الإجراءات التى تتخذها الدول فى مواجهة مخاطر الاستخدام غير المشروع للفضاء الإلكتروني

الباحث/ خالد محمود محمد مهران

تحت إشراف

أ.د. عصام محمد أحمد زناتي

أستاذ القانون الدولي العام- ونائب رئيس جامعة أسيوط سابقا

أ.د. ناصر محمد عثمان

أستاذ القانون الدولي الخاص- كلية الحقوق بجامعة أسيوط

(ISSN: 2537 - 0758)

الإجراءات التى تتخذها الدول فى مواجهة مخاطر الاستخدام غير المشروع للفضاء الإلكتروني

الباحث/ خالد محمود محمد مهران

ملخص البحث:

لمواكبة العصر الحديث وما حدث فيه من ثورة معلوماتية فى جميع المجالات اتجهت غالبية الدول إلى نظام التحول الرقمى وتطبيقه على مرافقها العامة والإستراتيجية وكذلك العسكرية .

مما قد يتسبب فى أضرار جسيمة للدول حال عدم إتخاذها الإجراءات التى تؤمن فضاءها الإلكتروني وتحول دون إختراق أنظمتها الإلكترونية وتضمن إحكام السيطرة على أمانها السيبراني .

وتأتى هذه الإجراءات على شكلين، الأول تقني مثل (جدران الحماية – أنظمة كشف التسلل – تحسين أمن نظام أسماء النطاقات – التركيز على سلامة الشبكة – تخفيف آثار الهجمات الخاصة بالحرمان من الخدمة – تعزيز البنى التحتية الحساسة – تحصين الأنظمة الحكومية والعسكرية – التشفير للشبكات على نحو يمنع اختراقها).

والثانى وضع استراتيجية وطنية للأمان السيبراني عن طريق (اجراء مسح وطني شامل للتشريعات ذات الصلة – تحديث تشريعات الجرائم السيبرانية وايجاد حلول لبعض إشكالياتها– تنسيق التشريعات بين الدول العربية والاسترشاد بإرشادات الإسكوا التشريعات السيبرانية – الاسترشاد باتفاقية بودابست – انشاء وحدات متخصصة لتطبيق القانون– تعزيز الإجراءات الاستباقية للأمان السيبراني– اعتماد وسائل ناجعة للتوعية والتدريب حول الأمان السيبراني– توعية مختلف الفئات في المجتمع– تشجيع النساء والرجال على التبليغ عن الجرائم السيبرانية– دورات للقضاة والمحققين والشرطة– إدخال موضوع الجرائم السيبرانية في المناهج التعليمية).

ومن هنا يجب إقرار مبدأ التعاون لمجابهة الجرائم السيبرانية سواء التعاون بين القطاعين العام والخاص والمجتمع المدني سواء التعاون بين الدول بعضهم ببعض سواء التعاون بين الدولة ومزودى الخدمة ووجوب الانضمام إلى الإتفاقيات المعنية بالفضاء الإلكتروني.

Abstract

to keep pace with the modern era and what happened in it of the information revolution in all fields, the majority of countries have turned to the system of digital transformation and its application to

their public, strategic as well as military facilities. This may cause serious harm to countries if they do not take measures that secure their electronic space, prevent the penetration of their electronic systems and ensure that the surveillance tightens their cybersecurity. These measures come in two forms, the first is technical such as (firewalls - intrusion detection systems - improving the security of the DNS - focusing on network safety - mitigating the effects of denial-of-service attacks - strengthening sensitive infrastructure - fortifying government and military systems - encryption of networks in a way that prevents their penetration) and the second is the development of a national strategy for cybersecurity through (conducting a comprehensive national survey of relevant legislation - updating cybercrime legislation and finding solutions to some of its problems- coordination of legislation between Arab countries and guidance ESCWA Guidelines Cyber Legislation - Guided by the Budapest Convention- Establishment of Specialized Law Enforcement Units- Strengthening Proactive Measures for Cyber Security– Adopting.

المقدمة:

أدت علاقة الفضاء السيبراني بعمل المنشآت الحيوية داخل الدول سواء أكانت مدنية أو عسكرية لقابلية تعرضها لهجوم سواء عن طريق استهدافها كوسيط وحامل للخدمات أو بشلل عمل أنظمتها المعلوماتية ، ويكون من شأنه التأثير على القيام بوظيفتها ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب.

وتكمن خطورة حروب الإنترنت والشبكات في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني لا سيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية إضافة إلى المؤسسات والشركات العامة والخاصة. ولا شك أنّ ازدياد الهجمات الالكترونية والتي نشهد جزءًا بسيطا منها اليوم يرتبط أيضًا بازدياد هذا الاعتماد على شبكات الكمبيوتر والإنترنت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطوّر الهجمات الالكترونية اليوم لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل علما بان أبعاد مفهوم الحرب الإلكترونية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين حتى العامة(١).

ومن المتوقع أن تصبح الحرب الإلكترونية نموذجًا تسعى إليه العديد من الجهات نظرًا للخصائص العديدة التي تنطوي عليها.

(ISSN: 2537 - 0758)

أهمية البحث:

تأتى أهمية البحث من خلال تعاظم إستخدام الفضاء الإلكتروني سواء عن طريق شبكة الإنترنت أو الشبكات الأخرى التى تسبح في الفضاء الإلكتروني وإتجاه أغلبية الدول إلى التحول الرقمى.

ومن هنا فإن جميع الإجراءات الحكومية سواء في التعامل مع الأفراد أو الهيئات أو الشركات الخاصة أو أسلوب التحكم في مرافقها أو الإحتفاظ بملفاتها أو إدارتها لأذرعتها تأتى من خلال شبكة الإنترنت أو شبكات مغلقة تتحكم فيها الدولة ومؤمنة.

إلا إن هذا التحول الرقمى كما أنه يأتى بإيجابيات عدة من سهولة ويسر وعدالة في التعاملات مما يؤثر إيجابيا في عدم ضياع الوقت وكذا إتخاذ قرارات سليمة بناء على معلومات لولا وجود هذه الشبكات ما كنا تحصلنا عليها بهذه الغزارة والجودة.

إلا انه يمكن أن يأتى بأمور سلبية عن طريق المفسدين الذين يتخذون من مواطن الضعف في هذه الشبكات منفذا لهم للدخول الى هذه الشبكات والعبث بها وإرتكاب جرائم قد تصل لحد القتل في بعض الأحيان والحصول على معلومات أو أموال مما يضر بالفرد والدولة وتهتز ثقة الأفراد في أسلوب حكوماتهم في التعامل مع هذه الشبكات مما قد يزعزع استقرار الدول وحكوماتها ومن هنا وجب على جميع الدول اتخاذ كثير من الإجراءات لحماية فضاءها الإلكتروني ومن ثم حماية مصالحها ومصالح مواطنيها .

منهج البحث :

سوف يتبع الباحث المنهج التحليلي والذى يعتمد على تجميع التشريعات القانونية في هذا الصدد وآراء الفقهاء حول موضوع البحث ومن استخلاص الأفكار والتجارب الواقعية من خلال المؤلفات والأبحاث والمقالات المتخصصة.

المبحث الأول

السُبُل والإمكانيات المتاحة والإجراءات التى يتم اتخاذها لمواجهة الإستخدام غير المشروع للفضاء الإلكتروني

تمهيد وتقسيم :

أمام الزيادة المتسارعة في وتيرة لجوء الدول لاعتماد الفضاء الالكتروني كسبيل لإلحاق الضرر بالأعداء والخصوم، والتزايد في قيمة الأضرار الناجمة عن هذه الهجمات التي تصيب المعلومات والشبكات ضمن الفضاء الالكتروني، وما يقترن ويرتبط بها من أنظمة ومنشآت ومصالح لا تقتصر على الجانب العسكري، وانما تشمل ما هو مدني أيضا ، من منشآت وبنى تحتية حيوية وحساسة.

إزاء كل ذلك تزداد حاجة الدول لبلورة وتملك منظومة دفاعية تسهم في صد الهجمات ومنعها، أو على الأقل التخفيف من ضررها في حال وقوعها، وذلك بالإضافة إلى تطوير الأساليب والأدوات القتالية الهجومية ضمن هذا الفضاء.

ولا تقتصر الأنظمة الدفاعية ضمن الفضاء الالكتروني على جانب واحد، بل هي متعددة. ويمكن تلخيص أهمها في جانبين، هما التقني البرامجي، والجانب التشريعي القانوني. في الجانب الأول هناك تقدم مستمر مصاحب للتطور المستمر في البرمجيات والتقنيات المعتمدة في عمليات الهجوم والاختراق، ومقارب له بالوتيرة والسرعة، في حين أن تطور المنظومة التشريعية الدفاعية ظلت أبطأ من وتيرة تطور الهجمات الإلكترونية.

ومن هنا سوف نتناول هذا المبحث في مطلبين :

الأول: منظومات التقنية للحد من الهجمات الإلكترونية

الثانى: الإجراءات التى تتخذها الدول في مواجهة مخاطر الاستخدام غير المشروع للفضاء الإلكتروني والتي تدخل في نطاق الجانب التقني

المطلب الأول

منظومات التقنية للحد من الهجمات الإلكترونية

تتعدد أساليب المواجهة والتصدي التقنية للهجمات الإلكترونية، وتتلخص بالأساس في اعتماد ثلاث نوعيات من التقنيات والأنظمة الأكثر انتشارا وثقة وكفاءة **ويأتي في مقدمتها جدران الحماية** أو ما يُعرف ب" الجدران النارية .(Firewall) "ومن ثم هناك البرامج المضادة للبرمجيات الخبيثة من فيروسات وغيرها(Antivirus program) وأنظمة كشف التسلل (IDS) وبالإضافة إلى هذه التقنيات هناك إجراءات احتياطية تقنية بسيطة تلجأ لها الدول ولكنها تكون ذات ومفعول ومردود أمني عالي، كإجراءات فصل وتقسيم الشبكات، والتشديد على بيانات الدخول، واجراء عمل النسخ الاحتياطي (. Backup).

وتعتبر جدران الحماية من أهم وسائل الدفاع التقنية لصد الهجمات الالكترونية من محاولات إختراق وبث للبرمجيات الضا رة، وهي تعرف أيضا ب" الجدار الناري) " (Firewallوتقوم جدران الحماية على مبدأ الفصل بين المناطق الموثوق بها والمناطق غير الموثوق بها في شبكات الحاسوب. بحيث يقوم برنامج جدار الحماية بمرا قبة العمليات التي تمر بالشبكة ويرفض أو يسمح فقط بمرور البرامج طبقا لقواعد معينة (ستولينج،622:2011) أصل الفكرة والتسمية جاءت من الحائط الذي يبنى بالطوب الأحمر العازل بشكل يوقف انتقال النيران المحتملة إلى داخل البيوت، ويطلق على هذا الحائط الطوبي اسم " الحائط الناري".

(ISSN: 2537 - 0758)

وبالمثل يقوم برنامج جدار الحماية بمنع إختراق الشبكة، ويمنع البرامج الضارة من الدخول إلى الجهاز أو الشبكة، وذلك عبر آلية ترشيح البيانات المُستقبَلة، وهو يسمح في الوقت نفسه للاتصالات غير الضارة بالوصول بحرية (ستولينج،623:2011)[٢] ظهرت هذه التقنية في أواخر عقد الثمانينات من القرن الماضي، وذلك استجابة لعدد من الاختراقات لشبكة الإنترنت المستجدة حينذاك .وقد ظهر منها عدة أجيال :

الجيل الأول يعرف بمرشحات العبوة (Packet Filters) ، ويقوم مبدأ عمله على فلترة (ترشيح) العبو Packet ، والتي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الإنترنت .فإذا كانت العبوة تطابق مجموعة شروط الجدار، فإنه يسمح بمرور العبوة، أو يرفضها ويتخلص منها ويقوم بإرسال إشارة" خطأ (Error) " للمصدر، في حال لم تكن مطابقة . (حسين ٢٠١١:١٩٦).

ولكن هذا النظام من مرشحات العبوات لم يكن يعير اهتماما إلى كون العبوة جزءا من تيار من المعلومات والبيانات المتدفقة، إذ لا يقوم بتخزين سلسلة من البيانات والمعلومات، وانما يقوم بترشيح العبوات بناءا على المعلومات المختزنة في العبوة نفسها، ويتعامل مع كلٍ منها على حدى، ما استدعى تطوير **الجيل الثاني** من جُدُرْ الحماية والمعروف ب" فلتر محدد الحالة(Stateful Filter) " والذي يقوم بمراقبة حقول مُعَينة في المعلومات المستقبلة، ويقارنها بالحقول المناظرة لها في سلسلة كاملة من المعلومات الواردة ضمن السياق نفسه، ومن ثم يجري رفض المعلومات التي تنتمي لسياق معين إذا لم تلتزم بقواعده، لأن ذلك يكون دليلا على أنها زرعت في السياق وليست جزءا منه، مما يثير الشكوك بأنها برامج خبيثة (حسين،٢٠١١:١٩٧).

ثم ظهر أخيرا **الجيل الثالث** والمعروف باسم طبقات التطبيقات (Application Layer Firewall) والفائدة الرئيسية منه أنه يمكن أن يفهم ويتعامل مع التطبيقات والأنظمة المُعَقدة، ومن ثم بإمكانه اكتشاف إذا ما كان هنالك نظام غير مرغوب فيه يتم تسريبه، أو إذا كان هنالك نظام يتم استخدامه بطريقة مؤذية(حسين، ٢٠١١:١٩٧)[٣] .

<u>أما التقنية الثانية</u> من ضمن التقنيات الأكثر اعتمادا وانتشا را في مجال التصدي للهجمات الإلكترونية فهي البرامج المعروفة باسم مضادات الفيروسات (Antivirus) ومُضاد الفيروسات هو برنامج يتم استخدامه لاكتشاف البرمجيات الضا رة ومنعها من إلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية، وذلك عن طريق إ زالتها أو إجراء التعديلات عليها واصلاحها، وبحيث يمكن لهذا البرنامج أن يتصدى لبرامج التجسس، وبرامج أحصنة طروادة، والتي هي عبارة عن شيفرات صغيرة تقوم ببعض المهام الخفية، وغالبا ما تتركز على إضعاف قوى الدفاع وإختراق جهاز الحاسوب وسرقة بياناته .

وكذلك تتصدى مضادات الفيروسات ل" الديدان الحاسوبية"، كما توصف، وهي برامج صغيرة، تصنع للقيام بأعمال تدميرية، أو لغرض سرقة البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت (الخالد،2018 :99) تم تطوير برامج مضادات الفيروسات أواخر الثمانينات من القرن الماضي، وقد ازداد تطورها بفعل زيادة حجم المخاطر التي تهدد الحواسيب .ولتحديد الفيروسات والبرامج الخبيثة، تقارن برامج مضادات الفيروسات محتويات الملف إلى قاموس فحص الفيروس . ولأن الفيروسات يمكنها تضمين نفسها في الملفات، عندها يتم البحث في الملف بأكمله لضبطها والكشف عنها، وهناك أسلوب آخر يعتمده مضاد الفيروسات، يتم عبر الكشف على نشاط البرمجيات الضارة، بحيث يقوم برصد نظام للاشتباه في تصرفات البرنامج .فإذا ما تم الكشف عن سلوك مريب، يقوم مضاد الفيروسات بعمل مزيد من التحقيق والفحص في البرنامج .ويمكن استخدام هذا الأسلوب لتحديد الفيروسات غير المعروفة أو نُسخ أخرى من الفيروسات الموجودة (طيطي،2010:191).

ومن ثم هناك أسلوب" مضاهاة ملف (File Emulation) وفيه يتم تنفيذ البرنامج في بيئة افتراضية، وتسجيل الإجراءات التي ينفذها، ومن ثم، واعتمادا على الإجراءات التي تم تسجيلها، يستطيع برنامج مضاد الفيروسات تحديد ما إذا كان البرنامج ضار أم لا ومن ثم تتخذ الإجراءات المناسبة (طيطي،2010:192).

أما التقنية الثالثة المستخدمة ضمن أنظمة التصدي لهجمات الفضاء الإلكتروني فهي أنظمة كشف التسلل (Intrusion Detection Systems)(وتعرف اختصا را ب (IDS) ونظام التصدي هو برنامج مصمم للكشف عن محاولات الوصول إلى نظام الحاسب الآلي غير مرغوب بها أو محاولة تعطيل هذا النظام بشكل عام والتلاعب به، وبحيث أن هذه المحاولات يمكن أن تتخذ عدة أشكال وسبل، منها كسر الحماية، أو استخدام البرامج الضارة(الفيروسات، حصان طروادة، والديدان (الخالد : 2018:63)[٤].

* **تتألف أنظمة كشف التسلل من عدة مكونات، هي :**

جهاز استشعار ينبه على وقوع الأحداث، ولوحة تحكم لمراقبة الأحداث والتنبيهات والتحكم بأجهزة الاستشعار، ومحرك يقوم بتسجيل إدخالات الأحداث المتلقاة من خلال أجهزة الاستشعار في قاعدة بيانات وتكون أنظمة كشف التسلل مصنفه بالاعتماد على نوع وموقع أجهزة الاستشعار والمنهجيات المستخدمة على المحرك. (الخالد : 2018:64).

(ISSN: 2537 - 0758)

وعدا عن استخدام البرمجيات والأنظمة التقنية لمواجهة الهجمات الإلكترونية هناك وسائل تقنية أخرى يمكن تفعيلها أيضا لتفادي وتقليل آثار هذه الهجمات، وذلك دون الحاجة إلى استخدام برمجيات وأنظمة متطورة ومعقدة، ومن ذلك اللجوء إلى عمل فصل جزئي احتياطي بين الشبكات فلا تكون كلها كتلة واحدة، وبحيث يتم تقسيم الشبكات إلى شبكات فرعية (Subnetting) لكل منها قواعد محددة للدخول، وذلك بهدف الحد من الاتصال بينها وبين أي شيء خارج هذه الشبكات. ومثال على ذلك إذا وقعت هجمة تستهدف إحدى شبكات المعلومات أو البنى التحتية فإن الأضرار تكون مقتصرة على تلك الشبكة دون امتدادها إلى شبكات أخرى (محمود، 81:2016).

إلى جانب ما تقدم، هناك إجراءات احترازية سهلة التطبيق، مثل التشديد وعدم السماح للدخول إلى الشبكة إلا بعد تقديم وابراز معلومات شخصية من قبل كافة المستخدمين على الشبكات الحيوية، مثل بوابات الحكومة الالكترونية، وذلك بتأكيد هويتهم عند الدخول إليها، باستخدام عُنصرَين على الأقل من عناصر تحديد الهوية، وبحيث تكون المعلومات بمثابة البصمة التي لا يمكن استنساخها أو الاشتراك بها، ومن الأمثلة على ذلك استخدام الأرقام الوطنية، وأرقام الهاتف، وكذلك التأكد من الهوية عبر إرسال رسائل التفعيل إلى أرقام الهواتف(المبيضين،106:202).

هناك إجراء آخر قد يكون بسيطا، ولكن يمكن أن يساهم في تلافي أضرار الهجمات الإلكترونية بدرجة كبيرة هذا الإجراء يتمثل في ضرورة المواظبة على عمل نسخ احتياطي (Backup) وبشكل دوري منتظم، لكافة الملفات والمعلومات والبيانات المهمة على الشبكة[٥] .

وفي قواعد البيانات، بما في ذلك البيانات الخاصة بالمؤسسة والعملاء .وبحيث في حال التعرض لأي تخريب أو هجوم إلكتروني يستهدف قرصنة المعلومات وتخريبيها ومسحها، فإنه يتم الحد من تأثيره ففي حالة توفر النسخ الاحتياطية فإنه سرعان ما يتم استعادة ورفع جميع البيانات من جديد وبكامل تفاصيلها وصحتها ودقتها، وكلما كانت عملية النسخ دورية ضمن مدد زمنية أقصر كلما كان حجم البيانات المفقودة أقل ويتم إجراء النسخ الاحتياطي من خلال شراء أقراص صلبة خارجية ذات مساحات كبيرة حتى تستوعب نسخ احتياطية من جميع الملفات، أو تحميل كل هذه المعلومات او البيانات على خوادم ذات قدرة استيعابية كبيرة .

مما تقد م نخلص إلى أنه هناك العديد من الوسائل التقنية المتاحة لمجابهة الهجمات في الفضاء الإلكتروني والتصدي لها، وبحيث إن الالتزام بتطبيق وتفعيل أكبر قدر منها يمكن إن يكون معينا إلى حد بعيد في التصدي لهذه الهجمات والحد من تأثيرها في حال وقوعها، وهو ما تزداد الحاجة إليه لدى مختلف الدول وبخاصة في ظل عدم التو صل إلى اجماع دولي واسع يفضي إلى بلورة معاهدات ومنظومة قانونية وقائية تحول وتحد من وقوع هذه الهجمات.

ونجد أن وسائل التصدي التقنية لا تقتصر فقط على البرمجيات المعقدة والمتطورة، وانما هناك إجراءات تقنية بسيطة نسبيا يمكن من خلال الالتزام بها تفادي جانب كبير من مخاطر الهجمات، بما في ذلك اللجوء إلى تقسيم الشبكات، والتشديد على إجراءات الدخول إلى الشبكات، والمواظبة على عملية النسخ الاحتياطي لكافة البيانات والمعلومات الهامة.

مع استمرار ربط العمليات الحيوية بالإنترنت واشتداد شراسة الأنشطة الخبيثة على الشبكات، فإن سلامة الفضاء الإلكتروني للدول ستشكل عنصرا جوهريا في قرارات الشركات حول أماكن إنشاء أعمالها، وبالتالي فإن الأمن الذي كان يعد مجرد تكلفة يجب تخفيضها سيصبح صاحب الكلمة في السوق.

فالبلدان التي لم تحصن شبكاتها الوطنية من شأنها أن تجتذب المجرمين والمتسللين الإلكترونيين وتحرضهم على ممارسة اعتداءاتهم، ولا يقتصر الأمر على ذلك بل ينال النمو الاقتصادي للبلاد فيعوقه. ولهذه الأسباب يجب على دول مجلس التعاون اتخاذ خطوات لتحويل منطقة دول المجلس إلى "منطقة فضاء إلكتروني آمن وسليم". وكانت الاستراتيجية الوطنية لأمن الفضاء الإلكتروني في الولايات المتحدة لعام ٢٠٠٣ قد اقترحت أمريكا الشمالية لهذا الدور ولكن هذه الفكرة لم تدخل حيز التنفيذ إطلاقا[٦].

المطلب الثانى

الإجـراءات التى تتخذها الدول في مواجهة مخاطر الاستخدام غير المشروع للفضاء الإلكتروني والتى تدخل فى نطاق الجانب التقنى

وتعد الإجراءات التالية التي تتخذها الدول تجاه مخاطر الاستخدام غير المشروع للفضاء الإلكتروني والتي تدخل في نطاق الجانب التقني من أهم العناصر المكونة لمنطقة إلكترونية آمنة:

(ISSN: 2537 - 0758)

١ – تحسين أمن نظام أسماء النطاقات (DNS)
٢ – حماية الفضاء الإلكتروني
٣ – التركيز على سلامة الشبكة الوطنية.
٤ – توطيد التعاون لمعالجة الجرائم الإلكترونية.
٥ – إعداد خطط تعاونية لتخفيف آثار هجمات الحرمان من الخدمة.
٦ – تعزيز البنية التحتية الحساسة
٧ – حماية الأنظمة الحكومية والعسكرية وتحصينها.

أولا :تحسين أمن نظام أسماء النطاقات (DNS)

إن نظام أسماء النطاقات هو عبارة عن دليل هاتف للإنترنت، فهو يتيح لمشغل الحاسوب طباعة عنوان سهل التذكر مثل www.google.com للدخول إلى هذا الموقع بدلا من أن يضطر إلى تذكر ٧٢.١٤.٢٠٤.٩٩.

ومثل بقية البروتوكولات الأساسية التي تجعل الإنترنت تعمل، لم يتم تصميم نظام أسماء النطاقات ليكون آمنا إذ يمكن بسهولة تقليد النظام فيتمكن المهاجم الذي يشن هجومه من السيطرة على النطاق والقيام بالاحتيال أو أي نشاط خبيث آخر. وقد تم استغلال نقطة الضعف هذه في الهجوم الإيراني على موقع بايدو الصيني الذي. حيث انه وفي أيار/مايو ٢٠١٠ صرح مسؤول كبير في الحرس الثوري الإيراني بأن «الجيش الإلكتروني التابع للحرس الثوري قد استطاع اليوم أن يصبح ثاني أقوى جيش إلكتروني في العالم ».وعلى رغم عدم وضوح أسس هذا الادعاء، تعتقد شركة الأبحاث الأمريكية "ديفنس تك" أن الشعبة الإلكترونية لديها حوالي ٢٤٠٠ موظف بالإضافة إلى ١٢٠٠ من قراصنة الإنترنت (الهاكرز) في القطاع الخاص ويعتقد أن ميزانيتها السنوية تفوق٧٥ مليون دولار(٧).

وحتى الآن اقتصرت أنشطة إيران في حرب الفضاء الإلكتروني على هجمات ضد مواقع إلكترونية، كتخريب أو حجب مواقع لشركات إخبارية تغطي حركات المعارضة الإيرانية. وفي ١٩ كانون الأول/ديسمبر ٢٠٠٩ تعرض موقع "تويتر" للمدوناتات لهجمات تسببت بإغلاقه في عدة مناطق من العالم. وقد أعيد توجيه المستخدمين الذين حاولوا دخول هذا الموقع إلى رسالة تقول: «تعتقد الولايات المتحدة الأمريكية أنها تتحكم بشبكة الإنترنت وتسيطر عليها، لكنها مخطئة، فنحن بقوتنا نتحكم بالشبكة، لذا لا تحاولوا استفزاز الشعب الإيراني... من منا على قائمة الحظر الآن،

إيران أم الولايات المتحدة الأمريكية؟ إننا نضعهم على قائمة الحظر، فاحذروا». وبعد شهر من هذه الحادثة تعرض محرك البحث الصيني "بايدو" إلى هجوم مشابه، حيث تم تشويه الصفحة الرئيسية للموقع بعبارة مفادها: «تم تأسيس جيش إيران الإلكتروني للاعتراض على تدخلات المواقع الأجنبية والصهيونية في الشؤون الداخلية لدولتنا ونشر الأخبار الكاذبة والمضللة».

ومن غير الواضح سبب تعرض موقع صيني لهجوم من هذا النوع، إلا أن الرد جاء سريعا من قراصنة الشبكة في الصين حيث وجه الاتحاد الصيني للقرصنة الإلكترونية ، وهو جماعة استهدفت مرارا مواقع أمريكية في السابق، ضربة انتقامية ضد سلسلة من المواقع الإلكترونية الإيرانية التي اختيرت بشكل عشوائي في هجمات مشابهة، وبثت الجماعة رسائل على هذه المواقع ردا على تلك المنشورة على موقع "بايدو"[٨].

وتقوم منظمات الجريمة بشراء مواقع إلكترونية في جزء من عمليات الاحتيال باستخدام الشبكة بالإضافة إلى هجمات التصيد أو الأعمال الخيرية المزيفة أو عروض الخدمات الكاذبة، كما يستخدم النظام للسيطرة على شبكات "البوت" والتحكم بها. ويحتاج البرنامج الخبيث المستخدم للسيطرة على جهاز حاسوب يشكل جزءا من شبكة البوت إلى استقبال التعليمات من المسيطر أو "راعي شبكات البوت" الذي يقوم بتجميعها. وللقيام بذلك يحتوي البرنامج الخبيث على قائمة طويلة من المواقع الإلكترونية التي لم يتم تسجيلها بعد باسم أحد، وفي وقت محدد مسبقا تقوم كافة أجهزة الحاسوب التي تشكل جزءا من شبكة البوت بمحاولة الاتصال بكل موقع إلكتروني، ويحاول راعي البوت نت مسبقا تسجيل النطاقات من أعلى القائمة إلى أسفلها إلى أن يتمكن من شراء أحدها وإعداد الموقع لاستقبال الرسائل من شبكات البوت والرد عليها. ولكي يعطي راعي البوت نت هذا التكتيك فاعلية، عليه أن يستخدم حصرا نطاقات الدولة أو النطاقات الأخرى العالية المستوى التي لا تطلب إثبات الهوية لشراء موقع.

وبالإضافة إلى مشكلات الجرائم والتجسس والحرب الإلكترونية التي أصبحت ممكنة بسبب ضعف أمن نظام أسماء النطاقات، فإن النظام نفسه يحتوي ثغرات أمنية تجعله عرضة للهجوم. وفي عام ٢٠٠٨ أنشأ دان كامينسكي الخبير في أبحاث الأمن أداة برمجية بإمكانها تقديم معلومات مزيفة إلى نظام أسماء النطاقات والسيطرة على المواقع والبريد الإلكتروني وحركة شبكة الإنترنت. وكان بالإمكان توظيف هذا الهجوم لجني الأرباح أو تعطيل النظام بتقديم معلومات خاطئة على مستويات عالية[٩].

وتمكن الباحثون في نظام أسماء النطاقات من التوصل إلى حل مؤقت، غير أن الثغرة الأساسية لاتزال موجودة ويمكن استغلالها من خلال هجمات أكثر تعقيدا. كما

(ISSN: 2537 - 0758)

يمكن تعطيل نظام أسماء النطاقات عن طريق شن هجوم شرس للحرمان من الخدمة كالذي استخدم في اختبارعام ٢٠٠٧ من قبل أفراد مجهولين.

وفي تلك الحادثة تم إغراق ستة من أصل ثلاثة عشر نطاقا عالية الأهمية بدفق من آلاف الطلبات في الثانية الواحدة. و تعطل نطاقان لعدم قدرتهما على تحمل الزحام، ولكن المهاجمين أمروا جحافلهم الإلكترونية بالانسحاب بعد ثماني ساعات، ولو استمر هجومهم لكان أطاح بقية الأنظمة.

ولمعالجة مشكلة أمن نظام أسماء النطاقات يجب العمل في مسارين منفصلين: مسارقانوني وتنظيمي من شأنه تصعيب مهمة المجرمين في تسجيل عناوين إلكترونية لأغراض غير مشروعة؛ ويوازيه مسار تقني لتطبيق أمن نظام أسماء النطاقات (DNSSEC). ويتطلب المسار الأول تحرك القائمين على تسجيل النطاقات الوطنية نحو تطبيق متطلبات تسجيل أشد صرامة للأفراد أو الشركات التي تريد شراء اسم نطاق(١٠).

وحددت شركة "مكافي" McAfee المختصة بأمن الإنترنت نماذج مبادرات لتأمين تسجيل النطاقات الوطنية في أربعة بلدان هي: هونج كونج (hk).وتشيلي (cl) واليابان (jp).وايرلندا (ie). حيث طبق مسؤولو التسجيل في كل من هذه البلدان متطلبات أشد صرامة لتسجيل المواقع الإلكترونية، كما عملوا عن كثب مع المراكز الوطنية للاستجابة لطوارئ الحاسب الآلي (CERTs) والشرطة والسلطات التنظيمية من أجل تحديد المواقع الخبيثة وإيقافها ومقاضاة القائمين على تشغيلها.

وطبقت تشيلي نظاما يتطلب تأكيدا من بنك العميل للقيام بعملية شراء باستخدام بطاقة الائتمان، وباعتماد هذا الإجراء أصبح من الصعب استخدام أرقام بطاقات الائتمان المسروقة لشراء مواقع إلكترونية بأسماء وهمية، وتتحرك تشيلي بسرعة لإيقاف المواقع الخبيثة حال اكتشافها. كما أن ايرلندا ركزت جهودها على "إمكانية التتبع" حيث عملت على التحقق من هوية المسجلين والتأكد من أن لهم صلة شرعية في ايرلندا، وأن لهم حقوقًا شرعية في اسم النطاق الذي يسجلون فيه. ويجدر بباقي الدول ولا سيما العربية النظر في تبني متطلبات مشابهة.

إن الانتقال إلى فئة أقل المخاطر لن يكون مهمة صعبة. وقد حددت مكافي عدد من النطاقات الخطرة . ومن الممكن التخلص من هذه المواقع ووضع قواعد ومعايير تدقيق جديدة لضبط المواقع الخطرة التي لميتم التعرف عليها، ومنع تأسيس أي مواقع جديدة من هذا النوع، وذلك قبل إصدار ترتيب بذاته.

ومن الناحية التقنية، على جميع الدول التحرك باتجاه تبني استخدام امتداد النطاقات الأمنية التي من شأنها أن تتحقق من كل جزئية في حركة نظام أسماء النطاقات، بدءا من المستخدمين الأفراد الذين يطلبون مواقع إلكترونية حتى "الجذر" (قائمة مجال المستوى الأعلى لمخدمات نظام أسماء النطاق (DNS servers) والعودة مرة أخرى إلى الأسفل. ولكي يعمل هذا النظام بشكل فعال يجب تحميل برنامج DNSSEC على كافة أجهزة الحاسوب، سواء كانت مخدمات أو أجهزة حاسوب محمولة أو هواتف ذكية. وقامت هيئة الإنترنت للأسماء والأرقام المخصصة "الآيكان" (ICANN) التي تتولى إدارة ملف منطقة الجذر "بإدراج" الجذر في ١٥ تموز/يوليو ٢٠١٠) أي أنها أنشأت توقيعا رقميا للدلالة على المصداقية).

ثانيا : التركيز على سلامة الشبكة:

يستغل مجرمو الإنترنت والعابثون الآخرون ذوو النيات الخبيثة ضعف أنظمة الوقاية وتلوث بيئة الشبكة لشن هجماتهم. ونظرا للطبيعة العالمية للإنترنت فغالبا ما يكون مصدر أنظمة الهجوم مختلفًا عن مكان وجود الفرد أو الأفراد الذين يتحكمون في الهجوم. إن أمن الشبكة الوطنية لا يرتبط بالضرورة بوجود مشكلات جريمة إلكترونية، إلا أن قياس مستوى الجريمة تمتع الشبكة الوطنية ببيئة نظيفة تحول دون وقوع الإلكترونية يبين درجة أنظمة الاستضافة ضحية للجرائم الإلكترونية أو التواطؤ من دون قصد مع منفذي هذه الجرائم.

ومن ذلك الهجمات الالكترونية كالأبواب الخلفية (backdoors) التي تسمح بالتسلل إلى الأنظمة بطرائق غير قانونية، فقد جاءت المملكة المتحدة في المرتبة الأولى تلتها إسبانيا في المرتبة الثانية ثم ألمانيا في المرتبة الثالثة. وصنفت مكافي كلا من المملكة العربية السعودية ودولة الإمارات العربية المتحدة ضمن فئة "المخاطر المنخفضة". إن مستويات استخدام الإنترنت في الشرق الأوسط أعلى بشكل طفيف من مثيلاتها في بقية العالم بنسبة ٣.٢٨ %مقابل ٥.٢٥ ،%إلا أن مستويات استخدام الحزمة العريضة (broadband) أقل من ١٠ %في الشرق الأوسط بعامة، وبنسبة ٧ %في دول مجلس التعاون لدول الخليج العربية. وتتوقع مؤسسة تيليجيوغرافي، وهي مؤسسة رائدة في أبحاث الاتصالات، أن يتضاعف معدل استخدام الحزمة العريضة في الشرق الأوسط خلال السنوات القادمة. ومما لا شك فيه أن هذا التوسع سيرافقه منافع اقتصادية، إلا أنه سيؤدي أيضا إلى ارتفاع مستويات الإصابة بالفيروسات وزيادة عدد الأنظمة الموبوءة. وربما يكون عدد مستخدمي الهواتف الجوالة الكبير سببا لهذا

(ISSN: 2537 - 0758)

القلق. ويتوقع الباحثون في مجال الأمن أن تشكل الهواتف الجوالة الهدف الرئيسي للمتربصين الإلكترونيين في ظل تسارع وتيرة ارتفاع معدلات مستخدمي الهواتف الذكية.

أما فيما يتعلق بالسلامة العامة، فإن تحسين أمن الشبكة يتطلب أولا جمع البيانات. لذا على مزودي خدمة الإنترنت العمل عن كثب مع مراكز الاستجابة لطوارئ الحاسب الآلي (CERTs) والشركات الخاصة لمراقبة أمن الفضاء الإلكتروني للتمكن من القيام برصد فوري لأمن الشبكة وإعداد تقارير فصلية وسنوية بناء على هذه البيانات ويمكن استخدام هذه التقارير لرسم الخط الأساسي للسنة الجارية، ووضع أهداف لتخفيف المشكلات في كل بلد عن كل فئة، إلا أن عملية الضبط هذه لا تقتصر على إعداد تقارير منمقة.

وقد يتيح الوعي الظرفي على الشبكات إمكانية تحديد حلول مباشرة لأي برمجيات ضارة أو شبكات "البوت" أو رسائل تطفلية أو أي أنشطة خبيثة أخرى . بإمكان التقنية المتوافرة اليوم تحديد المشكلات على الشبكات الوطنية لحلها على الفور. وتقوم حاليا شركة "كومكاست" Comcast ، وهي شركة لتزويد خدمة الإنترنت في الولايات المتحدة، بإعداد مشروع تجريبي ينبه أن الحركة من أجهزتهم تبدو كجزء من شبكة "بوت" المشتركين في حال تبين أو أن هناك أي مؤشر ينذر بأنه قد تم تحميل برنامج خبيث على أجهزتهم. كما تقدم كومكاست نصائح مجانية وأدوات لإزالة البرمجيات الخبيثة مع إرسال الإشعار، وفي نهاية المطاف قد تبدأ بحظر الأنظمة من الدخول على الشبكة. ويجب إلزام مزودي خدمة الإنترنت بإعداد برامج مشابهة، وقد يكون من الحكمة التحقق من أن الأجهزة تقوم بتشغيل برامج مشروعة، وأنه يتم تحديث هذه البرامج، وأن الأنظمة تتمتع بتقنية فعالة لمضادات الفيروسات ومضادات البرامج الخبيثة. بالإمكان أيضا إيقاف الأنشطة الخبيثة على الشبكة قبل وصولها إلى أجهزة تستضيفها بما يضاعف المشكلة، وباستطاعة تقنيات الفحص الدقيق للحَزم رصد الحركة على الشبكة لاستبعاد البرامج الخبيثة، وتستطيع التقنيات الآن العمل بانتظام ومن دون تأخير، أي أن باستطاعتها العمل بنفس سرعة الإشارات التي تحمل حركة الإنترنت ولاُتسبب أي تأخير في حركة المعلومات على الشبكة. وبالإضافة إلى رصد البرمجيات الخبيثة المعروفة وإيقافها، يمكن استخدام عملية التفتيش الدقيق للحزم لرصد أي حركة غريبة تشير إلى أي هجوم جديد من نوعه لم يتم رصده سابقا. إن الأخذ بهذه الخطوات مجتمعة من شأنه أن يحسن بشكل كبير أمن الشبكة بين الدول. وعلى رغم أن هذه الإجراءات لن تكون عصية على الاختراق، فإنها ستتمكن مجتمعة من إيقاف ٩٩ %من الهجمات التي تعتمد على جوانب الضعف المعروفة[١١].

ثالثا : الاستثمار في تخفيف آثار هجمات الحرمان من الخدمة:

ليس من حل قاطع وحيد لمنع هجمات الحرمان من الخدمة، إلا أنه من الضروري اتباع استراتيجية متعددة المحاور يكون أساسها التركيز على إيقاف الهجمات على الشبكة قبل وصولها إلى الأنظمة المستهدفة.

إن الميزة المؤذية التي تتمتع بها هجمات الحرمان من الخدمة تستمد قوتها من إمكانية استخدام عدة أنظمة لاستهداف نظام واحد. ويمكن انتهاج تكتيك على شبكة الإنترنت من أجل إيقاف هذه الهجمات للقضاء على هذه الميزة، وذلك بتبديدها عند عدة نقاط. فمع أن أكبر شبكة "بوت" تستطيع إغراق الأنظمة بتسونامي من البيانات يقارب ١٢٠ جيجابايت في الثانية، وهو يفوق إلى حد كبير قدرة استيعاب أي شبكة خاصة، إلا أن هذا الكم من البيانات لا يشكل قطرة في محيطات الشبكة الوطنية المترامية الأطراف. لذا تجب إزاحة مسؤولية إيقاف هجمات الحرمان من الخدمة عن كاهل المستهدفين لتصبح من اختصاص مشغلي شبكة الإنترنت. وفي الولايات المتحدة الأمريكية يقوم عديد من مزودي خدمة الإنترنت بتقديم إجراء تخفيف لهجمات الحرمان من الخدمة في جزء من "خدمات الأمن التي تديرها"، وهي خدمة استثنائيةُ تقدم للمشتركين لقاء رسم إضافي. ولتخفيف هجمات الحرمان من الخدمة، تقوم هذه الخدمات بمراقبة الحركة ورصد التهديدات وتصفية الحزم التي يتضح أنها جزء من هجوم والسماح بمرور الحركة التي لا تشكل تهديدا، وإخضاع الحزم التي لا يمكن تصنيفها ضمن أي من الفئتين لمستويات تحليل أشد صرامة قبل تمرير البيانات النظيفة إلى وجهتها. وعلى الدول تشجيع مزودي خدمة الإنترنت فيها على تقديم خدمات مشابهة لكافة مشتركيها شركات أو أفرادً. وتتبع الصعوبة الحقيقية في مواجهة تنفيذ هذه الاستراتيجية من التنسيق المطلوب بين مزودي خدمة الإنترنت من جهة، ومالكي الأنظمة المستهدفة من جهة أخرى ويجب أن يتم التنسيق بشكل فوري تقريبا، ويتطلب قيام مزودي خدمة الإنترنت بالتعامل جديا مع التهديد، وهو أمر لم يقتنع مزودو خدمة الإنترنت في الولايات المتحدة بالقيام به حتى الآن. وفي خطوة أولى، على مزودي الخدمة والمستخدمين التعاون فيما بينهم لترسيخ إدراك الموقف (awareness situational). وعادة ما تقوم هجمات الحرمان من الخدمة بإغراق الشبكات المستهدفة بنوع واحد من الزحام، كطلب صفحة إنترنت بشكل متكرر على سبيل المثال. لذا فإن الخطوة الأولى لرصد هجوم حرمان من الخدمة يجب أن تبدأ بالتعرف على الموجات الغريبة لنوع مرورمعين، وحال رصد الحزم الغريبة يجب أن تعمل الأنظمة

(ISSN: 2537 - 0758)

المستهدفة بشكل فوري وبالتنسيق مع مزودي خدمة الإنترنت على محاصرة الهجمات واستبعادها والسماح للحزم السليمة بالعبور.

ويمكن إعداد وضبط مكونات الشبكة لتطلب إقرارا بخصوص الحزم، وبالتالي لا تستطيع الأنظمة المرسلة حال حدوث هجوم حرمان من الخدمة التي تشن الهجوم بدء الإرسال من دون إتمام عملية إنشاء ارتباط متبادل. كما أنه باستطاعة مزودي خدمة الإنترنت اتخاذ خطوات لكبح الحزم التي تحمل عناوين بروتوكول إنترنت زائفة، كالعناوين الخاصة أو عناوين بروتوكول الإنترنت التي لميتم تخصيصها بعد.

رابعا :تعزيز البنى التحتية الحساسة ضد الهجمات الإلكترونية:

ثلاثة أنواع من البنى التحتية الحساسة التي تجب حمايتها مهما كلف الأمر، وهي: مرافق استخراج النفط والغاز، ومولدات الكهرباء، ومحطات تحلية المياه. ولحماية البنية التحتية الحساسة من الهجمات الإلكترونية، على الدول أن تركز جهودها حول ثلاثة محاور، وهي: ١ (الحد من إمكانية الاتصال) ٢ (وجوب تشفير وترميز كافة أنظمة التحكم) ٣ (استبقاء وصيانة أجهزة التحكم اليدوية). ويجب اختبار وتدقيق مستوى الأمن في هذه النواحي بشكل دائم للتأكد من الالتزام بكافة التعليمات. ويتضمن الحد من إمكانية الاتصال؛ فصل مكونات هذه الأنظمة عن شبكة الإنترنت العامة، إذ يمكن استخدام الاتصال بالشبكة للولوج إلى أنظمة حساسة، وبالتالي التحكم والتلاعب بهذه الأنظمة. وقد يدعي معظم مرافق الخدمات عدم اتصال أنظمتها بشبكة الإنترنت العامة، ومع ذلك تحدث حالات تطفل باستخدام الإنترنت. وقد أظهرت مجلة وول ستريت جورنال الأمريكية في تقرير صدر عنها عام ٢٠٠٩ أن وكالات استخبارات أجنبية تمكنت من الدخول إلى شبكة الكهرباء الأمريكية وزرعت فيها "قنابل منطقية" (bombs logic)يمكن ضبطها على توقيت محدد لتدمير النظام. وفي عام ٢٠٠٩ أشار برنامج التقارير الإخبارية ٦٠ دقيقة "60 Minutes "إلى قيام بعض المخربين بتعطيل شبكة الكهرباء في أحد بلدان أمريكا الجنوبية. وفي أغلب الحالات يقوم مصنعو المعدات بالاتصال بشبكة الإنترنت للقيام بفحوصات عن بعد، وتستخدم بعض المرافق في الولايات المتحدة وأوروبا الإنترنت للتحكم بأنظمتها في نوع من تخفيض التكاليف. وفي حالات أخرى تم الدخول عبر هواتف الصوت عبر الإنترنت (VoIP) التي تم تحميلها في غرف التحكم. وللتحقق من حالات الاتصال بالإنترنت يجب إجراء تدقيق دوري للأنظمة وتأسيس "الفرق الحمراء " لإجراء اختبارات بمحاولة اختراق الأنظمة.

ولا تعد الأنظمة غير المتصلة بالإنترنت منيعة ضد الهجمات الإلكترونية، فعلى رغم أن قطع الاتصال بالإنترنت سيمنع المهاجمين من شن هجماتهم عن بعد، فإن ذلك

لن يمنعهم من شن الهجمات باستخدام وسائل أخرى. فبالإمكان دس البرمجيات الخبيثة في الوسائط المحمولة، مثل سواقات الناقل التسلسلي العام(USB) والأقراص المدمجة التي يتم استخدامها لتحديث الأنظمة. ويمكن اختراق الشبكة والتحكم فيها عبر الارتباط بالشبكات، والاستيلاء أو إعادة البث على الموجات الصغرى وموجات البث الأخرى، أو إنشاء نقاط ربط خفية مع الشبكة العامة. وهذا لا يعني أن إزالة الارتباط بالإنترنت أمر غير مجد، فإذا تعذر على المهاجمين دخول الأنظمة عبر الإنترنت سيضطرون إلى الاقتراب فعليا من الأنظمة، ما سيزيد من احتمالات ضبطهم وتعريض أنفسهم للخطر. إلا أن الحد من الاتصال بالإنترنت لا يغطي سوى جانب واحد من جوانب الأمن، لذا يجب تشفير كافة الحزم على الشبكة، وعدم السماح بالدخول إلى الشبكة إلا بموجب مصادقة متعددة العوامل.

وأخيرا، وتحسبا لفشل هذه الإجراءات الأمنية يجب أن يتمتع القائمون على تشغيل هذه البنى التحتية الحساسة بالقدرة على العودة إلى استخدام أجهزة التحكم اليدوية التي لا تتطلب الاعتماد على التقنيات والنظم الرقمية والبرامج التكنولوجية، ولاتزال إمكانية التغيير إلى الدعم اليدوي متاحة في معظم الصناعات، إلا أن الأنظمة الحديثة لا يمكن تشغيلها في حال تعطلت أجهزة التحكم الإلكترونية الخاصة بها أو تم استغلالها من قبل العابثين الذين يضمرون السوء.

خامسا : تحصين الأنظمة الحكومية والعسكرية:

كما هي الحال بالنسبة للبنى التحتية الحساسة، على الأنظمة الحكومية والعسكرية الحد من الاتصال بالإنترنت وفصل الأنظمة الحساسة بشكل تام عن الأنظمة المتصلة بالإنترنت. ويجب عند بوابات الإنترنت معاينة كل حركة بحثا عن أنماط الهجوم المعروفة(١٢). كما يجب استخدام برامج رصد الحزم الغريبة لضبط أي أنماط مشبوهة، ويجب رصد كافة المعلومات التي تخرج من الشبكات الحكومية وتحليلها بغرض ضبط تسريب المعلومات غير المصرح بها.

كما يجب استخدام الأنظمة داخل محيط الشبكات لمراقبة وضبط وتحليل تدفق المعلومات بحثا عن أنماط مشبوهة في سلوكيات الشبكة. وتنبغي حماية كافة أجهزة الحاسوب التي تعمل على هذه الشبكات باعتبارها أصولا خاصة، وذلك باستخدام برامج منع الاختراق ومكافحة الفيروسات والبرمجيات الخبيثة. وعلى كافة مستخدمي هذه الأنظمة تطبيق المصادقة بعاملين على الأقل، كما يجب تقسيم شبكات الإنترنت إلى شبكات فرعية بحيث يمنح إذن الدخول حسب الحاجة فقط(١٣).

(ISSN: 2537 - 0758)

التشفير كأحد أساليب تأمين الشبكات على نحو يمنع اختراقها:

ولعل في محاولة الشركات والمؤسسات والحكومات تأمين شبكاتها المعلوماتية ضد الاختراق بمثابة وسيلة تحد – إن لم تمنع مطلقاً – من عملية الاختراق لهذه الشبكات، ومن ثم فهي تؤدي بطريقة غير مباشرة إلى منع اختراق هذه الشبكات. ومن طرق تحصين الشبكات الداخلية كذلك من الاختراق عملية التشفير، والتشفير يعني تحويل البيانات المكتوبة إلى أرقام أو رموز لا يمكن حلها إلا بالنسبة لمن يمتلك شفرة حل هذه الرموز والأرقام، وتستخدم عملية التشفير في تداول النقود والبيانات عبر الشبكة في التجارة الإلكترونية، وفي تداول غيرها من البيانات التي تتعلق بالأمن القومي.

وهناك برامج تشفير متقدمة لحماية البيانات المخزنة على شبكات الحاسب الآلي للعبور، والتوقيع السيبراني، وهناك شهادات التصديق على هذا التوقيع السيبراني، وجميعها برامج معلوماتية تساعد في حماية نظام وبيانات الحكومة السيبرانية(١٤).

المبحث الثانى

إطار عمل للأمان السيبراني ومكافحة الجرائم السيبرانية

تمهيد وتقسيم :

ليس بإمكان الحلول التقنية وحدها أن تعالج بشكل كاف جميع مشكلات الجريمة الإلكترونية والتهديدات الأخرى التي تحيق بالفضاء الإلكتروني، فالأنظمة والتحقيقات والإجراءات القانونية ضرورية أيضا. ونظرا إلى قدرة المهاجمين في بلد ما على استهداف الأنظمة في بلد آخر، فلا بد من وضع آليات تتيح إمكانية التحقيق والمقاضاة دوليا.

كما يجب على البلدان وضع آليات للتعامل مع طلبات إغلاق الشبكات في وجه الأنظمة التي يتم رصدها، من حيث هي أطراف مشاركة في هجمات الحرمان من الخدمة أو أي نمط آخر من الهجمات. وعلى الدول أن تدرس التوقيع لمعاهدة المجلس الأوربي حول جرائم الشبكات الإلكترونية والمصادقة عليها.

ويتضح لنا أن هناك تقدم مستمر مصاحب للتطور المستمر في البرمجيات والتقنيات المعتمدة في عمليات الهجوم والاختراق، ومقارب له بالوتيرة والسرعة، في حين أن تطور المنظومة التشريعية الدفاعية ظلت أبطأ من وتيرة تطور الهجمات الإلكترونية. وسوف نقوم بتناول هذا المبحث في مطلبين كالآتي :

المطلب الأول : وضع استراتيجية وطنية للأمان السيبراني ومكافحة الجرائم السيبرانية
المطلب الثاني: إقرار مبدأ التعاون لمجابهة الجرائم السيبرانية

المطلب الأول

وضع استراتيجية وطنية للأمان السيبراني ومكافحة الجرائم السيبرانية

تتمثل الخطوة الأولى في هذا الإطار بوضع استراتيجية متكاملة للأمان السيبراتي ولمكافحة الجرائم السيبرانية، وتتضمن هذه الاستراتيجية نواحي مختلفة، منها التشريعي والتنفيذي والتنظيمي والتثقيفي. تجدر الإشارة إلى أنه إذا كان قد سبق لبعض الدول أن وضعت استراتيجية مماثلة، فينبغي عليها تحديثها وإعادة النظر فيها دوريا في ظل المتغيرات وسرعة التطور التقني وما اختبرته في ظل الاستراتيجية القديمة. وعلى كل دولة وضع خطط عمل مفصلة لتطبيق استراتيجيتها عن طريق تحديد الأهداف الجزئية والمشاريع والإجراءات والتحديثات المنوي تنفيذها والهوامش الزمنية لها والترابط بينها ويمكن، كفكرة أولية، اعتماد الدول النامية، نفس استراتيجيات مكافحة الجرائم السيبرانية المقررة في الدول المتقدمة، لما في ذلك من توفير الوقت والمال؛ غير أن اعتماد هذه المقاربة يثير عدة إشكاليات، فبالرغم من أوجه الشبه في المخاطر السيبرانية بين الدول النامية والمتقدمة، فإن أفضل الحلول لأي بلد ترتبط بموارده وإمكاناته وبالنظام القانوني المطبق فيه وبعقلية المجتمع ومدى تعاون القطاع الخاص(١٥).

وتجدر الإشارة أنه في محاولة لتحديد أنجع الوسائل للأمن السيبراني، أظهرت نتائج استطلاع للرأي أجري في عام ٢٠١١ على ١٨٦١ مختصا في تكنولوجيا المعلومات، أن ٥٨ في المائة منهم يرون أن تطبيق ممارسات وسياسات أمن فعالة له أكبر وقع على الأمان السيبراني، في حين أفاد ١٥ في المائة فقط أنه يمكن زيادة مستوى الأمان السيبراني بالدرجة الأولى بواسطة التكنولوجيا، وأقر ٧ في المائة فقط أن القوانين هي الحل الأول(١٦).

وبناء على التجارب الدولية، يوصي بان تتضمن استراتيجية الأمان السيبراني ومكافحة الجريمة السيبرانية في كل دولة البنود التالية كحد أدني:

١- وضع التشريعات السيبرانية الضرورية وتحديثها.

٢- وضع منهجية للاستجابة للحوادث السيبرانية، وبوجه خاص إنشاء مراكز للاستجابة السريعة لطوارئ الحاسوب، ووضع أسس التواصل والتعاون بين هذه المراكز في المنطقة العربية(١٧).

٣- دعم صناعة البرمجيات والتجهيزات والحلول التقنية الخاصة بالحماية من المخاطر السيبرانية.

(ISSN: 2537 - 0758)

٤- تعزيز الشراكة بين القطاع العام والخاص، وبخاصة فيما يتعلق بحملات التوعية، وتطوير الحلول التقنية، وحفظ معلومات حركة البيانات وبيانات التعريف عن المستخدمين، والتمويل.

٥ – تشجيع اعتماد الهوية الإلكترونية للمستخدمين على الشبكة، وبوجه خاص عند الدخول إلى الأنظمة ذات الطبيعة الحساسة، كالأنظمة المالية؛٦ – تطوير نظام التبليغ السريع عن الجرائم السيبرانية بحيث يعتمد على السرية ويضمن حقوق المرأة والطفل.

٧ – اعتماد المؤشرات التي تراعي النوع الاجتماعي وتسمح بتقصي مستوى الجريمة السيبرانية، وتحديثها دوريا.

٨ – التوعية الحثيثة والمستمرة حول الأمان السيبراني والجرائم السيبرانية للمؤسسات والأفراد.

٩- تعزيز التدريب والتأهيل في مجال الأمن السيبراني، بغية زيادة عدد المتخصصين في هذا المجال.

١٠ – إقرار مبدأ التعاون في محاربة الجرائم السيبرانية ضمن إطار الامم المتحدة، بغية زيادة تبادل المعلومات بين الأجهزة الرسمية.

ويجب أيضا على كل دولة تطبيق مجموعة من الوسائل، يكون فيها إطار عمل للأمن والأمن السيبراني ولمكافحة الجرائم السيبرانية وهذه الوسائل هي تشريعية وتنظيمية وتوعوية وتثقيفية وتقنية وتعاونية فيما بين القطاع العام والقطاع الخاص في ذات الدولة[١٨].

(١) : <u>الوسائل التشريعية المقترح اعتمادها للأمان السيبراني :</u>

بداية، ينبغي على كل دولة العمل على تحديث تشريعاتها، وسن قوانين لتجريم الجرائم السيبرانية؛ فقوانين العقوبات التقليدية ليست صالحة على الدوام الحكم هذه الأفعال الجرمية الجديدة، على الأقل في حالة الأفعال التي تكون فيها المعلوماتية محل الاعتداء. وكذلك ينبغي العمل باستمرار على تحديث التشريعات لمواكبة التطور التقني والأساليب المبتكرة التي يعتمدها المجرمون وإعادة النظر في العقوبات وفي ظروف تشديدها وفق ما يظهر من ممارسات إجرامية.

(أ)- اجراء مسح وطني شامل للتشريعات ذات الصلة:

بغية وضع سياسة تشريعية فعالة ومستندة إلى معطيات علمية ودقيقة، ينبغي للدولة القيام بدراسة شاملة وتفصيلية للقوانين الموجودة فيها قبل المسارعة إلى وضع قوانين

جديدة. فهذا يحول دون إصدار قوانين غامضة قد تتعارض مع القوانين السابقة النافذة، ويحول دون الاستقصابية في تفسير المصطلحات والتعابير المبهمة من قبل النيابة العامة للتوسع في الادعاء[١٩]. وهذا يعني ضرورة النظر إلى بعض الأفعال الجرمية على الإنترنت باعتبارها جرائم عادية كلاسيكية ولكنها تستعمل وسيلة جديدة في الإنترنت أو المعلوماتية.

(ب)- تحديث تشريعات الجرائم السيبرانية وايجاد حلول البعض إشكالياتها:

تحتاج التشريعات الوطنية إلى التحديث دوريا خاصة في مكافحة الإشكاليات القانونية الناتجة عن طبيعة الفضاء السيبراني، ومن تلك الإشكاليات، علم وضع تعريف واضح وموحد للجرائم السيبرانية عامة في دولة معينة، حيث يبدو غير ذي أولوية، باعتبار أنه من الأهم وضع تعريفات محددة في التشريع الداخلي لكل جريمة سيبرانية تبين أركانها وعناصرها، تطبيقا لمبدأ "لا جريمة ولا عقوبة دون نص قانوني". ومن المسلم به أن القواعد القانونية الإجرائية التقليدية في الدول العربية المتعلقة بتنظيم آليات التحقيق في الجرائم الجزائية عاجزة عن حكم قضايا جرائم المعلوماتية نظرا للطبيعة الخاصة لها، فالمعلوماتية تمتاز بالطابع اللامادي والتقني المتخصص وبالقدرة على الزوال بسرعة وباختراق الحدود وبوجود هوية إلكترونية مختلفة عن الهوية الحقيقية وبالقدرة على إحداث أضرار جسيمة عن بعد، فلا بد من تحديث هذه القواعد.

وعلى سبيل المثال، تعتبر البيانات المعلوماتية في حيازة الشخص إذا كان يحوز ماديا جهاز الحاسوب الذي يخزنها، أو هو قادر على الوصول عن بعد إلى هذه المعلومات المخزنة على وسائط حفظ إلكترونية، حتى خارج البلاد، عبر شبكات نقل المعلومات. كما أن الإذن بالبحث عن بيانات ضمن نظام معلوماتي يمكن توسيعه ليشمل بيانات مخزنة في نظام آخر، ولكن يمكن الوصول إليها من النظام المعلوماتي الأول[٢٠].

ومن الإشكاليات التي تواجه تحديث أو وضع القوانين السيبرانية تحديد المسؤوليات الجزائية على نحو متناسق بين القوانين، وفي هذه الحالة، لا بد من إطار قانوني إجرائي في دول المنطقة ينظم جمع الأدلة المعلوماتية، مثل مراقبة الشبكات واعتراض الاتصالات وضبط أجهزة الحاسوب والبيانات المعلوماتية ولاسيما تلك التي تزول بسرعة، وإلزام مزودي خدمات الاتصال بحفظ معلومات حركة البيانات وبيانات التعريف عن أصحاب مواقع الإنترنت التي يستضيفونها وتزويد أجهزة التحقيق بها عند الحاجة. كذلك ينبغي وضع حلول لمشاكل الاختصاص القضائي، كالتنازع الإيجابي على الصلاحية،

(ISSN: 2537 - 0758)

أي عندما تدلى محاكم الدول المعنية باختصاصها بالموضوع، أو التنازع السلبي على الصلاحية، أي عندما تدلى محاكم الدول المعنية بعدم اختصاصها، وتحديد القانون الذي ينبغي تطبيقه إضافة إلى ما تقدم، يمكن لكل دولة عربية تطبيق مجموعة من الممارسات الفضلى التي تثبت نجاحها نتيجة التجارب الدول الأخرى، وضمن التوصيات المهمة حول التغييرات المفترض اعتمادها لمكافحة الجرائم السيبرانية، ينبغي القيام بما يلي (لمزيد من التفاصيل انظر التوصيات)[٢١].

- إجراء التغييرات التشريعية بالحد الأدني الكافي لضمان مستويات ملائمة من الأمن السيبراني.
- تفسير القوانين وفق طرق تسمح لأصحاب الشأن بإعطاء الأولوية للأمن السيبرائي.
- تجنب الخلط بين الجرائم السيبرانية وغيرها من المسائل، مثل الملكية الفكرية والخصوصية وحرية التعبير.
- وضع التشريعات التي تسمح لأجهزة الدولة بمهاجمة مراكز التحكم (الحواسيب الرئيسية التي تسيطر على حواسيب الأشخاص.
- تسريع إجراءات التعاون بين أجهزة التحقيق في الدول عن طريق الربط الإلكتروني بينها (مثل حفظ وتبادل البيانات المعلوماتية).
- إمكانية محاكمة الجاني في بلد إقامته لا في بلد إقامة الضحية، وذلك في حال رفض طلب استردادها.
- في هذا الإطار، تقترح الإسكوا، استكمالا ل "إرشادات الإسكوا للتشريعات السيبرانية" الصادرة في عالم ٢٠١٢، قانونا نموذجيا جديدا متعلقا بالقواعد الإجرائية الخاصة بالجرائم السيبرانية والأدلة الرقمية، وهو مقتبس من اتفاقية بودابست(٢٢).

(ت): تنسيق التشريعات بين الدول العربية والاسترشاد بإرشادات الإسكوا التشريعات السيبرانية:

ينبغي توحيد المقاربة التشريعية بين الدول ، أو على الأقل تنسيقها. كما ينبغي وضع تعاريف موحدة أو متناسقة، للجرائم السيبرانية وكذلك ينبغي وضع سلم متناسق للعقوبات؛ إذ يمكن التفلت من الملاحقة إذا كانت دولة معينة تجرم فعلا معينا في حين لا تجرمه دولة أخرى. كما أن التعاون بين الأجهزة الرسمية فيما بين الدول لا يكفي لوحده، بل يعتبر إشراك القطاع الخاص ذا أهمية، خاصة الشركات التي توفر التجهيزات

والبرامج المعلوماتية وكذلك شركات الاتصالات[٢٣] إن معظم الدول ترفض التعاون إذا كان الفعل الجرمي المرتكب في دولة أخرى غير مجرم في قانونها الداخلي (التجريم المزدوج)، فالتعاون بين الدول يقتصر على الجرائم المجرمة في جميع هذه الدول. فطالما أن التقنيات المستخدمة في مجال تكنولوجيا المعلومات هي نفسها على مستوى العالم، فمن الأولى أن تكون تعاريف الانتهاكات المستندة إلى هذه التقنيات هي ذاتها".

كما يمكن للدول الأسترشاد في سن تشريعاتها المتعلقة بالجانب الموضوعي وبقسم من الجانب الإجرائي بإرشادات الإسكوا للتشريعات السيبرانية التي صدرت عام ٢٠١٢، وهي ملائمة للتطبيق في الدول ذات النظام القانوني المبني على القانون اللاتيني، وذلك باعتبار أن هذه الإرشادات مستوحاة من إرشادات الاتحاد الأوروبي والقوانين الفرنسية والأوروبية كما يمكن للدول الاسترشاد بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات العام ٢٠١٠، وبالقانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام ٢٠٠٣، والقانون العربي الاسترشادي للإثبات بالتقنيات الحديثة لعام ٢٠٠٨، والقانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية لعام ٢٠٠٩.

وقد تضمنت إرشادات الإسكوا للتشريعات السيبرانية لعام ٢٠١٢ القواعد الموضوعية المتعلقة بهذه الجرائم، ومنها التعدي على البيانات المعلوماتية، والتعدي على الأنظمة المعلوماتية وإساءة استعمال الأجهزة أو البرامج المعلوماتية، والتعدي على الأموال والمعاملات بوسائل إلكترونية، وجرائم الاستغلال الجنسي للقاصرين بوساتل معلوماتية، والتعدي على الملكية الفكرية للأعمال الرقمية، وجرائم البطاقات المصرفية والنقود الإلكترونية، وجرائم المعلومات الشخصية، وجرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، والمقامرة وترويج المواد المخدرة بوسائل معلوماتية[٢٤].

وجرائم المعلوماتية ضد الدولة والسلامة العامة، وتشفير المعلومات. ومن ثم فقد تضمن الإرشاد النوع الأول من جرائم المعلوماتية، حيث تكون المعلوماتية موضوع الفعل الجرمي، كالاعتداء على الأنظمة المعلوماتية، وكذلك النوع الثاني من الجرائم المعلوماتية، حيث تكون المعلوماتية هي وسيلة ارتكاب فعل جرمي تقليدي كالاحتيال أو السرقة أو السب.

ولم ينظم الإرشاد القضايا الإجرائية في التحقيقات القضائية، بل أشار فقط في مادة وحيدة إلى التعاون الدولي في هذا المجال، حيث تنص المادة ٥٦ على أنه على الدول

(ISSN: 2537 - 0758)

الأعضاء أن تلتزم المعاهدات والاتفاقيات الدولية ذات الطابع الجماعي أو الثنائي المتعلقة بمكافحة الجرائم عموما، مع مراعاة طبيعة الجرائم السيبرانية، وذلك من حيث تسهيل وتسريع الإجراءات الخاصة بجمع الأدلة وضبطها وتبادل المعلومات حول الجرائم المذكورة وملاحقة مرتكبيها، كما تحرص الدول الأعضاء على التعاون فيما بينها في مجال التحقيقات القضائية في جرائم المعلوماتية، وأعمال رصدها ومكافحتها.

(ث) – الاسترشاد باتفاقية بودابست:

يمكن الاسترشاد بالقواعد الإجرائية الأساسية في مجال تحقيقات جرائم المعلوماتية التي يمكن العودة إليها أيضا في اتفاقية بودابست، حيث تقوم الدول العربية بإدخال مبادئها ضمن أنظمتها القانونية. وتتمحور القواعد الإجرائية حول إعطاء أجهزة التحقيق الصلاحيات التالية:

- إلزام أي شخص يحفظ بيانات معلوماتية، ومنها معلومات حركة البيانات (Tnaflic data).
- إلزام مزودي خدمات الاتصال بتزويد أجهزة التحقيق بمعلومات حركة البيانات وببيانات التعريف الشخصية حول أصحاب المواقع الإلكترونية subscriber information التي يستضيفونها، وإلزام أي شخص بتزويدها ببيانات معلوماتية محددة هي بحوزته.
- الوصول إلى أنظمة الحاسوب والمعلومات وضبطها.
- الوصول إلى معلومات حركة البيانات في زمن الإرسال الحقيقي، إما مباشرة أو عن طريق مزودي خدمات الاتصال.
- الوصول إلى محتوى الاتصال أو المعلومات بذاتها content data في زمن الإرسال الحقيقي، إما مباشرة أو عن طريق مزودي خدمات الاتصال.
- إلزام أي شخص لديه معلومات حول طرق عمل نظام معلوماتي والتدابير التقنية لحمايته بالمساعدة على ضبط البيانات أو النظام[٢٥].
- إعطاء الصلاحية القضائية المحاكم البلد الذي وقع فيه الجرم أو في حال وجود المتهم على أراضي هذا البلد، وعدم إجابة طلب الاسترداد المقدم من بلد أخر بسبب جنسية المتهم التابع البلد الأول.

- ومن المفيد إعطاء الصلاحية لمحاكم البلد الذي نشأ منه الاعتداء المعلوماتي ومكان وجود المرتكب (محل وإقامة المجرم)، وإن كانت آثار الفعل قد لحقت بنظام معلوماتي خارج البلاد، وذلك نظرا لتسهيل السير بالتحقيق وإمكانية توقيف الفاعل.

(ج) انشاء وحدات متخصصة لتطبيق القانون:

أشارت إرشادات الإسكوا للتشريعات السيبرانية بمادة وحيدة إلى التطويرات البنيوية في الهياكل التنظيمية للسلطات بهدف محاربة جرائم المعلوماتية، عن طريق إنشاء وحدات متخصصة في أجهزة الشرطة التي تتولى التحقيقات الجزائية، حيث تنص المادة ٥٥ على أنه "تحرص الدول الأعضاء على إنشاء وحدة متخصصة في جرائم المعلوماتية في الأجهزة الأمنية المولجة بالتحقيقات القضائية تحت إشراف القضاء، كالضابطة العدلية تتولى هذه الوحدة أعمال التحقيق في هذه الجرائم ورصدها تحت إشراف القضاء. ويتألف الجهاز البشري لهذه الوحدة من عناصر فنية متخصصة ذات كفاءة في مجال المعلوماتية والاتصالات"[٢٦] وتوجد عدة نماذج معتمدة في الدول التنظيم وحدات التحقيقات في مجال الأدلة المعلوماتية) لجات بعض الدول إلى إنشاء وحدات متخصصة داخل النيابات العامة لتتولى التحقيق في الجرائم السيبرانية، فيراس الوحدة مدع عام ويتشكل فريق من محققين وتقنيين(٢٧). أو كخيار آخر، يمكن تكوين قوة مشتركة بين عدة مؤسسات تتضمن محققين وفنيين ورجال شرطة؛(٢٨) وفي الخيار الأخير، يمكن إنشاء وحدات مركزية للتحقيق في مجال الأدلة المعلوماتية أو وحدات لامركزية في المناطق، ويمكن اعتماد أي من هذه النماذج من قبل الدول العربية. وقد يدخل الأمن السيبراني، وفق توزيع الصلاحيات في كل دولة عربية، ضمن اختصاص عدة وحدات أو أقسام في وزارات مختلفة، منها ما يتعلق بحماية المستهلك (من الاحتيال المعلوماتي) أو أجهزة الأمن القومي ضمن وزارة الدفاع، إضافة إلى مراكز الاستجابة لطوارئ الحاسوب.

ومن الأهمية بمكان التنسيق فيما بين الوزارات والهيئات المتخصصة في البلد الواحد من أجل مكافحة الجرائم السيبرانية وخاصة وزارة العدل ووزارة الاقتصاد ووزارة الاتصالات ووزارة الداخلية وذلك بهدف منع التضارب في الصلاحيات والاختصاصات وتعزيز التعاون فيما بينها وتدريب العاملين المعنيين فيها على التشريعات السيبرانية وصولا إلى التعاون لمكافحة الجرائم السيبرانية. وبهدف التعامل مع خصوصيات المرأة، ينبغي أن تتوفر لدى فرق التحقيق خبرات في التعامل مع الجرائم السيبرانية التي يمكن

(ISSN: 2537 - 0758)

أن تركز على العنف القائم على النوع الاجتماعي أو العنف ضد المرأة، خاصة عندما تكون الضحية امرأة، إضافة إلى إدخال عناصر نسائية ضمن فرق التحقيق لديها خبرات كافية بالجرائم السيبرانية. وينبغي أيضا أن يكون لدى أعضاء النيابة العامة خبرة في هذا الموضوع حتى يتمكنوا من ملاحقة المذنبين بارتكاب جرائم سيبرانية ترتبط بالنوع الاجتماعي، دون التأثير على الصحة البدنية والعقلية للضحايا وفي جميع الأحوال، تكمن مهمة النيابات العامة في توجيه المحققين خلال التحقيقات وتحديد الأدلة المعلوماتية المطلوب جمعها لإثبات الوقائع الجرمية وتطوير الآليات والنماذج لمذكرات التفتيش والتوقيف والعمل على توعية الجمهور من الجريمة المعلوماتية وينبغي أن يكون المدعي العام المشرف على هذه التحقيقات مطلعا على التشريعات السيبرانية وعلى دراية بالتقنيات المعلوماتية[٢٩].

د) تعزيز الإجراءات الاستباقية للأمان السيبراني:

إن رصد الجرائم السيبرانية والاحاطة الكاملة بتقنياتها واستيقاها، وضبطها وإعاقتها على الخط، دوئه صعوبة الوتيرة السريعة والطابع العابر للحدود الجريمة السيبراتية، الذي يطرح تحديات جديدة على صعيد تطبيق القانون، ويتطلب آليات قانونية مبتكرة تفوق تلك المتبعة بخصوص الجرائم التقليدية [٣٠]. ويتبين من دراسة للأمم المتحدة أن نسبة الجرائم السيبرانية المكتشفة من خلال تحقيق استباقي متدنية، لكن بعض الدول تركز على استراتيجية الأعمال المخفية ضد المخاطر السيبرانية[٣١]. ومن هنا تنبع أهمية بناء قدرات الأجهزة الرسمية في الدول العربية لاستباق أي اعتداء على الأمن السيبراني والاستعداد له وإعاقته، وفي هذا الإطار، يتم إعداد ما يعرف بالمحققين الاستباقيين proactive investigators القادرين على التواصل مع المرتكبين المرتقبين، حيث يمكن للمحقق أن ينتحل شخصية الضحية للإيقاع بالمرتكب كذلك تقوم وحدات متخفية بمراقبة مواقع التواصل الأجتماعي وبعض منتديات الثقاش والرسائل الفورية وخدمات الند للند pcr–to–peer ومراقبة أجهزة التحكم لبعض البرمجيات الخبيثة ويتوقف هذا الأمر على إجازة القانون في كل دولة لهذا العمل التحقيقي الاستباقي ففي نظام غير مركزي كالإنترنت، يؤدي نظام الإنذار المبكر عن المخاطر دورا حاسما في الأمن السيبراني؛ ومن هنا تبرز أهمية وضع خطط للاستجابة السريعة للأحداث التي قد تحصل على الشبكة وللدفاع عن البلد ضد الهجمات السيبرانية وعلى الدول العربية الأستثمار في مراكز الاستجابة لطواري الحاسوب وإعطائها دورا قياديا على صعيد استباق وتحديد

المخاطر السيبرانية وكذلك إعطائها صلاحية تنسيق المعالجات المطلوبة لدى أجهزة الدولة كافة ويتطلب دعم هذه المراكز توظيف كفاءات تقنية عالية وتطوير قدراتها الدفاعية في الفضاء السيبراني، وتأمين الإمكانيات لإعادة الوضع إلى ما كان عليه قبل حصول الخلل المعلوماتى recovery. وقد تبين أن أداء المراكز الحالية للاستجابة لطوارئ الحاسوب في المنطقة العربية لا يوفر الفعالية المطلوبة في بعض الأحيان، بسبب ضعف آليات التواصل مع المجتمع، ومحدودية الموارد البشرية الفنية المؤهلة، أو الحاجة لمزيد من التمويل أو التنظيم أو التنسيق مع باقي وزارات الدولة المعنية.

(ز) اعتماد وسائل ناجعة للتوعية والتدريب حول الأمان السيبراني:

(١)- اعتماد آليات ناجحة للتوعية ونشر ثقافة إدارة مخاطر تكنولوجيا المعلومات:

يفتقد المجتمع العربي اليوم إلى ثقافة إدارة مخاطر تكنولوجيا المعلومات. فالمواطن العربي نادرا ما يهتم لهذا الأمر، إما لعدم المعرفة أو الإهمال أو رمي المسؤولية على عاتق الدولة. إلا أن إدراك الأشخاص ووعيهم لمخاطر التعاملات على الإنترنت هو خط الدفاع الأول في مكافحة الجرائم السيبرانية. لقد كان المحتالون يستعملون برامج المسح بوابات أجهزة الحاسوب والعثور على غير المحمي منها أو اختراق كلمات السر. ومع تطور برامج مكافحة الفيروسات والتجسس المعلوماتي وبرامج مكافحة البرمجيات الخبيثة عموما، وازدياد فعاليتها، أصبح المعتدون يلجأون أكثر إلى ما يسمى "الهندسة الاجتماعية" للوصول إلى ضحاياهم. وهذه الطريقة ترتكز على التفاعل الإنشائي عن طريق منتديات النقاش أو رسائل البريد الإلكتروني[٣٢].

وتهدف إلى خداع الضحية لتنزيل برامج تحكم على حواسيبها أو فضح معلومات عنها. وهذه الطريقة غير التقنية لاستهداف الضحايا تنجح حتى في حالة الحواسيب المحمية تقنيا. ومن هنا تظهر أهمية دور الحكومات العربية في اعتماد وسائل تواصل فعالة مع المجتمع النشر التوعية. ويمكن تنبيه وتوعية المستخدم على بعض المخاطر المستجدة عن طريق شبكات التواصل الاجتماعي، التي يرتادها الأشخاص ارتيادا شبه يومي مما يسرع عملية الاستجابة للخطر المستجد. كما يمكن الاسترشاد بما يقوم به مكتب التحقيقات الفدرالية في الولايات المتحدة الأمريكية، من حيث نشره على موقعه الإلكتروني (١) حالات الاحتيال الإلكتروني التي يتم الإبلاغ عنها، وذلك لتلبية الجمهور من التعرض لها، وكذلك الإعلامه بالخطوات المطلوبة من قبل الأفراد لحماية أنفسهم.

(ISSN: 2537 - 0758)

كما تقوم مراكز الاستجابة السريعة لطواري الحاسوب بتوعية مستخدمي الإنترنت عبر نشر الأخطار السيبرانية التي يتم اكتشافها أو الإبلاغ عنها حديثا بما فيها جرائم العنف ضد المرأة على الفضاء السيبراني، مع طرق تفاديها من الناحية التقنية والعلانية . ويمكن أيضا اعتماد عدة وسائل لنشر الوعي حول المخاطر في الفضاء السيبراني عن طريق: البرامج التلفزيونية، والمقابلات الإعلامية، وتوزيع الكتيبات، والمحاضرات في الجامعات والمدارس، والأفلام القصيرة، واللعب التفاعلية، وإنشاء مواقع إلكترونية أو صفحات على الإنترنت أو الفيسبوك للتوعية، والرسائل النصية القصيرة، والمؤتمرات، والخطابات الموجهة للجمهور. ويمكن أن تتضمن هذه البرامج وصفا لأشكال وأنواع الجرائم السيبرانية بما فيها تلك التي تستهدف النساء والأطفال. كما ينبغي للدول العربية الاهتمام بالتوعية بمخاطر العنف ضد المرأة على الفضاء السيبراني، ويحبذ أن تتفاعل السلطات الحكومية مع المنظمات غير الحكومية ومنظمات المجتمع المدني المعنية بشؤون المرأة لتثقيف النساء حول الجريمة الإلكترونية وأليات الحماية والأمن في الفضاء السيبراني. وذلك نظرا لكونها موضع ثقة للنساء في المجتمع، ولكونها وسيلة جيدة للوصول إلى أكبر طيف من النساء سواء في المدينة أو في الريف. كما يمكن زيادة التوعية وبشكل خاص عند النساء عن طريق نشر بعض التجارب أو القصص التي قامت فيها السيدات بإبلاغ عن جرائم سيبرانية خاصة بهن مع ضرورة الحفاظ على السرية والخصوصية عند سرد مثل هذه التجارب. ويمكن للدول الأقل نموا طلب المساعدة في مجال التوعية والتدريب من الدول الأكثر نموا، خاصة تلك التي لها مصلحة في ذلك، والاستفادة من الخبرات التي اكتسبتها في مجال التوعية.

(٢) توعية مختلف الفئات في المجتمع:

*** المستخدمون:**

يجب أن تكون برامج التوعية موجهة إلى فئات محددة من المجتمع، منها: الأطفال، والطلاب، والهيئات الحكومية، والمؤسسات الخاصة، والأشخاص المسنون، والأشخاص ذوي الإعاقة فهكذا، يمكن تحديد هدف برنامج التوعية وآليته وأنشطته بحسب الفئة المستهدفة وحاجاتها ومستوى المعرفة فيها. وتؤكد دراسة للأمم المتحدة أهمية حملات التوعية المستمرة، ولا سيما تلك التي تتعلق بالمخاطر السيبرانية التي تستجد، وكذلك التي تستهدف فتات معينة كالأطفال مثلا(٣٣).

وتعتبر التوعية محورية لطلاب المدارس والجامعات، حيث أن نسبة كبيرة من هؤلاء الطلاب أصبحوا مستخدمين معتادين للإنترنت بحكم دراستهم ونمط حياتهم اليومي على شبكات التواصل الاجتماعي ومنتديات النقاش والبريد الإلكتروني. وينبغي التركيز على الفروق الجنسية بين الفتيات والفتيان في حملات التوعية.

كما يمكن حث الشركات في الدول العربية على اعتماد الخطوات العملية التالية لتوعية الموظفين إشراك الإدارة العليا ومجلس الإدارة بهذه المخاطر ومدى تأثيرها على وضع السياسات الاستراتيجية للأعمال، وإعادة النظر دوريا وبسرعة في مدى استعداد المؤسسة لهذه الجرائم، وإنشاء فريق عمل مسيبراني للتدخل السريع، وتوظيف كفاءات تقنية، واتخاذ الإجراءات القانونية الحازمة بحق المنتهكين، والتواصل المستمر مع الآخرين لمعرفة اتجاهات الجرائم السيبرانية الحالية، فالخبراء مدعوون إلى بذل جهد متواصل وإلى إدخال مواد التدريب حول الأمن السيبراني في مناهج المدارس والجامعات وساتر المؤسسات التربوية التثقيف المجتمع برمته، إضافة إلى تدريب مركز المديرين ومتخذي القرارات في الشركات وتدريب مستمر متخصص للفنيين المعلوماتيين[٣٤] .

*** المشرعون والقضاة والمحامون:**

إن التوعية اللازمة من أجل تحسين الأمن السيبراني تشمل بالإضافة إلى المستخدمين المختلفين المشرعون أيضا، إذ لا بد من توعية المشرع حول مخاطر الجرائم السيبرانية لحثه على تحديث التشريعات الضرورية في هذا المجال، مع العلم أن العملية التشريعية عملية بطيئة وغير مواكبة عادة التقدم السريع للتكنولوجيا. كما لا بد من توعية القضاة حول مخاطر الجرائم السيبرانية والأضرار الجسيمة التي تنشأ عنها، وبيان الأبعاد المختلفة للاستخدام المسيء لتكنولوجيا المعلومات والاتصالات وآلياته ونتائجة الأجتماعية والاقتصادية كما لا بد من إعلام المشرعين أيضا بالدليل الرقمي وإمكانيات الاستفادة منه وبالإضافة إلى برامج التوعية للمشرعين، لا بد من وضع خطة عمل لبرامج تدريبية متخصصة للقضاة والمحامين كما هو مبين في الفقرة التالية.

(ص)- تشجيع النساء والرجال على التبليغ عن الجرائم السيبرانية:

ينبغي أن تتخذ الحكومات خطوات عملية لتشجيع النساء والرجال والمؤسسات في الدول العربية على التبليغ عن الجرائم السيبرانية لعدة أهداف، منها بناء قاعدة معلومات وطنية تصلح لرسم استراتيجية للتعامل في المستقبل مع هذا النوع من الجرائم. وتحتاج هذه العملية إلى تحديد مرجع موحد لتلقي شكاوي الجرائم السيبرانية، ومن الأفضل أن يتم ذلك على الخط بحيث يستطيع جميع الأفراد التبليغ عن الانتهاكات التي تعرضوا لها حتى ولو كانوا يقطنون مناطق ريفية أو ثانية وتجدر الإشارة إلى أنه قد يكون من

(ISSN: 2537 - 0758)

الصعب على بعض الفئات الاجتماعية، مثل المرأة أو الطفل، تقديم تقرير أو الإبلاغ عن الجرائم السيبرانية التي تعرضوا لها، ولذلك فإنه من الأهمية بمكان إنشاء وحدات خاصة تتضمن بالإضافة إلى ضباط الشرطة أخصائيين اجتماعيين ومستشارين في شؤون المرأة أو الطفل المساعدة في التبليغ عن الجرائم السيبرانية وبيان ملابساتها. وفي حالات التبليغ عن الجرائم على الخط، يمكن إضافة خيارات تسمح للأشخاص بالتبليغ دون التصريح عن هويتهم من أجل زيادة السرية(٣٥). وينبغي أيضا إنشاء قاعدة بيانات وطنية حول الجرائم السيبرانية لتجميع المعلومات والإحصاءات عنها بالتفصيل بحيث تكون هذه الإحصاءات دقيقة ومعبرة فعليا عن الاعتداءات السيبرانية ومصنفة حسب النوع الاجتماعي ويجدر، بعد تحليل قاعدة البيانات، تحديث النماذج التي يملؤها الضحايا. وفي كثير من الدول لا يتم التمييز في تقارير الشرطة بين الجرائم التقليدية التي تتم على الخط Online أو خارج الخط Offline. لذا، من المهم اتباع نماذج جديدة للتقارير الشرطة تفرق بين هذين النوعين من الجرائم(٣٦).

(ض) دورات للقضاة والمحققين والشرطة :

يعتبر بناء قدرات القانونين من أهم الأنشطة التي تقوم بها الدول للحفاظ على الأمان السيبراني. ويتم ذلك عبر إطلاق دورات تدريبية تخصصية للعاملين في مجال السلامة المعلوماتية ومكافحة الجرائم السيبرانية لتمكينهم من القيام بمهامهم على أكمل وجه، وتحديث معارفهم، ولا سيما مع تسارع التطور التقني وابتكارات المجرمين والمخترقين. ويهدف التدريب الموجه إلى القضاة والمحققين وإلى الرجال والنساء العاملين في الشرطة إلى بناء قدراتهم ومعارفهم لمحاربة الجرائم السيبرانية، وتدريبهم على استخدام الأدوات المعلوماتية في التحقيقات الجزائية وتتضمن مواضيع التدريب الموجهة إلى المحققين الإطار القانوني للجرائم والتحقيقات وضبط أو جمع الأدلة الرقمية وحفظها وتحليلها(٣٧)، والتحقيقات المتوفرة على الإنترنت، وضبط أجهزة الهاتف النقال وتحليلها١٣ إضافة إلى كيفية التعامل مع القضايا الحساسة وتلك المتعلقة بالعنف ضد المرأة. ويتم التدريب بواسطة متخصص بالتدريب ضمن القضاء ووحدات الشرطة، كمعهد القضاة وأكاديمية الشرطة، وبالاستعانة بخبراء محليين ودوليين. أما الحالات الأكثر تعقيدا من الجرائم السيبرانية، أو تلك التي تستخدم تقنيات متقدمة، فتترك الوحدات متخصصة من الشرطة(٣٨).

ومن الأهمية بمكان إدراج مواضيع الجرائم السيبرانية المتعلقة بالنوع الاجتماعي والجرائم التي تستهدف النساء بشكل خاص ضمن برامج الدورات التدريبية ويبين التدريب كيفية مقاربة الجرائم التقليدية ضد المرأة بجرائم سيبرانية، والآليات المطلوب اعتمادها

لمعالجة هذه الجرائم. وينبغي أن تشمل حملات التوعية والتدريب جميع المعنيين بالأمان السيبراني من الرجال أو النساء، سواء في السلك القضائي أو الإجرائي والجزائي، حتى لو تلقوا دورات سابقة، وذلك لمواكبة التطور التقني وتطور الأساليب التي يتبعها المرتكبون.

*** دورات تدريبية للتقنيين في جهاز الشرطة**

أو مراكز الاستجابة لطوارئ الحاسوب ينبغي أن تجري الدولة دورات تدريبية تخصصية دورية للتقنيين في جهاز الشرطة أو مراكز الاستجابة الطوارئ الحاسوب، لتمكينهم من القيام بعملهم على أكمل وجه، وتحديث معارفهم في ظل التطور التقني المتسارع(٣٩).

وتشمل هذه الدورات المواضيع التالية: جمع الأدلة الرقمية وحفظها، والتحليل المتقدم للأدلة الرقمية، واكتشاف الحوادث السيبرانية والإنذار المبكر، والمعالجة أو الإدارة المتقدمة للحوادث السيبرانية، وكيفية إنشاء مركز للاستجابة لطوارئ الحاسوب، وتحليل الفيروسات وبرامج التجسس والاختراق، ومكامن الضعف للبرامج، وأمن الشبكات والمعلومات، وأمن الإنترنت والسيناريوهات المختلفة للهجمات، وكتابة البرمجيات الآمنة، والضمان المتعلق بموردي البرامج(٤٠).

*** إدخال موضوع الجرائم السيبرانية في المناهج التعليمية:**

يجب حث الجامعات على إدخال مناهج حول تعزيز آليات الأمن السيبراني ومكافحة الجرائم السيبرانية في الجامعات المتخصصة وخاصة في كليات المعلوماتية والحقوق وفي المعاهد القضائية والإدارية كما يجب إدراج برامج خاصة للدراسات العليا وإنشاء اختصاصات في هذا المجال وذلك من أجل توفير خبرات متخصصة في الدول العربية، كما يجب أيضا إدراج موضوع الأمان السيبراني في برامج المعلوماتية في المدارس والمعاهد كافة

المطلب الثانى
إقرار مبدأ التعاون لمجابهة الجرائم السيبرانية

(أولا) التعاون بين القطاعين العام والخاص والمجتمع المدني:

*** التعاون بين القطاعين العام والخاص ومبرراته ومواضيعه:**

تدعم الشراكة بين القطاع العام والخاص عملية حفظ الأمان والأمن السيبراني عبر تبادل المعلومات وتشارك العبء المادي والتعاون العملي والإجرائي (التحقيقات، التتبع، الإنذار، إدارة الأزمة)(٤١). فإنشاء الشراكة بين هذين القطاعين في مجال الأمان والأمن السيبراني هو أمر هام وواعد، وقد تم تطبيقه في عدة دول متقدمة مثل الولايات المتحدة

(ISSN: 2537 - 0758)

الأمريكية والاتحاد[٤٢]. لذا يجدر بالدول وضع وتحفيز آليات التعاون والشراكة بين القطاعين العام والخاص وخاصة مع مزودي خدمات الاتصال وفي ما يخص تبادل المعلومات حول الجرائم السيبرانية، وحفظ معلومات حركة البيانات وبيانات التعريف عن المستخدمين، وتقديمها لأجهزة التحقيق. كما أن للقطاع الخاص ومزودو خدمات الشبكة دور هام في تطوير وتشجيع البرمجيات الأمنة، ونشر وتحفيز طرق الوقاية من الجرائم والمخاطر السيبرانية، وكذلك في وضع برامج التوعية الملائمة لكافة أفراد المجتمع. ويجب حكما في هذا النوع من الشراكة إيجاد توازن بين مصالح كل من الطرفين فكثيرا ما تكون الشركات الخاصة سباقة في كشف الطرق المستجدة لارتكاب الجرائم السيبرانية واختراق الأنظمة المعلوماتية، وكيفية الوقاية منها؛ غير أنها غالبا ما تحجم عن التعاون لأسباب تتعلق بالخصوصية، والأسرار التجارية، أو عدم المبالاة. ومن ناحية ثانية، ترفض الدول تزويد الشركات الخاصة بالمعلومات لأسباب تتعلق بالأمن القومي. ويعود لكل دولة عربية تمويل الأبحاث في مجالات الأمن السيبراني لابتكار حلول جديدة ومبتكرة في هذا المجال. كما ينبغي تشجيع الشركات والمعاهد والجامعات على الاستثمار في مجال أبحاث الأمن السيبراني، من حيث صناعة التجهيزات والبرمجيات المعلوماتية.

*** تنسيق دور القطاعين العام والخاص كمزودي خدمات الشبكة :**

نشأت نتيجة التجربة في بعض الدول، مجموعة من الممارسات الفضلى في مجال الأمان السيبراني التي يمكن الاسترشاد بها، ومنها تولى الحكومات الرقابة التقنية في مجال الأمن السيبراني، لا تفويضها إلى القطاع الخاص إيجاد حلول تضمن الأمن السيبراني من دون التعرض للخصوصية؛ .جعل المؤسسات التي تتولى إدارة الإنترنت شريكة في وضع الحلول؛ .جمع المعلومات حول الجرائم السيبرانية وبناء قاعدة معلومات وطنية/إقليمية عالمية عنها؛ .إلزام مصنعي التجهيزات المعلوماتية يجعل منتجاتهم آمنة، عن طريق جعل تحديثات البرامج المتعلقة بالأمان السيبراني آلية، وأن لا تتم (لا تفعل الصيانة عن بعد إلا من قبل المستخدم بعد اعتماد كلمات سعر معقدة إجراء تغييرات لدى كل شخص ليس فقط لحماية نفسه بل لحماية الأشخاص الآخرين؛ النظر إلى موضوع الأمان السيبراني من منظور دولي بسبب عالمية الإنترنت (الحيز العالمي) وبالتالي يجب إجراء التعديلات الفنية والتقنية في كل بلد ضمن إطار عمل متناسق؛| حفظ بيانات التعريف الخاصة بالموردين في مجال التجارة الإلكترونية؛ فالغفلية لا تساعد في مكافحة الجرائم السيبرانية؛.زيادة الاستثمارات في مجال تطبيق القانون لمكافحة الجرائم السيبرانية، علما أنها تبقى أقل من تلك المخصصة للجرائم التقليدية؛ .مراقبة الشبكات والتعاون مع مزودي خدمات الاتصال، وتزويدهم بالعناوين الرقمية IP للحواسيب المسيطر عليها لإبلاغ أصحابها؛[٤٣]. تخويل مزودي خدمات الشبكة الذين

يقومون بالنقل العابر للبيانات Transit Providers وقف البيانات الصادرة عن الحواسيب المسيطر عليها Botnet بعد فحص البيانات التقنية لرزم المعلومات packet headlers .

تمكين مزودي خدمات الاتصال من منع رزم المعلومات من الخروج من شبكتهم إذا كان العنوان الرقمي المذكور فيها للمرسل غير صحيح، وهو ما يعرف بتقليد العنوان الرقمي IP Spooling. زيادة التمويل من القطاع الخاص والعام للجهود الرامية إلى تثقيف المستهلك حول الأمان السيبرائي؛ .عدم السماح للحواسيب غير المحمية تقنية من الاتصال بالإنترنت؛ إنشاء وسائل أمنة للشركات الخاصة من أجل تبادل المعلومات حول المستخدمين المخترقين معلوماتيا وذلك خارج إطار القواعد التقليدية؛ حث مسجلي مواقع الإنترنت (registries/registrars) للتدقيق في بيانات التعريف حول أصحاب المواقع والتأكد من صحتها، وحث الأيكان (ICANN The Internet Corporation for Assignol Names and Numbers) على تطبيق قواعد السلامة لديها.

*** تعاون الدولة مع المجتمع المدني ومزودي خدمات الشبكة :**

يقتضي على الدولة محاورة جمعيات المجتمع المدني التي قد تعارض الإجراءات الجزائية في مجال تحقيقات القضايا السيبرانية ومن هذه الجهات، جمعيات الدفاع عن الحريات العامة، التي قد تتسبب بتعريض الخصوصيات والحريات الخاصة للانتهاك يفعل ضبط معلومات حركة البيانات ومحتوى الرسائل. ومن هذه الجهات أيضا، مزودو خدمات الاتصال والذين قد يعترضون على الأعباء الإضافية التي ألقيت على عاتقهم من حيث حفظ معلومات حركة البيانات ومحتوى الرسائل

(و) التعاون بين الدول من أجل تعزيز الأمان السيبراني

***- تعزيز التعاون البيني في العالم ومبرراته ومضامينه:**

يشكل تعزيز التعاون بين الدول العربية، وبينها وبين بقية الدول، حجر الأساس لمكافحة الجرائم السيبرانية ولتعزيز الأمان السيبراني، نظرا للطابع العابر الحدود لهذه الجرائم. ويمكن البدء بتفعيل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات العام ٢٠١٠ وتطبيقها؛ وقد تضمنت هذه الاتفاقية تنظيما حديثا لآليات التعاون. ويمكن كذلك الاسترشاد بإرشادات الإسكوا الخاصة بالتشريعات السيبرانية ومنها الاسترشاد الخاص بالجرائم الإلكترونية مضافا إليه الجزء الإجرائي الموضح في المرفق الثالث لهذه الدراسة والمقتبس من اتفاقية بودابست. وتفيد هذه الاتفاقيات الإرشادات في إعداد واعتماد اتفاقيات ثنائية أو صياغة تفاهمات بين الدول العربية أو في مراجعة الاتفاقية العربية لجرائم تقنية المعلومات. وقد تضمنت الاتفاقيات المذكورة قواعد خاصة حول التعاون القضائي بين الدول بخصوص جمع الأدلة المعلوماتية والتحقيق في الجرائم السيبرائية

(ISSN: 2537 - 0758)

وهذه القواعد تتلخص بالآتي:

- التعاون إلى أقصى الحدود بين الدول في التحقيقات الجزائية وجمع الأدلة المعلوماتية، حتى في الجرائم التقليدية.
- اعتبار الجرائم السيبرانية من الجرائم التي يقبل فيها استرداد المتهمين إذا كان معاقب عليها في الدولتين بعقوبة سالبة للحرية لمدة تزيد على سنة، أو بعقوبة أشد.
- الاستجابة لطلبات التعاون الموجهة بوسائل الاتصال السريعة، كالبريد الإلكتروني أو الفاكس، بشرط ضمان مستوى ملائم من الأمن والمصادقة على المصدر، ويمكن اشتراط تأكيد الطلب بمراسلة رسمية.
- إرسال معلومات إلى دولة أخرى قد تفيدها في التحقيق في جريمة سيبرانية.
- تسمية نقطة اتصال لدى كل دولة لإرسال طلبات المساعدة المتبادلة أو للإجابة عليها أو لتنفيذها.
- حفظ البيانات المعلوماتية الموجودة على أراضي دولة مدة لا تقل عن ٦٠ يوما، بناء على طلب دولة أخرى، على أن يتم ضبط هذه البيانات بصورة الأحقة بناء على طلب الدولة الأخرى.
- الاستجابة لطلبات المساعدة المتبادلة المقدمة من دولة أخرى للبحث عن بيانات معلوماتية أو لضبطها أو لإعطائها، عندما تكون موجودة على أراضي الدولة الموجه اليها الطلب.
- السماح لسلطات دولة بالوصول، عن طريق نظام معلوماتي موجود على أراضيها، إلى بيانات معلوماتية مخزنة على أراضي دولة أخرى، وذلك في حال موافقة الشخص صاحب السلطة على البيانات.
- تقديم المساعدة المتبادلة، عن طريق تقديم معلومات حركة البيانات الجارية tralTic data على أراضي إحدى الدول في زمن الإرسال الحقيقي real time تقديم المساعدة المتبادلة، عن طريق تقديم أو تسجيل محتوى الرسالة أو المعلومات المنقولة بواسطة نظام معلوماتي على أراضي إحدى الدول في زمن الإرسال الحقيقي rcal time، بالقدر الذي تسمح به قوانين تلك الدولة.
- تسمية نقطة اتصال متاحة ٢٤ /٢٤ ساعة، سبعة أيام في الأسبوع، لتقديم المساعدة المتبادلة.

من ناحية أخرى يجب أيضا العمل على توحيد المصطلحات الخاصة بالأمان والأمن السيبراني وكذلك التشريعات السيبرانية من أجل تسهيل تبادل المعرفة والخيرات، وكذلك من أجل التنسيق بين التشريعات، وتسهيل التعاون والتفاعل فيما بين القضاة ورجال الشرطة وخاصة عند مكافحة الجرائم السيبرانية

*** تحسين آليات التعاون القضائي بين الدول:**

يبدو في التحقيقات الجزائية المهمة، حيث يكون عامل الوقت حاسما، أن التعاون القضائي في مجال الجرائم السيبرانية قد تحسن تحسنا ملحوظا في السنوات الأخيرة، وذلك نتيجة لاتفاقية بودابست وللاتفاقية العربية لمكافحة جرائم تقنية المعلومات. غير أن نقاط ضعف اتفاقية بودابست هي عدم اعتمادها لدى أطراف أساسيين في العالم في هذا المجال، كروسيا والصين، وكذلك بعض دول آسيا وأفريقيا وأمريكا الجنوبية وقد يرد على ذلك بتبني دول عديدة محتوى اتفاقية بودابست ضمن قانونها الداخلي. ومن نقاط الضعف الأخرى عدم وجود آلية لإجبار أي دولة موقعة على الاتفاقية على تنفيذ التعاون، وإتاحة المجال لأية دولة موقعة عليها الرفض طلب المساعدة، لأسباب خاصة مثل وجود ضرر لاحق بعيادتها أو أمنها أو نظامها العام أو مصالحها الأساسية(٤٤). وتجدر الإشارة إلى أن الدول العربية لم توقع على اتفاقية بودابست، باستثناء المملكة المغربية والتي ليست ملزمة بها وفي هذا الإطار يجدر التركيز على آليات التعاون غير الرسمية بين الأجهزة المختصة بين الدول، باعتبار أن اتباع الإجراءات الرسمية في مجال التعاون القضاتي يتطلب وقتا طويلا، قد يؤدي إلى ضياع الأدلة المعلوماتية وقرار المجرمين وقد ظهرت في مؤتمرات كثيرة رغبة قوية للتعاون بين الدول. فعلى سبيل المثال، أوصى المشاركون في المؤتمر الإقليمي السادس للجمعية الدولية لأعضاء النيابة العامة الدول الشرق الأوسط وآسيا والمحيط الهادي، تحت عنوان "النيابات العامة في القرن ٢١"، الذي انعقد بدبي في عام ٢٠٠٩، بضرورة تعاون أعضاء(٤٥) النيابة العامة في جميع أنحاء العالم بصورة فاعلة لمكافحة العدد المتزايد من الجرائم السيبرانية، عن طريق الدعم والمساعدة القانونية المتبادلة، ونقل أفضل الممارسات، وتدريب النيابات العامة (٤٦). وأخيرا، يدخل ضمن مفهوم التعاون العمل بين دول المنطقة على تطوير آليات تبادل الخبرات والمعارف العلمية والتقنية والتجارب والحلول، عن طريق الزيارات المتبادلة والمؤتمرات الدورية وإنشاء قنوات اتصال دائمة، ويمكن أن يتم ذلك عن طريق توقيع بروتوكولات تعاون وتنسيق بين دول المنطقة العربية.

الخاتمة

أولا- النتائج :

١- يتضح جليا مما سبق على أهمية حماية الفضاء الإلكتروني لكل دولة وبما يحويه من شبكات سواء عن طريق الإجراءات المتخذة من الجانب التشريعى او من الجانب التقنى .

٢- أهمية التوعية المستمرة للأفراد وللموظفين على اساليب الإختراق وكذا تدريب القائمين على تنفيذ القانون بجميع مراحله على هذه الأساليب ويتم ذلك عبر

(ISSN: 2537 - 0758)

إطلاق دورات تدريبية تخصصية للعاملين في مجال السلامة المعلوماتية ومكافحة الجرائم السيبرانية لتمكينهم من القيام بمهامهم على أكمل وجه.

٣- وضع منهجية للاستجابة للحوادث السيبرانية، وبوجه خاص إنشاء مراكز للاستجابة السريعة لطوارئ الحاسوب.

ثانيا- التوصيات :

١- نهيب بالدول العربية التي لم تسن قوانين تحرم بها الجرائم الالكترونية بسرعة معالجة هذا القصور القانوني لإقامة العدل واحترام حقوق الإنسان.

٢- تعزيز التعاون بين أجهزة التحقيق الجنائي في الجرائم الالكترونية وتبادل المعلومات وتتبع البيانات حول الجريمة الالكترونية ومرتكبيها على المستويين الإقليمي والدولي.

٣- ويجب أيضا على كل دولة تطبيق مجموعة من الوسائل، يكون فيها إطار عمل للأمن والأمن السيبراني ولمكافحة الجرائم السيبرانية وهذه الوسائل هي تشريعية وتنظيمية وتوعوية وتثقيفية وتقنية وتعاونية فيما بين القطاع العام والقطاع الخاص في ذات الدولة.

٤- الإنضمام إلى الإتفاقيات الدولية ذات الصلة وخاصة إتفاقية بودابست .

هوامش ومراجع البحث:

(١) على حسين باكير المجال الخامس .الحروب الإلكترونية في القرن ال . 21 مركز الجزيرة للدراسات 12 يناير، 2011 .

(٢) صلاح حيدر (حروب الفضاء الإلكتروني دراسة فى مفهومها وخصائصها وسبل مواجهتها) جامعة الشرق الاوسط ٢٠٢٠ ص ٥٧ ـ ٥٨

(٣) المرجع السابق، ص ٥٨ ـ ٥٩

(٤) المرجع السابق، ص ٦٠ ،٦١

(٥) المرجع السابق، ص ٦٢.

(٦) المرجع السابق، ص ٦٣

(٧) المرجع السابق، ص٧ و١٦

(٨) حماية الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية (مركز الامارات للدراسات والبحوث الاستراتيجية) ص٨

(٩) حماية الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية (مركز الامارات للدراسات والبحوث الاستراتيجية) ص١٨

(١٠) المرجع السابق ص١٩-٢٠

(١١) المرجع السابق، ص ٢٤-٢٥

(١٢) المرجع السابق، ص ٣١-٣٢

(١٣) المرجع السابق، ص ٣١-٣٢

(١٤) أميرة عبد العظيم محمد عبد الجواد (المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام)قسم القانون العام /شعبة الشريعة والقانون /كلية الدراسات الإسلامية والعربية بنات القاهرة / جامعة الأزهر. ص ٥٢٣-٥٢٤

(15) ITU, Marco Gercke: Understanding Cybercrime: Phenomena Challenges and legal Response, September 2012. p.98

(16) Steven Titch: Four principles for effective cybersecurity law and policy, 25 April 2014, http://www.streetarg 2014/ 04/25/four principles for effective cybersecurity law and policy, p. 4.

(١٧) الأمان فى الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية : توصيات سياسية (اللجنة الاقتصادية والاجتماعية لغربى آسيا (الاسكوا) الامم المتحدة نيويورك ٢٠١٥ ص٥٠

(١٨) المرجع السابق، ص٥١

(19) Steven Titch: Four principles for effective cybersecurity law and policy, 25 April 2014, http://www.strect.org/ 2014/01/25/Four principles for effective cybersecurity law and policy, p. 2.

(20) Michael A. Vatis: The Council of Europe Convention on Cybercrime, http://cs.hrown.edu/courses oscil950 psources lec 16/Vatis.pdf, p. 6, 7.

(21) Micheal Barrett: Andy Steingrabl, Bill Smith, Combating Cybercrime: Principles, Policies and Programs, April 2011, https://www.paypal-media.com/assets/pdf/fact sheet/PayPal CombatingCybercrime WP 0411 vd.pdf, p. 7 to 25.

(٢٢) المرجع السابق، الأمان فى الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية ص ٥٢

(23) Challenges for international rules against cyber crime Fausto Pocar, New About that review : 1 hti://link.sprinCT.COmarticle/10.1007/B:CRIMI_00000_3755.255.10

(٢٤) المرجع السابق الأمان فى الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية ص ٥٣

(٢٥) المرجع السابق الأمان فى الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية ص ٥٣.

(26) University of Mississippi, School of Law, National Center for Justice and the Rule of law, Comhating cyber crime: essential tools and effective arganisational structures. A guide for policy makers and managers, http://www.alemiss.edu depis'ncirl/pdf/CyberCrimehooklet.pdf, p. 17.

(٢٧) المرجع السابق الأمان فى الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية ص ٥٤ .

(28) . University of Mississippi, School of Law, National Center for Justice and the Rule of law, Comhating cyber crime: essential tools and effective arganisational structures. A guide for policy makers and managers, http://www.olemiss.edu depls/ncirl/pdf/CyberCrimchooklet.pdf, p.31.

(٢٩) المرجع السابق الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية ص ٥٥

(30) Attorney General's Department, National Plan Government, Australian to Combat Cybercrime, http://www.gman CrimeAndCorruption

(ISSN: 2537 - 0758)

Cybercrime/Documents/National%20Plan20%20Combat%20Cybercrime.pdf.p . 16.

(31) United Nations Office on Drugs and Crime, UNODC Comprehensive study on cybercrime, draft, February 2013, p. 117.

(٣٢) المرجع السابق الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية ص ٥٦ .

(٣٣) United Nations Office on Drugs and Crime, UNODC Comprehensive . study on chercrime, draft, February 2013.p.234 167

(34) National French Police, Prospective analysis on trends on cybercrime from 2017 to 2020, http://www.mcafee.com resources/white papers/wptrends in chercrime 2011-2020.pdf, p. 39.

(٣٥) المرجع السابق الأمان فى الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية ص٥٨.

(36) Attorney Government, Australian http://www.agsuyau CrimeAndCorruption Cybercrime Documents National%20Plan201820Comhal%20Cybercrime.pdf. p. 15

(37) United Nations Office on Drugs and Crime, UNODC Comprehensive study on gyhercrime, draft, February 2013, p. 175

(38) Combat Cybercrime, to Plan National Department General's Attorney Government Australian National%20Plan%201620Comhat%20Cybercrime.pdf. p. 17, http://www.as.gov.au/CrimeAnd Corruption/Cybercrime/Document

(٣٩) المرجع السابق الأمان فى الفضاء السيبراني ومكافحة الجرائم السيبرانية فى المنطقة العربية ص٥٩.

(40) TENISA, Roadmap to provide more proactive and efficient Computer Timergency Response Team training, http://www.enisa.europa.eu/activities ort/support/exercise/roadmap to provide more proactive and efficient cert training,

(41) 2011 to 2020, 173 her crime from trends on (2) on analysis Police, Prospective French National bercrime 2011-2020.pdf. p. 12, 13. http://www.mafcs.com/sg/resources/white papers/wp_trends in

(٤٢) INISA مثل لجنة التجارة الفيدرالية في الولايات المتحدة الأمريكية وفي الاتحاد الأوروبي

(٤٣) المرجع السابق الأمان في الفضاء السيبراني ص٦١.

(٤٤) Michael A. Vatis, The Council of Europe Convention on Cybercrime, http://es.brown.edu/courses/cci950 p/ sources/lec16/Vatis.pdf, p. 14.

(٤٥) المرجع السابق الأمان فى الفضاء السيبراني ، ص ٦٣.

(٤٦) جريدة دار الخليج، محمد رباح، طارق زيد، الثلاثاء ١٧ تشرين الثاني/نوفمبر ٢٠٠٩ء ادعا إلى ضمان أمن وسلامة أضاء النيابة العامة مؤتمر التهابات العامة في القرن ٢١ يوصي بالتعاون لمكافحة الجريمة الإلكترونية.

http//www.micharnoonmulat.com9216.aspx?Action DisplayNews&type