آراء وتعليقات وزارة الداخلية

حيال الدراسة الشاملة لمشكلة الجريمة السيبرانية

أولا. جهود المملكة في هذا المجال.

- المملكة العربية السعودية أعدت نظام مكافحة جرائم المعلوماتية الذي يهدف إلى الحد من وقوع هذا النوع من الجرائم وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها.

- تم إنشاء المركز الوطني للأمن الإلكتروني ووحدة الجرائم الإلكترونية بوزارة الداخلية، ووحدة الجرائم الإلكترونية بهيئة الأمر بالمعروف والنهي عن المنكر بالإضافة إلى هيئة التحقيق والادعاء العام وجميعها معنية بمكافحة هذه الجريمة.

- مع تطور هذا النوع من الجرائم ولمواكبة تطورها تقوم الجهات المعنية بالمملكة بمراجعة الأنظمة وموادها، ومتى ما اقتضت الحاجة لسن تشريعات إضافية أو إجراء تعديلات على ما يتطلب تعديله، يقوم المختصين والخبراء في هذا المجال بإعدادها وفقاً للإجراءات النظامية وبما يتوافق مع القانون الدولي.

- تتخذ المملكة جميع التدابير الوقائية التوعوية والقانونية والتقنية من الجريمة السيبرانية.

ثانياً. التعليق على نتائج الدراسة.

كما هو معلوم في الدراسات المسحية عادة لا يمكن الجزم بدقة نتائجها وهذا يعود لأسباب منهجية تتعلق مثلاً بالعينة، ودقة وجودة أداة البحث (الاستبيان)، وفي السياق المتعلق بهذه الدراسة تحديداً فإنه يمكن طرح مجموعة من التساؤلات والملاحظات التي قد توضح ذلك، وهي:

١ . الدول التي اجابت على الاستبيان (٦٩) دولة من أصل (١٩٢) هي مجموع الدول الأعضاء مما يعني أن (١٢٣) دولة لم تجب على الاستبيان المرسل لها، وهذا ولا شك سبب رئيس ومؤثر في نتائج الدراسة.

٢ . على أسئلة الاستبيان غطت كافة الجوانب المتعلقة بالجرائم السيبرانية؟

٣ . هل الغالبية من الدول التي قامت بالرد على الاستبيان هي من الدول المتقدمة أم من النامية، أو مزيج بينهما؟ فعدم وضوح ذلك ربما يكون له أثر على النتائج.

٤ . ماهي الجهة التي قامت بالرد على الاستبيان في تلك الدول، فهل هي الجهات العدلية؟ أم الجهات التنظيمية (التشريعية) أم الفنية والتقنية؟ أم أنه جميع الجهات؟

٥ . هل الدول التي أجابت الاستبيان لديها وحدات خاصة بالجرائم السيبرانية؟ أم أنها تعالج في إطار القضايا الجنائية التقليدية؟

٦ . يلاحظ من خلال العدد الكبير من القطاع الخاص والأكاديميين والمنظمات الحكومية الذين لم يستجيبوا لطلب الأمم المتحدة بالمساهمة بأي معلومات حيال موضوع الدراسة وهذا مؤشر على انه: إما لا يوجد وعي كاف بخطورة الجرائم السيبرانية إجمالا، او أن هناك خطأ ما في إجراءات التواصل مع هؤلاء.

٧ . بذل في الدراسة جهد كبير يستحق الشكر، والنتائج والتوصيات التي توصلت إليها من المناسب أن تؤخذ بالحسبان، إلا أن الدراسة غير شاملة لموضوع الجريمة السيبرانية ولم تتضمن تعريفاً واضحاً للجريمة السيبرانية وكيفية تشخيصها.

٨ . الدراسة لم تبرز التباين الدولي والإقليمي في محاور الجريمة السيبرانية، ولم توجد حلول شاملة لمكافحتها، وإيجاد تعاون وتنسيق سلس وحقيق بين الدول والأقاليم.

٩ . لم تتناول الدراسة أفضل الممارسات لمكافحة الجريمة السيبرانية، كما أنها مبوبة بطريقة غير علمية مما يصعب فهم فقراتها وربطها ببعضها البعض.

ثالثاً. المرئيات حيال الدراسة.

نقترح ما يلي:

- تحديث الدراسة بحيث يتم الممازجة بين الرصد المعرفي الذي تضمنته وتجارب الدول الأعضاء العملية في التعامل مع هذا النوع من الجرائم، بحيث تقدم نماذج وأمثلة حقيقية لبعض

الجرائم السيبرانية التي تم التعامل معها سواء على المستوى القانوني أو الفني او على مستوى التعاون الدولي، حتى تصبح هذه الدراسة كدليل استرشادي يساعد الدول الأعضاء خصوصاً النامية في التعامل مع هذه الجريمة.

- مناسبة إضافة التوصيات التالية إلى الخيارات التي انتهت إليها الدراسة:

١. صياغة إطار تنظيمي للتعاون غير الرسمي بين الدول الأعضاء والشركات التقنية الكبرى كفيسبوك وتويتر للمكافحة والوقاية من الجرائم السيبرانية، بحيث يشمل هذا الإطار الدعم الفني، والمعلوماتي، والتوعوي، والتدريبي، ويمكن تبني مقترح وضع مدونة سلوك بين الأمم المتحدة والشركات الكبرى لتهتم بجوانب محددة.

٢. دراسة فكرة تأسيس مختبرات تحليل جنائي رقمي لتدريب العاملين في مجال الجرائم السيبرانية، وذلك لمساعدة الدول خصوصاً النامية في التعامل مع هذا النوع من الجرائم. فرض معايير عالية على المنظمات الحكومية وشبة الحكومية للحفاظ على أمنها التقني وسلامة بياناتها وتكليف جهة مختصة ذات كوادر مؤهلة (المركز الوطني للأمن الألكتروني) لمتابعة ذلك.

٣. وضع متطلبات على مقدمي الخدمات للحفاظ على معايير سلامة الشبكة والخدمات مثل (ISO).

٤. تحديث أنظمة حماية المستهلك لتتضمن متطلبات الأمن السيبراني.

٥. تطوير عمليات وإجراءات تقنية بالتعاون مع المؤسسات التنظيمية المختصة.

٦. دعم الأفكار والبرامج الخاصة بحماية أمن المعلومات ومكافحة الإرهاب السيبراني.

٧. المساعدة على وضع سياسة الحماية الوطنية من الإرهاب السيبراني.

٨. نشر الوعي على المستوى الوطني حول مخاطر الفضاء السيبراني.

٩. المساعدة على توحيد وتحديث القوانين والأنظمة وكافة الأطر القانونية والتشريعية اللازمة لحماية الفضاء السيبراني في المملكة.

١٠. التعاون الدولي لمنع ومكافحة الإرهاب السيبراني ودعم تبادل المعلومات حول الأخطار المحتملة.

١١. توفير أدوات مراقبة للأهل لحماية أبنائهم على الأنترنت وعقد ورش تدريبية للأهل في المدارس والجامعات.

١٢. القيام بالمشاركة والمساهمة في عدد من المؤتمرات المحلية، والإقليمية والدولية حول خطر الإرهاب السيبراني وكيفية مواجهته.

١٣. إطلاق حملة إعلامية مكثفة عبر مواقع التواصل الاجتماعي والإعلام المرئي والمسموع.

١٤. نشر التوعية والترويج لحقوق المستهلك نحو مقدمي خدمات الاتصالات عبر الإعلان المرئي والمسموع.

١٥. استحداث تطبيقات للأجهزة الذكية للإبلاغ عن حالات الإرهاب السيبراني.

١٦. إنشاء مركز الاستجابة لطوارئ الحاسب الآلي (CERT) ومن مهامه:

- تأمين استجابة لطوارئ أمن تكنلوجيا المعلومات والاتصالات لتشكيل دعماً للهيئات الحكومية والبنى التحتية الوطنية الحساسة من الجمهور العام في البلد عبر مبادرات معترف بها قانونياً ومرخص لها ومنسقة مركزيا على المستوى الوطني.

- تحفيز الأمن، والحماية عبر نشر المعلومات المهمة مثل الإنذارات المبكرة والتنبيهات والاستشارات الأمنية ودعم أفضل الممارسات الأمنية.

- دعم والحفاظ على هذه المبادرات مما يتطلب اعتماد تكنولوجيا وتقنيات متطورة، تأسيس مناهج بحث لتحليل التهديدات والتخفيف منها.

- تلقي بلاغات هجمات الاختراقات الأمنية والإرهابية السيبراني ومعالجتها أو تمريرها للجهات المعنية لمعالجتها.

- فرض وتحديث سياسات أمن المعلومات على المؤسسات والمنظمات الحكومية والخاصة والمنشآت الحيوية في البلد.

١٧. إنشاء مركز مختص لإدارة مشتركة بين القطاعين العام والخاص لمكافحة الإرهاب السيبراني.

١٨. وضع استراتيجية وطنية لأمن الفضاء الإلكتروني ومتابعتها وتطويرها من قبل السلطات العليا في المملكة.

١٩. وضع أسس تعاون وطني بين الحكومة (القطاع العام) والخاص.

٢٠. خلق القدرات الوطنية لإدارة الحوادث ومحاربة الإرهاب السيبراني.

٢١. التنسيق والتعاون مع الجهات الإقليمية والدولية في مكافحة الإرهاب السيبراني.

رابعاً. ملاحظات عامة.

١) يلاحظ أن معظم البلدان لا تجرم أدوات إساءة استعمال الحواسيب، ونرى أن يتم الاتفاق بين الدول على تجريم الأدوات طالما أنها تستخدم في تنفيذ الجريمة.

٢) أهمية تثقيف مستخدمي الانترنت في الوقت الراهن باتخاذ احتياطات أمنية على اجهزتهم الحاسوبية.

٣) إجراء مزيد من الدراسات والأبحاث في الجرائم السيبرانية.

٤) وجود حاجة فيما يخص "الازدياد الطردي لنسبة الجرائم الالكترونية المتوقعة مع زيادة الموصولية العالية لمستخدمي الانترنت، ويدعم ذلك التوجهات العالمية إلى انترنت الأشياء والحوسبة السحابية" إلى جانب دراسة الجانب القانوني للجريمة السيبرانية من قبل

الجهات القانونية ذات العلاقة في المملكة والتأكيد من تماشي هذه القوانين مع التحديات المعاصرة.

٥) ضرورة توفر المعلومات فيما يخص "التعاون الدولي" حول الهجمات الالكترونية بشكل سريع وفعال مع الجهات المختصة، فالجريمة السيبرانية هي جريمة عابرة للقارات وأحداثها متسارعة جداً مما يتطلب التنسيق والمتابعة باستخدام وسائل فعالة.

٦) مراجعة الدراسات الحالية فيما يخص "نظام الخصوصية" وإيجاد نظام وطني للخصوصية على مستوى المملكة.

٧) بناء كوادر وطنية مؤهلة فيما يخص "نقص الكوادر المتخصصة في الأدلة الجنائية الرقمية والمحققين في الجريمة السيبرانية.

٨) عدم الاعتماد على "منهج توزيع الاستبيان" في جمع وتحليل البيانات، وإنما يوصي على نقاط الضعف لدى الجهات، بالإضافة إلى مرئياتهم.