ودوافع الجناة

انتشـار التكنولوجيا بين أيدي العامة من متخصـصـين وكبار السـن والأطفال والمراهقين أدى إلى وجوب مراعـاة اختلاف الأعمـار عنـد تطبيق العقوبـات المتعلقـة بـالجرائم الإلكترونيـة، أمـا مـا يتعلق بالدوافع فهناك من يرتكب الجرائم الإلكترونية لدواعي التسـلية والبعض الآخر لدواعي إرهابية أو تخريبية فكل هذه تعتبر تحديات وصـعوبات يجب على جهات تطبيق القانون الجنائي المتعلق بالجرائم الإلكترونية مراعاتها ووضعها في عين الاعتبار.

- ضعف البنى التحتية والكوادر التخصصية

جهات إنفاذ القانون في حالة سباق وصراع دائم مع الجريمة الإلكترونية بسبب توفر أدوات الجريمة وسهولة الوصول إليها واستخدامها لإحداث الضرر الفردي أو المجتمعي أو المؤسساتي على الفرد والحكومة، لذلك نجد أن المجرم يمتلك أدوات أكبر وأوسع وأسهل بأحداث الضرر، فيما لا تزال جهات إنفاذ القانون لا زالت في مراحل المعالجة الأولى للجرائم الإلكترونية وهي مرحلة الكشف أو منع الضرر بسبب عدم امتلاك العراق على أي بنية تحتية فنية أو قضائية أو كوادر تخصصية كبوابات إنترنت نموذجية أو تعاون مع شركات الاتصالات أو شركات الإنترنت العالمية لكشف وتتبع الجرائم الإلكترونية أو مختبرات جنائية رقمية أو كوادر تخصصية تتعامل مع الجريمة الإلكترونية بالسياقات الصحيحة.

- ثقافة المواطن الرقمية (الأمن الشخصي الرقمي)

عدة عوامل أدت إلى ضعف أدت إلى ضعف انتشار ثقافة الأمن الإلكتروني الشخصي لدى المواطن، أو عدم اهتمام المواطن بالتحوط الأمني الإلكتروني منها عدم وجود مناهج أو ثقافة حياتية تبدأ من المناهج التعليمية والبرامج التثقيفية المجتمعية التي ترسخ وتبسط شرح خطر الجرائم الإلكترونية وأساليبها وطرق المعالجة والتفادي والخطر، وكل تلك الوسائل أدت إلى انتشار وسهولة المواطنين بمصائد المجرمين بشكل سريع ومؤذي بشكل كبير.

- التعاون مع شركات التواصل الاجتماعي وسياسات الخصوصية المتبعة

من أكبر المشاكل التي تعرقل جهود جهات إنفاذ القانون بالتعامل مع الجرائم المعلوماتية وهي عدم وجود تواصل ثابت ودائم مع شركات التواصل الاجتماعي تضمن الكشف أو إيقاف الضرر أو وجود قنوات مباشرة بالاتصال السريع معهم حيث أن العراق يعاني في الشأن بشكل كبير جدًا مما أتاح الفرصة للمجرمين استغلالها بأسوأ صورة ممكنة من خلال ارتكاب جرائم الإرهاب والابتزاز والتشهير والإساءة وخرق الخصوصية بشكل دائم وسهل وإفلاتهم من العقوبة.

قطر: أفادت بأن هناك العديد من التحديات التي تواجه الجهات المسؤولة عن مكافحة الجرائم الإلكترونية ومن أبرزها الآتي

- **العملات الرقمية (Cryptocurrency):**

هي عبارة عن عملات مشفرة يتم إنشاؤها وتبادلها بشكل افتراضي على شبكة غير مركزية متواجدة خارج نطاق النظم المصرفية المتعارف عليها ويتم تسجيل جميع المعاملات الخاصة بها في قاعدة بيانات لا مركزية تسمى (سلاسل الكتل block chain) وهي عبارة عن ملف أو سجل رقمي عالمي موزع ومفتوح بصورة تسمح بنقل أصول الملكية من طرف لآخر آنيًا دون الحاجة إلى وسيط أو جهة مركزية وسنتعرض تاليًا المخاطر الناتجة من استخدام العملات الرقمية المشفرة.

١-المخاطر المتعلقة بالاستخدام: انخفاض خبرات المستخدمين وثقافتهم تجاه التعامل بالعملات الافتراضية المشفرة وعلى وجه التحديد ما يتعلق بقيمتها نتيجة تقلبات أسعار الصرف غير المتوقعة وتذبذبات الأسعار السريعة جدًا.

٢-مخاطر الائتمان: حيث يتعرض المستخدمون للعملات الافتراضية المشفرة لهذا النوع من المخاطر فيما يتعلق بالأموال المحتفظ بها في الحسابات الافتراضية حيث لا يمكن ضمان أن الطرف المقابل قادر على تلبية كامل احتياجاته المالية والتزاماته عند استحقاقها أو في أي وقت في المستقبل.

٣-مخاطر الاحتيال: وتتمثل من خلال التسبب للمستخدم بخسارة ممتلكاته من العملات الافتراضية المشفرة نتيجة للقرصنة أو الاختراق أو السرقة أو التحايل.

٤-مخاطر غسل الأموال وتمويل الإرهاب وانتشار التسلح: المجرمون قادرون على غسل عائدات الجريمة لأنهم يستطيعون إيداع ونقل العملات الافتراضية المشفرة أو الرقمية بشكل عام دون التعريف بأنفسهم، كما يمكن أن يتم ذلك عالميًا بسرعة وبشكل لا رجعة فيه نسبة لقبولها كوسيلة للدفع عابرة للحدود القضائية.

التوصيات:

١. وضع أدوات وآليات رقابية تعمل على قياس مخاطر وايجابيات وسلبيات التداول وللوقوف على تلك التي يمكن أن تكون مصدر ثقة من عدمه، حيث أن العملات

الافتراضية والاستخدامات المختلفة لتقنية (سلسلة الكتل Block chain) قد أضحت واقعًا لا يمكن إنكاره أو رفض التعامل معه بشكل دائم.

٢. العمل على تطوير منصة متخصصة (تحالف) يشمل بالضرورة (المستوردين، المصنعين، الموردين، المؤسسات المالية المحلية، وجهات إنفاذ القانون) تعمل كمنصة أو شبكة حكومية مشتركة تسمح للجهات الحكومية المختلفة بتنفيذ حالات الاستخدام وقيام كل جهة بإنشاء منصات بشكل منفرد.

٣. تدريب وتطوير المحققين في مجال تقنيات العملات الرقمية المشفرة وسلسة الكتل ولا سيما المعنيين بمكافحة الجرائم الإلكترونية ومكافحة جرائم غسل الأموال وتمويل الإرهاب.

٤. تعزيز التعاون مع المؤسسات البحثية وحثها على إجراء المزيد من الأبحاث في مجال التحقيق في سلسلة الكتل وتتبع العملات الرقمية المشفرة وإنشاء الأدوات والأنظمة التي تسهل عمل مؤسسات إنفاذ القانون.

٥. اقتراح التعديلات التشريعية اللازمة بإضافة النصوص القانونية التي تعالج وتؤطر قواعد للتعامل مع العملات الرقمية والأصول الافتراضية وعمليات الشراء والبيع والتبادل (للعملات الافتراضية والأصول الرقمية).

- فيروسات الفدية (Ransomware):

١. برامج الفدية هي برامج ضاره (برمجيات خبيثة) تستخدم في هجوم إلكتروني لتشفير بيانات الضحية بمفتاح تشفير لا يعرفه سوى المهاجم مما يجعل البيانات غير قابلة للاستخدام حتى يتم دفع فديته (عادة ما تكون عملة مشفرة مثل Bitcoin) من قبل الضحية بعد فيروس الفدية أحد أسرع تهديدات البرامج الضارة انتشارًا اليوم وهو بالفعل وباء ولا تعد برامج الفدية تهديدًا جديدًا ولكنها تتطور وتصبح أكثر تعقيدًا وتنتشر وتصبح أكثر ربحًا وانتشارًا، مع تطورات مثل:

٢. التحول الرقمي المستمرة مع قيام المزيد من المؤسسات برقمنة عملياتها واستخدام الموظفين للبريد الإلكتروني والتطبيقات السحابية والأجهزة المحمولة لإنجاز العمل، وبالتالي يزداد عدد نقاط الدخول المحتملة للمهاجمين بشكل كبير.

٣. استخدام العملات المشفرة: تتيح العملات مثل (البيتكوين) مدفوعات سهلة وغير قابلة للتعقب فعليًا لمجرمي الإنترنت المجهولين مع استمرار المضاربة بالعملات المشفرة لزيادة أسعارها فتزداد احتمالية حدوث هجمات قدية بصورة كبيرة.

٤. برامج الفدية كخدمة (Raas): هي عبارة عن برامج فدية يمكن شراؤها مقابل رسوم رمزية أو نسبة مئوية من دفع الفدية مما يجعل الأمر سهلًا عمليًا لأي شخص لاستخدام برامج الفدية.

التوصيات:

- إجراء التوعية والتدريب الأمني بشكل منتظم للمستخدمين النهائيين ويجب أن يحتوي هذا التدريب على أحدث المعلومات حول التهديدات الأمنية.
- القيام بإجراء تقييمات مستمرة للمخاطر وتحديد نقاط الضعف الأمنية ومعالجة أي تعرض للتهديدات لتقليل المخاطر.
- عمل نسخ احتياطية للأنظمة والبيانات الهامة بشكل منتظم واختبار النسخ الاحتياطية بشكل دوري للتأكد من إمكانية استعمالها وأنها جيدة.
- تشفير النسخ الاحتياطية الخاصة والاحتفاظ بها منفصلة عن الإنترنت أو على شبكة منفصلة مخصصة للنسخ الاحتياطية.
- تصميم ونشر بنية أمان قوية وآمنة بطبيعتها تستخدم التجزئة لتقييد الحركة الجانبية للمهاجم.
- التدريب وتنمية القدرات في مجال الاستجابة للحوادث ومراقبة وقياس الفعالية الشاملة للنظام الأمني على أساس مستمر.

الكويت: أفادت بأن 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.

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

لبنان: أفادت أنه لا يوجد مرئيات بشأن أبرز التحديات الناشئة في مجال جرائم تقنية المعلومات.

التوصية رابعًا/ ب:

نص التوصية " الطلب من الأمانة الفنية للفريق استطلاع آراء الدول الأعضاء حيال أولوياتها من هذه البنود، وتحديد ذات الأولوية منها ليتم مناقشتها في الاجتماع المقبل للفريق".

الإجراءات والنتائج

قام المكتب العربي لمكافحة التطرف والإرهاب بمخاطبة مع مؤسسات العمل العربي المتخصصة بخطاباته رقم ٣٨٨ ورقم ٣٨٩ ورقم ٣٩٠ وتاريخ ٢٠٢٢/٥/٢٥م ولم يتلقى إجابات تتعلق بهذا الشأن.

التوصية رابعًا/ج:

نص التوصية " الطلب من الأمانة الفنية للفريق استطلاع آراء الجهات المعنية في الدول الأعضاء للوصول لتعريف موحد لعددٍ من المصطلحات الهامة مثل: الأمن السيبراني وجريمة تقنية المعلومات، وعرض النتائج على الاجتماع المقبل للفريق".

الإجراءات

قام المكتب العربي لمكافحة التطرف والإرهاب بمخاطبة شعب الاتصال في الدول الأعضاء بخطابه رقم ٤٩٢ وتاريخ ٢٠٢٢/٩/١٥م المتضمن موافاته بآراء الجهات المعنية بشأن وضع تعريف موحد لهذين المصطلحين.

النتائج

تلقى المكتب إجابات الدول الآتية: (مملكة البحرين - الجمهورية الجزائرية الديموقراطية الشعبية – المملكة العربية السعودية - جمهورية العراق – دولة قطر- دولة الكويت – الجمهورية اللبنانية) وكانت الإجابات على النحو الآتي:

البحرين: أفادت أن النهج التشريعي العام هو عدم وضع تعريف خاص والجريمة أو الجرائم المبينة في القانون، وهو ما ذهبت إليه جل القوانين الخاصة وكذلك الاتفاقيات والقوانين الاسترشادية الصادرة عن جامعة الدول العربية، حيث أن هذه الفلسفة قائمة على بيان القواعد العامة للجريمة وأركانها المادية والمعنوية في القانون العام (قانون العقوبات) القسم العام – أما القسم الخاص منه فهو الذي تطرق إلى بيان وتحديد كل من القصد الجنائي – كجزء من الركن المعنوي- والوسيلة التي ترتكب من

خلال الجريمة، ولم يضع تعريفًا لهذه الجرائم، واستكمالًا لهذه الفلسفة ذهب المشروع في مملكة البحرين إلى إفراد تشريعات خاصة لبعض الجرائم المستحدثة مع التأكيد من خلال هذه التشريعات على الإحالة للقواعد العامة فيما يتعلق بأركان الجريمة وعدم وضع تعريف خاص لها كقانون جرائم تقنية المعلومات رقم (٦٠) لسنة ٢٠١٤م الذي لم ينص على تعريف للجريمة الإلكترونية أو جريمة تقنية المعلومات، وإنما جاء تعريفها أو تمييزها من خلال تحديد القصد الجنائي للجريمة أو وسيلة ارتكابها، أو محل الاعتداء المتمثل في نظام تقنية المعلومات، وبناءً عليه ترى مملكة البحرين عدم التوجه إلى وضع تعريف خاص لجريمة تقنية المعلومات لتعارضه مع فلسفة المشروع البحريني في التعاطي مع النصوص الجنائية .

الجزائر: أفادت أنه بخصوص مصطلح الأمن السيبراني فيقترح تعريفه على أنه " هو مجموعة الوسائل التي من شأنها الحد من خط الهجوم على البرمجيات أو أجهزة الحاسوب والشبكات".

كما يمكن تعريفه بأنه " الأمن الذي يعني بتطبيق التقنيات، والعمليات، والضوابط بهدف حماية الأنظمة وشبكة الحواسب والبرامج والأجهزة والبيانات من التعرض للهجمات الإلكترونية".

أما مصطلح الجريمة الإلكترونية فيقترح تعريفها على أنها " كل أشكال السلوك غير المشروع الذي يرتكب أو يسهل ارتكابه باستخدام تكنولوجيات الإعلام والاتصال"

السعودية: أفادت بأن الأمن السيبراني: هو حماية الشبكات وأنظمة تقنية التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمة من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الامن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.

الجريمة المعلوماتية/ الإلكترونية: هي أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية (أو أي أجهزة أخرى مماثلة مثل الحاسوب اللوحي والهواتف النقالة وغيرها) بالمخالفة لأحكام نظام مكافحة الجرائم المعلوماتية.

العراق: أفادت أن استراتيجية الأمن السيبراني العراقي عرفت الأمن السيبراني بأنه الاستعداد الوطني لتوفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء

السـيبراني وحماية البنى التحتية الحيوية للمعلومات وبناء ورعاية مجتمع انترنت موثوق. كما عرفته مسـودة مكافحة الجريمة الإلكترونية في العراق على أنه كل فعل يرتكب باسـتعمال الحاسـب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل التقنية التي يعاقب عليها القانون.

قطر: أفادت بأن القانون رقم ١٤ لسـنة ٢٠١٤م الخاص بمكافحة الجرائم الإلكترونية القطري قد عرف الجريمة الإلكترونية بأنها (أي فعل ينطوي على اسـتخدام وسـيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية ، بطريقة غير مشروعة ، بما يخالف أحكام القانون ، ومصطلح الأمن السـيبراني/ هو مصـطلح شـامل يطلق على أمن المعلومات على شـبكة الإنترنت ، وأمن العمليات الإلكترونيـة ، أمن الشـبكات ، وأمن التطبيقـات ، وهو عبـارة عن خطوات الـدفـاع عن البيـانـات والمعلومات على جميع الأجهزة الإلكترونية المرتبطة بشـبكة الإنترنت من الهجمات الضـارة وعمليات القرصنة وسرقة البيانات والتخريب ، وهو فرع من فروع التكنولوجيا يُعنى بحماية الأنظمة والممتلكات والشبكات والبرامج الرقمية التي تهدف عادةً للوصول إلى المعلومات الحساسة، أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية .

وأشـمل تعريف يمكن الأخذ به للأمن السـيبراني (أن هو مجموع الوسـائل التقنية والتنظيمية والإدارية التي يتم استخدامه لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصـالات والمعلومات التي تحتويها، وذلك بهدف ضـمان توافر واسـتمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المستخدمين من المخاطر في الفضاء السيبراني).

الكويت: أفادت بأن جهاتهم المختصـة ليس لديها مرئيات بهذا الخصـوص، حيث أن مفهوم الأمن السـيبراني والجريمة الإلكترونية مفهوم عام وسـبق أن تم مناقشـته بشـكل متكرر والتعريف المبسط هو (كل فعل مجرم قانونًا يصدر عبر الشبكة الإلكترونية).

لبنان: أفادت أنه لم يتبين وجود تعريف موحد لمصطلحي الأمن السيبراني والجريمة الإلكترونية وفقًا للقوانين والأنظمة والتعليمات المرعية الإجراء في لبنان. مع العلم أنـه بتـاريخ ٢٠١٨/١٠/١٠م صدر القانون رقم /٨١/ المتعلق بالمعاملات الإلكترونية والبيانات ذات الطابع الشخصي، حيث حد في مواده/ ١١٠ – ١١١ – ١١٢ - ١١٣ ـ ١١٤ و١١٥/ الجرائم المتعلقة بالأنظمة والبيانات المعلوماتية

والبطاقات المصـرفية بالإضـافة إلى العقوبات والقواعد الإجرائية المتعلقة بضـبط الأدلة المعلوماتية وحفظها، وفقًا للعناوين الآتية:

- ❖ 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.

ويوجب القرار الصادر عن رئاسة مجلس الوزراء رقم ١٧٢/٢٠١٨ وتاريخ ٢٠١٨/٩/٢٦م وضع خطة لمواجهة مخاطر جرائم المعلوماتية وإعداد استراتيجية وطنية لمأسسة عمل الأمن السيبراني.

وبموجب القرار رقم /٢/ وتاريخ ٢٠١٩/٨/٢٩م الصادر عن رئاسة مجلس الوزراء أعد الفريق الوطني المكلف بموجب القرار رقم ١٧٣/٢٠١٨ المذكور الاستراتيجية الوطنية اللبنانية للأمن السيبراني، التي تهدف إلى أن يكون للبنان فضاء سيبراني أكثر أمنًا واستقرارًا سواء في داخل الوطن أو في التبادلات الدولية.

أما فيما يخص قوى الأمن الداخلي ومكافحتها لهذا النوع من الجرائم فقد تم بموجب مذكرة الخدمة رقم ٦٠٩/٢٢٠٤ وتاريخ ٢٠٠٦/٣/٨م إنشاء مكتب لمكافحة الجرائم المعلوماتية وحماية الملكية الفكرية بغية مواكبة التطورات التكنولوجية والتقنية الحديثة في مجال المعلوماتية ومكافحة الجرائم المستجدة في مجال المعلوماتية.

وبتاريخ ٢٠١٣/٦/٧م صدر عن النيابة العامة التمييزية التعميم رقم ٧٢/ص/٢٠١٣ الذي حدد صلاحيات مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية وفقًا لما يلي:

- جرائم التعدي على الملكية الفكرية المحددة ضمن مصلحة حماية الملكية الفكرية والتي تشمل الماركات والعلامات التجارية وبراءات الاختراع.
- الجرائم المعلوماتية التي تستخدم الأجهزة الذكية كوسيلة مساعدة لارتكاب الجرائم منها:
  - ❖ جرائم التعدي على أنظمة المعلوماتية وشبكاتها ومواقعها وخوادمها.

- ❖ جرائم الإرهاب Terrorism crimes (إرسال المعلومات وتبادل الرسائل صناعة المتفجرات، معلومات عن الأسلحة البيولوجية، رسائل تهديد السفارات).
- ❖ الجرائم المالية الهامة (الحسابات المالية والبطاقات المصرفية Credit Card بأنواعها.
- ❖ جرائم السرقات الدولية (ترويج المسروقات، تبادل المعلومات).
- ❖ جرائم المخدرات Drug Trafficking (ترويج من خلال برامج المحادثة. (Chat rooms)
- ❖ جرائم الميسر وألعاب القمار وكازينو الإنترنت والمراهنات التي تتم عبر الإنترنت (Gambling - Poker - Online Casino).
- ❖ جرائم الآداب (المواقع الإباحية، صور الأطفال Pornographical Sites).
- ❖ جرائم الإعلام الإلكتروني. - الاتصال الدولي عبر الإنترنت.
- ❖ جرائم القرصنة.
- ❖ الجرائم الواقعة على الاقتصاد الرقمي.

وفي ذات السياق أعدت اللجنة المشكلة من قبل المديرية العامة لقوى الأمن الداخلي دليل للتوعية حول الأمن السيبراني والذي يتضمن أفضل الممارسات التي يتوجب على عناصر قوى الأمن الداخلي اعتمادها لتأمين مستوى أعلى من الحماية ورفع مستوى الوعي لديهم.

التوصية خامسًا:

نص التوصية: "تعميم الاستراتيجية العربية لمواجهة جرائم تقنية المعلومات على الجهات ذات العلاقة في الدول الأعضاء من خلال مجالسها الوزارية؛ للاستفادة منها و ابداء المرئيات حيال تطويرها".

الإجراءات والنتائج

قام المكتب العربي لمكافحة التطرف والإرهاب بمخاطبة مع مؤسسات العمل العربي المتخصصة بخطاباته رقم٣٨٨ ورقم ٣٨٩ ورقم ٣٩٠ وتاريخ ٢٠٢٢/٥/٢٥ م ولم يتلقى أي معطيات تتعلق 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 – المملكة العربية السعودية – جمهورية السودان – جمهورية العراق – دولة فلسطين – المملكة المغربية – الجمهورية الإسلامية الموريتانية) تجاربها وممارساتها المتميزة في مكافحة جرائم تقنية المعلومات على الصعيد الوطني لتحقيق الاستفادة المتبادلة وتقييم المخاطر ورصد التهديدات المشتركة.

البند الثالث

التحديات الناشئة في مجال جرائم تقنية المعلومات

في هذا البند قدمت الأمانة الفنية لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات ورقة عمل تناولت فيه إيضاح المؤشر العالمي للتهديدات السيبرانية، ومجموعة من التقنيات والتحديات الناشئة التي تمثلت في الآتي: الويب العميق (المظلم) – إنترنت الأشياء – التهكير والتصيد – الجيل الخامس للاتصالات – البرمجيات الضارة – الحوسبة السحابية – الإرهاب الإلكتروني – التجسس والقرصنة – الحرب الإلكترونية – العملات الرقمية – الذكاء الاصطناعي (الحوسبة الكمومية) – سلاسل الكتل...وغيرها، واستعرض العرض كيفية مواجهة تلك التحديات عبر استراتيجية تكاملية شاملة تأخذ في الحسبان عدد من المحاور من أهمها الآتي:

- **الإطار التشريعي:** سن القوانين ذات الصلة بالأمن السيبراني، واجراءات التقاضي في دعاوي الجرائم الحاسوبية، وحماية الملكية الفكرية والخصوصية، وحماية الحقوق والقيم الثقافية وأعراف المجتمع.
- **بناء وتطوير القدرات:** من خلال تعزيز وإدارة ومراقبة الشبكات والأنظمة بفعالية وكفاءة وتحسين أداء الخدمات والتطبيقات وإنشاء فرق الاستجابة للطوارئ الحاسوبية CERT . وكذلك نشر ثقافة الأمن السيبراني والتوعية بها.
- **تطبيق المعايير التقنية والإجرائية:** من المهم تنفيذ توصيات المنظمات المعيارية مثل "الاتحاد الدولي للاتصالات ITU"؛ و"منظمة المعايير الدولية ISO"؛ و"المعهد الوطني الأمريكي للمعايير والتقنية NIST"؛ و"المعهد البريطاني للمعايير BSI"؛ وغيرها من وثائق التوصيات العامة لإدارة أمن المعلومات ISO 27001؛ والتوصية الخاصة المكملة لها في مجال الأمن السيبراني ISO 27032 .
- **دعم منظومة التعاون الإقليمي والدولي:** ضرورة إتاحة سبل التعاون والتنسيق وتبادل المعلومات بين مختلف الجهات المحلية والإقليمية والدولية في مجال الأمن السيبراني لردع الجريمة السيبرانية كونها جريمة عابرة للحدود. كما تضمنت مجموعة من التوصيات المتعلقة بهذا الشأن، بالإضافة إلى مجموعة من المداخلات والإيضاحات ذات العلاقة.

البند الرابع

تحديد الأولويات بشأن بنود اجتماعات الفريق

استعرض هذا البند الموضوعات الآتية:

١. **القوانين والتشريعات:**

يشتمل هذا الموضوع على كل ماله علاقة بحثّ الدول الأعضاء التي لم تقم بوضع قوانين وتشريعات تُعنى بمواجهة جرائم تقنية المعلومات على استحداث هذه التشريعات أو تحديث تشريعاتهم الوطنية لمواجهة مستجدات جرائم تقنية المعلومات، كما يحث هذا البند الدول الأعضاء على الانضمام والتصديق على الاتفاقية العربية لمواجهة جرائم تقنية المعلومات، وموائمة تشريعاتهم الوطنية لأحكام هذه الاتفاقية.

٢. **تجارب الدول الأعضاء في مواجهة جرائم تقنية المعلومات:**

تُعدّ تجارب الدول الأعضاء وممارساتها الميزة في مواجهة هذه الجرائم من أبرز آليات التعاون العربي من خلال الاستفادة المتبادلة وتقييم المخاطر ورصد التهديدات المشتركة،

٣. **التحديات الناشئة في مجال جرائم تقنية المعلومات:**

تُعدّ جرائم تقنية المعلومات الأكثر توسعًا وانتشارًا، وتختلف أنماطها باختلاف ظروف وآليات ارتكابها، ومع التطورات الناشئة في الفضاء الرقمي وأبرزها استخدام العملات الرقمية، أصبح من الممكن ارتكاب الجريمة الرقمية الكاملة؛ فموقع الجريمة الفضاء الرقمي، وأطراف الجريمة مستخدمين للفضاء الرقمي والهدف الربحي عملة رقمية؛ ما يشكل تحديًا كبيرًا لأجهزة إنفاذ القانون أثناء محاولتهم في العثور على أدلة تسهم في التوصل للجناة أو القاء القبض عليهم.

٤. **التعاون العربي في مجال جرائم تقنية المعلومات:**

تتسم جرائم تقنية المعلومات بأنها جرائم لا تخضع للحدود الوطنية والجغرافية من حيث مرتكبيها أو ضحاياها أو آثارها؛ لذا فإن تعزيز التعاون بين الدول الأعضاء في مجال التحقيق الرقمي سيُسهم في توحيد الجهود لتقفي آثار مرتكبيها والعثور على الأدلة.

٥. **بناء وتطوير قدرات المكافحة لجرائم تقنية المعلومات:**

يتضـمن هذا الموضـوع بناء وتطوير القدرات البشـرية والتكنولوجية والتنظيمية التي من شأنها أن تسهم في الارتقاء بجهود منع ومكافحة جرائم تقنية المعلومات.

٦. **التعاون مع الهيئات والمنظمات الإقليمية والدولية:**

التعاون العربي الدولي يُعدّ أهم الآليات لبناء وتطوير القدرات، فمن خلال المشـاركة العربية الفاعلة في اللقاءات والمنتديات الإقليمية والدولية المعنية بمواجهة جرائم تقنية المعلومات، يمكن معرفة إلى ماذا انتهى الأخرون 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 اقليميين ودوليين يمتلكون الخبرة والرغبة لتحقيق الاستفادة المتبادلة في مواجهة جرائم تقنية المعلومات.

٧. **التعاون مع شركات مزودي الخدمات التقنية الكبرى مثل: شركات وسائل التواصل الاجتماعي والشركات ذات العلاقة.**

فقد ثبت أن كثير من جرائم تقنية المعلومات كالابتزاز الإلكتروني والقرصنة وغيرها تحدث عبر صفحات وسائل التواصل الاجتماعي، لذا يعد من المهم إيجاد آلية للتعاون المباشر معها، وتحديد آلية مُثلى يمكن من خلالها تلقي طلبات الدول الأعضاء بشأن الحسابات المستخدمة لأغراض إجرامية، أو التي تروج لأفكار متطرفة أو تدعم نشاطات مشبوهة أو غيرها من الجرائم التقنية.

البند الخامس

استعراض لوضع إطار عربي موحد لمواجهة القرصنة الإلكترونية وحماية الشبكات

قدمت الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري ورقة عمل حول" إطار عربي موحد لمواجهة القرصنة الإلكترونية وحماية الشبكات لمؤسسات ومنظمات العمل العربي المشترك"، تناولت مدى الحاجة إلى مثل ذلك الإطار باعتبار أن الدول العربية تتبنى في الوقت الراهن سياسة التحول الرقمي في ظل الثورة الصناعية الرابعة؛ ما يتطلب معه إنشاء العديد من مراكز البيانات الضخمة التي يجب حمايتها، كما أن أمن البيانات والمعلومات مسألة غاية في الأهمية كونها تعد موردًا اقتصاديًا وعاملًا أساسيًا من أساسيات التطور في هذا العصر الرقمي. وتم الاستشهاد من خلال الورقة بالعديد من هجمات الأمن السيبراني التي وقعت مؤخرًا وطرق مواجهة القرصنة الإلكترونية وحماية الشبكات.

البند السادس

ما يستجد من أعمال

تلقت الأمانة الفنية للفريق اقتراح المندوبية الدائمة لجمهورية مصر العربية المتضمن إدراج البندين الآتيين:

١. **تطورات بلورة اتفاقية دولية بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية في إطار الأمم المتحدة.**

٢. **إعداد آلية دورية لاستعراض ومراجعة تنفيذ ما جاء في الاتفاقية العربية لمواجهة جرائم تقنية المعلومات.**

التوصيات

في نهاية الاجتماع أوصى الفريق بالآتي:

أولًا: بشأن نتائج تطبيق توصيات الاجتماع الأول للفريق

أ. تقديم الشكر للدول الأعضاء التي أجابت على مراسلات الأمانة الفنية للفريق والأمانة الفنية لمجلس وزراء الاتصالات العرب بشأن تنفيذ توصيات الاجتماع الأول للفريق.

ب. الطلب من الدول الأعضاء الالتزام بمصطلح جرائم تقنية المعلومات الوارد بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات، كوصف على كافة الجرائم التي تتم عبر الفضاء الافتراضي.

ج. 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.

د. تقديم الشكر لجامعة نايف العربية للعلوم الأمنية على موافاتها للأمانة الفنية للفريق بقائمة الدورات وورش التدريب التي يقدمها مركز الجرائم السيبرانية والأدلة الرقمية، والطلب من الأمانة الفنية للفريق تعميمها على الدول الأعضاء للمشاركة فيها.

ثانيًا: بشأن تجارب الدول الأعضاء في مواجهة جرائم تقنية المعلومات:

أ. تقديم الشكر للدول الأعضاء التي قامت بموافاة الأمانة الفنية للفريق بتجاربها في مجال مواجهة جرائم تقنية المعلومات، وتعميم تلك التجارب الواردة على الدول الأعضاء للاستفادة منها.

ب. الطلب من الأمانة الفنية للفريق تخصيص بند دائم على جدول أعمال اجتماعات الفريق لعرض تجارب الدول الأعضاء في مجال مواجهة جرائم تقنية المعلومات؛ على أن يتم في كل اجتماع عرض تجارب ثلاث دول وفقًا للترتيب الهجائي، والطلب من الدول الآتية: (المملكة الأردنية الهاشمية، دولة الإمارات العربية المتحدة، مملكة البحرين) موافاة الأمانة الفنية للفريق بتجاربها في مجال مواجهة جرائم تقنية المعلومات، لعرضها على أعمال الاجتماع الثالث للفريق.

ثالثًا: بشأن التحديات الناشئة في مجال جرائم تقنية المعلومات:

أ. تقديم الشكر للدول الأعضاء التي قامت بموافاة الأمانة الفنية للفريق بالتحديات التي تواجهها في مجال مواجهة جرائم تقنية المعلومات، والطلب إلى الأمانة الفنية للفريق تعميمها على الدول الأعضاء للاستفادة منها.

ب. الطلب من الأمانة الفنية للفريق إعداد ورقة عمل بشأن الابتزاز الإلكتروني ومخاطره، وعرضه على أعمال الاجتماع الثالث للفريق.

ج. الطلب من جامعة نايف العربية للعلوم الأمنية تنظيم ورشة عمل ودليل إرشادي لمصطلحات جرائم تقنية المعلومات، وتقديم ملخصًا عن الدراسة التي أعدتها عن الاحتيال الإلكتروني.

رابعًا: بشأن استطلاع آراء الفريق حول الموضوعات ذات الأولوية لطرحها ضمن الاجتماعات المقبلة:

- **الطلب من الأمانة الفنية اتخاذ اللازم بشأن عرض عدد من البنود على الاجتماع المقبل للفريق حسب الآتي:**

أ. تجارب الدول الأعضاء في مجال مواجهة جرائم تقنية المعلومات.

ب. التحديات الناشئة في مجال مواجهة جرائم تقنية المعلومات.

ج. الابتزاز الإلكتروني.

خامسًا: بشأن وضع إطار عربي موحد لمواجهة القرصنة الإلكترونية وحماية الشبكات:

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

سادسًا: بشأن مقترح جمهورية مصر العربية حول الآتي:

- تطورات بلورة اتفاقية دولية بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية في إطار الأمم المتحدة.
- إعداد آلية دورية لاستعراض ومراجعة تنفيذ ما جاء في الاتفاقية العربية لمواجهة جرائم تقنية المعلومات.

تقديم الشكر لجمهورية مصر العربية على ما قدمته من مقترحات مهمة، والتوصية بالآتي:

أ. 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.

ب. 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 تنفيذ ما جاء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وعرضها على اجتماع مقبل للفريق.

سابعًا: بشأن موعد انعقاد الاجتماع القادم للفريق:

- عقد الاجتماع القادم للفريق في مقر الأمانة العامة لمجلس وزراء الداخلية العرب في تونس خلال الربع الثاني من عام ٢٠٢٣م، والطلب من الأمانة الفنية للفريق التنسيق في ذلك.

وفي ختام الاجتماع تقدم أعضاء الفريق بأسمى آيات الشكر والتقدير لسعادة العقيد مهندس عبد الرحمن الشطي رئيس فريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات على حسن إدارته لجلسات الاجتماع، وتقديم جزيل الشكر للأمانة الفنية للفريق والأمانة الفنية لمجلس وزراء الاتصالات العرب والأمانة الفنية لمجلس وزراء العدل العرب على التنظيم المتميز والتنسيق المتكامل لأعمال هذا الاجتماع.

أسماء السادة المشاركين في الاجتماع الثاني لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات

جمهورية مصر العربية – جامعة الدول العربية

٢١-٢٠٢٢/١١/٢٢م

أولا: الدول الأعضاء

❖❖❖❖❖❖❖❖❖

المملكة الأردنية الهاشمية

الاســـم	الجـهـة
١. السيد/ معتصم توفيق مريان ٢. السيد/ وسام مصاروة ٣. ملازم أول /سجى جسار الزبن ٤. الملازم ثاني/ مخلد فلاح شواق	وزارة الداخلية

دولة الإمارات العربية المتحدة

الاســـم	الجـهـة
١. العقيد. د/إبراهيم حميد المياحي ٢. النقيب/ عبيد محمد المنصوري ٣. السيد/ سالم الظاهري ٤. السيد/ راشد الغفلي	وزارة الداخلية

مملكة البحرين

الاســـم	الجـهـة
الرائد. محمد يوسف بوعلي	وزارة الداخلية

الجمهورية التونسية

الاســـم	الجـهـة
المستشارة/ ضحى الشويخ	وزارة الداخلية

الجمهورية الجزائرية الديمقراطية الشعبية

الاســـم	الجـهـة / الصـفـة
العميد شرطة/ بارة عبدالكريم	وزارة الداخلية - نائب رئيس أمن ولاية البيض

المملكة العربية السعودية

الاســـم	الجـهـة
١. عقيد.د/ ناصر بن هادي القحطاني	وزارة الداخلية
٢. عقيد مهندس/ عبدالرحمن عنيت الله المطيري	الشؤون الفنية
٣. المقدم/ زهران بن رجب الزهراني	مديرية الأمن العام
٤. المقدم/ زهر أحمد الشريف	رئاسة أمن الدولة
٥. المقدم/ ناصر سعد آل طارش	رئاسة أمن الدولة
٦. الأستاذ/ وليد بن خالد العودة	وزارة الداخلية
٧. الأستاذ/ خالد بن محمد المنيعي	هيئة الأمن السيبراني
٨. النقيب/ عبدالإله بن سعد العريفي	وزارة الداخلية
٩. النقيب عبدالإله بن جمعان القحطاني	رئاسة أمن الدولة
١٠. الملازم أول/ عبدالرحمن بن حمد الباتلي	وزارة الداخلية
١١. الملازم أول/ ريان بن جابر غجري	رئاسة أمن الدولة
١٢. الأستاذة. أسماء بنت حاكم الشعلان	هيئة الأمن السيبراني

جمهورية السودان

الاســـم	الجـهـة
مقدم شرطة/ معتز عباس محمد	وزارة الداخلية
فاطمة محمد أحمد محمد الحسن	وزارة الاتصالات والتحول الرقمي

جمهـوريـة العـراق

الاســـم	الجـهـة
حسن الهاشمي	مندوبية جمهورية العراق

سلطنـة عـمـان

الاســـم	الجـهـة
١. المقدم/يحيى بن سالم الصوافي ٢. الرائد/ عبدالله محمد مقيبل	وزارة الداخلية

دولـة فلسطين

الاســـم	الجـهـة
السيدة/ ريان عبدالرزاق	وزارة العدل
السيد/ إبراهيم أحمد ناصر أبو بكر	وزارة الاتصالات وتكنولوجيا المعلومات.

دولـة قطـر

الاســـم	الجـهـة
١. النقيب/ جاسم بن يوسف الكواري	وزارة الداخلية
٢. الملازم أول/ عبد الرحمن البوعينين	وزارة الداخلية

دولة ليبيا

الاســـم	الجـهـة
١. عميد/ محمد حسين سالم سويسي	جهاز المباحث الجنائية
٢. عقيد/ وسام محفوظ الصادق أرجوبة	مديرية أمن طرابلس
٣. الموظف/ إبراهيم أبو بكر محمد عبدالرزاق	مركز المعلومات والتوثيق
٤. الموظف/ محمد لطفي محمود الزياني	شعبة اتصال طرابلس
٥. موظف/ أحمد جمعة سالم غومة	مكتب وزير الداخلية
٦. د. حسين عبدالحميد	المندوبية الدائمة

جمهورية مصر العربية

الاســـم	الجـهـة
١. العميد/ محمد علي البرنس	وزارة الداخلية
٢. المستشار/ محمد رامي حسين	وزارة العدل
٣. العقيد/ وائل ماهر ذكي	هيئة الرقابة الإدارية
٤. د. إسلام محمد رضوان الحديدي	النيابة العامة
٥. المستشار/ عمرو فاروق	المكتب الفني لوحدة غسل الأموال والإرهاب
٦. سماء عبدالناصر عاصي	المكتب الفني لوحدة غسل الأموال والإرهاب
٧. المقدم. حسام حسن	هيئة الرقابة الإدارية
٨. السيد/ ثامر السيد القزاز	مدير التعاون الدولي بالجهاز القومي لنظم الاتصالات
٩. السيد/ أحمد محمد حلمي	نائب رئيس قطاع الأمن السيبراني
١٠. د. محمد السيد	رئيس المكتب القانوني بالأمن السيبراني

المملكة المغربية

الاســـم	الجـهـة
العميد إقليمي/ محمد ساسي	مديرية الأمن الوطني

الجمهورية الإسلامية الموريتانية

الاســـم	الجـهـة
١. ضابط شرطة/ الصوفي على محمياي	وزارة الداخلية
٢. المفوض/ الشيخ إبراهيم ولد حيبلا	مصلحة مكافحة الجريمة السيبرانية بمديرية الاستخبارات
٣. السيد/ محمد الأمين ولد البخاري	مديرية مكافحة الجرائم الاقتصادية والمالية
٤. السيد/ محمد سالم إمام الصف	وزارة الاتصالات

رئيس فريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات

الاســـم	الجـهـة
عقيد. مهندس/ عبدالرحمن بن مبارك الشطي	وزارة الدفاع

ثانيًا: المنظمات العربية:

الأمانة العامة لمجلس وزراء الداخلية العرب

الاســـم	الجـهـة /الصفـة
١. العقيد دكتور/ نايف بن سليمان المطلق	مدير المكتب العربي لمكافحة الإرهاب والتطرف
٢. الدكتور/ محمد ولد بابا سلامة	الأمانة العامة لمجلس وزراء الداخلية العرب
٣. العقيد/ محمد بن عبد الله السحيلي	المكتب العربي لمكافحة الإرهاب والتطرف.
٤. المهندس/ خالد بن بندر الشلهوب	المكتب العربي لمكافحة الإرهاب والتطرف.
٥. الرائد/ فيصل بن حسن القحطاني	المكتب العربي لمكافحة الإرهاب والتطرف.
٦. الرائد/ سيف بن سعد الزيادي	المكتب العربي لمكافحة الإرهاب والتطرف.
٧. السيد/ عبدربه عساف	الأمانة العامة لمجلس وزراء الداخلية العرب
٨. السيد/ علي بن محمد كومان	المكتب العربي لمكافحة الإرهاب والتطرف

إدارة تنمية الاتصالات وتقنية المعلومات

الاســـم	الجهة/ الصفـــــة
حازم حزة	جامعة الدول العربية

قطاع الشؤون القانونية

الاســـم	الجهة/ الصفـــــة
الحسين الأكحل	جامعة الدول العربية

جامعة نايف العربية للعلوم الأمنية

الاســـم	الجـهـة / الصـفـة
د. عبد الرزاق عبد العزيز المرجان	جامعة نايف العربية للعلوم الأمنية

الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

الاســـم	الجهة/ الصفـــــة
١. أ.د. محمد أبو الذهب ٢. د. محمد مصطفى الطويل	الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

الاتحاد الدولي للاتصالات

الاســـم	الصفـــــة
السيد/ عادل محمد درويش	المدير الإقليمي للاتحاد
السيد/ أحمد الراجحي	مستشار أول في الاتحاد