مجلة العلوم الإنسانية العربية
المجلد (٣) العدد (٢)
الإصدار التاسع
٢٠٢٢ (٤٦-٢٨)

AHJ Arab Humanities Journal
Middle East Institution of scientific Publishing

الأردن بين الخدمات الرقمية والأمن السيبراني

صفاء محمد محمود الحياري

مديرية الدراسات، قسم الحاسوب، بلدية السلط الكبرى

نشر إلكترونياً بتاريخ: ١٦ مايو ٢٠٢٢م

الملخص

أسهم التطور التقني المتلاحق في أجهزة وأنظمة وشبكات الحاسوب و تحويل معظم المعاملات الى معاملات رقمية و ازدياد استخدام نظم المعلومات في معظم الميادين الاقتصادية والعلمية في انتشار جرائم نظم المعلومات وفي ابتداع أساليب جديدة ارتكاب الجرائم السيبرانية ،حيث | أنه لم يعد المجرم بحاجة الى أدوات إجرامية وأساليب غير تقليدية، و يكفي أن يكون الشخص ملماً باستعمال الحاسوب و واستعمال أنظمته لكي يقوم بارتكاب جريمة الكترونية من جرائم الفضاء السيبرانية، سواء كانت الوسائل المعلوماتية هي الأداة الجرمية أو كانت ضحية الفعل الاجرامي. مما يتطلب من كافة الهيئات العلمية و الأدبية أن تبذل جهودا علمية وعملية للوقاية من الجرائم السيبرانية . بالاضافة ان ذلك يستدعي من الجهات المختصة أن تكون على مستوى الأحداث في إعداد البرامج ، ووضع الخطط ، واستحداث الأنظمة والتشريعات التي تساعد على مواجهة نظم المعلومات وردع مقترفيها . إذ نقدم هذه الدراسة الهامة لنأمل أن يكون فيها ما يفيد لدعم جهود الوقاية من جرائم نظم المعلومات والجرائم الحاسوبية و التوعية بخصوص الجرائم السيبرانية بالاضافة لأهمية حماية و تطوير المعلومات الالكترونية في المؤسسات الحكومية والخاصة في الاردن .

Abstract

The successive technical development in computer devices, systems and networks, the conversion of most transactions into digital transactions, and the increase in the use of information systems in most economic and scientific fields have contributed to the spread of information systems

crimes and the invention of new methods of committing cyber-crimes, as the criminal no longer needs criminal tools and non-traditional methods. Rather, it is sufficient for a person to be familiar with the use of a computer and its systems in order to commit a cyber-crime m, whether the information means are the criminal tool or the victim of the criminal act. This requires all scientific and literary bodies to make scientific and practical efforts to prevent cybercrimes. It also calls for the competent authorities to be on the level of juveniles in preparing programs, setting plans, and introducing regulations and legislation that help confront information systems and deter their perpetrators. We present this important study in the hope that it will be useful to support efforts to prevent information system crimes and raise awareness about cybercrime and the importance of protecting and developing electronic information in government and private institutions in Jordan.

*** المقدمة**

في السنوات الاخيرة اعتمدت المؤسسات بشكل كبير في تسيير أعمالها على تقنية المعلومات وشكلت شبكات الاتصال وسطاً تنساب فيه البيانات وتسكن فيه خزائن المعلومات وبذلك تحتاج هذه الشبكات إلى حماية تصون سلامة محتوياتها وتضمن استمرارية عملها، ونظراً لكثرة الأخطار التي تهدد سلامة البيانات التي تنساب في الشبكات أو البيانات المحتضنة في خزائنها وتعدد الأخطار التي تهدد استقرار تلك الشبكات وأمنها كمحاولات الاختراق و الإصابة بالفيروسات والبرامج الضارة و لأغراض التعديل والعبث أو سرقة المعلومات أو التخريب ، تأتي أهمية الحماية على مدار الساعة لمكوِّنات شبكات المعلومات المادية والبرمجية بتثبيت أجهزة وبرامج الحماية في بوابات الشبكات المحلية وداخل تلك الشبكات، وإدارة تلك الأجهزة والبرمجيات من الزاوية الأمنية وسد الثغرات أولا بأول لتضييق فرص قراصنة المعلومات والمنافسين والأعداء من التمكن من اختراق أو سرقة أية بيانات من شبكات المعلومات.

إن اهمية المعلومات لا تخفى على أحد ، و كما هي حال المعلومات دائما فهي في خطر، لذا فانه ليس غريبا أن يصبح أمن المعلومات هاجس الجميع من مؤسسات و أفراد و منظمات . خصوصا وأن الجريمة تطورت تطورا أدى الى انتهاك حرمة المعلومات و تعريض أمنها للخطر الشديد ، و بالمقابل فإن هذا الخطر دفع الكثير إلى القلق على المعلومات و الحرص على حمايتها و تأمينها و ابعادها عن أيدي العابثين .

إن هذا البحث يتناول موضوع " الأمن السيبراني و حماية المعلومات الرقمية في الاردن" وهي الجرائم التي ترتكب على نظم المعلومات حيث يكون الحاسوب موضوعها أو وسيلتها .

ومن هنا توجهت العديد من الدول لوضع استراتيجية وطنية شاملة من أجل ضمان أمن المعلومات في الفضاء السيبرانية، فأمن المعلومات مهمة تعتبر ضمن مفهوم الأمن الوطني العام والشامل للدول مؤسسات وأفراد، وبدأت الكثير من الدول تدرك أن التغيرات المتسارعة في التكنولوجيا تؤدي الى تهديدات ليست بالسهلة لأمن الوطن والمواطن، ولذا لا بد من ضرورة العمل على ضمان أمن المعلومات من خلال خطوات مهمة للأمن السيبراني لحماية الأمن الوطني بمفهومه الشامل، فالأمن السيبراني يعتمد على مجموعة كبيرة من وسائل قانونية وتقنية لمقاومة الاستخدام الغير قانوني للشبكة العنكبوتية ومن أجل حماية نظم المعلومات ووسائل الاتصالات لحماية الوطن والمواطن والمؤسسات من أخطار الفضاء السيبراني،وذلك من خلال الإجابة على التساؤل الرئيس التالي: ما هو دور المؤسسات في تعزيز مفهوم الامن السيبراني؟

إن العمل على بناء جدران الحماية لمنع الهجمات الالكترونية وتقليل انتهاكات أمن المعلومات واختراقات الحسابات الحكومية والخاصة مسألة في غاية الأهمية، سواء كان ذلك بحسن نية و بسوء نية في بعض الاحوال ، فلا يمكن حماية الوطن والأمن الوطني بمفهومه الشمولي والاقتصاد الوطني والمؤسسات المصرفية ومعلومات الدولة بدون ذلك، وبدون زيادة الثقة بأنظمة المعلومات الوطنية، وإنشاء هيئات وطنية للأمن السيبراني، فالفضاء السيبراني هو عالم غير مادي ولكن لأن وسائل الاتصالات وخزن المعلومات تستخدمه من خلال شبكات الانترنت والشبكة العنكبوتية في العالم وفي الفضاء، فالمعلومات يتم تخزينها ولذا من الضروري حمايتها من الاختراق والسرقة والتجسس، ومن خلال انشاء الهيئات الوطنية للأمن السيبراني يكون بالإمكان من خلالها الاستجابة والمساعدة للمؤسسات والأفراد والقطاع الخاص والعام لمواجهة الحوادث مثل الاختراق والتجسس والقرصنة والتقليل من تأثيرها وزيادة الوعي والفهم للتهديدات التي تفرضها التطورات الهائلة في وسائل التواصل والاتصال في الفضاء السيبراني، وخصوصا أن انشاء الحكومات الالكترونية في تقدم مستمر وبتطور جيد في العديد من الدول ، وهذا يستدعي اهتماما أكبر في عمليات الحماية كون هذه الحكومات الإلكترونية تقدم الخدمات الالكترونية للمواطن وهذا يستدعي اداء جيد مشمول بالحماية حفاظا على أمن الأفراد والمؤسسات والدولة، وهذا يحتاج الى بناء على معايير لتطوير سياسات ومعايير أمن وحماية المعلومات.

ولأن انجاز هذه المهمة يحتاج للحصول على أفضل الوسائل التكنولوجية، من أجل مقاومة الاختراقات والتخريب، وضرورة الاطلاع على افضل الطرق لحماية الأمن الوطني بشموليته، وحماية البنية المعلوماتية لكل المؤسسات، بالإضافة لعمليات التدريب والتثقيف والتوعية، مما يعني تكاليف عالية لا يمكن لمؤسسات فردية أن تتحملها، فمن هنا كانت ضرورة انشاء الهيئات الوطنية للأمن السيبراني، فمن خلالها يمكن التوجه ايضا لصناعة وطنية تعزز مفهوم الحماية وتوفر بالتكاليف المتزايدة لحماية أمن الوطن والمواطن، اضافة لتشريع قوانين جديدة تحمي المؤسسات والأفراد من الجرائم الالكترونية.

وفي ذلك فقد عملت الأردن على اصدار تنظيم الجرائم السيبرانية ضمن تشريعات خاصة بها، فقد اصدرت قانونا خاصا بها، لمكافحة جرائم أنظمة المعلومات وتتناول هذه التشريعات تحديد الأفعال الجرمية المرتكبة عبر شبكة الانترنت والتي تعتبر جرائم معلوماتية كما تناولت العقوبة المقررة لكل منها وذلك لتحقيق الامن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للشبكات المعلوماتية وحماية المصلحة العامة والآداب والاخلاق العامة وحماية الاقتصاد الوطني.

ومن الملاحظ أن الدول أصبحت ترتب أمورها لمواجهة حروب المستقبل التي تعتمد على التخريب والتدمير والتطفل من خلال الفضاء السيبراني، وهذا أصبح جزءً من تكتيك واستراتيجيات الدول المتقدمة، لمواجهة هذه الحروب أو القيام بها، وأصبحت عمليات مقاومة هذه الحروب جزءً لا يتجزأ من استراتيجيات وخطط الدفاع لدول كثيرة، ومن هنا جاءت أهمية الدراسة.

*** أهمية الدراسة**

هذه الدراسة تؤمن مصدرًا هاماً للعاملين بمجال الأمن السيبراني حيث يستفاد منها بالتعرف على دور المؤسسات بحيث يتم إدراك حجم هذا الدور وتعزيزه في حال كون دوره ضعيفا وذلك لأن مواجهة المخاطر السيبرانية تتطلب بيئات تعليمية وذلك لإيجاد التعريف المناسب، الذي يحدد التصرفات التي يمكن ان تشكل مصادر حتمية للمخاطر السيبرانية، كالمسيئة والمؤذية، والتي يتبعها تحديد مسؤولية القائمين بها، كما يتبعها تحديد السلوك الواجب اتباعه، ما يعني عدم الالتزام به، امتناعا او اهمالا، ترتب مسؤولية هو الآخر. ويستدعي هذا الامر بداية، معرفة معنى الجريمة السيبرانية، التي تشكل الخطر الأساس الذي تجب مكافحته، ليتمكن اختصاصيو المعلومات، من تحديد الافعال التي لا بد من تلافي ارتكابها، وتلك التي لا بد من التبليغ عنها، كما انه يسمح للسلطات المعنية بالمكافحة، من التحرك على أساسها، بدءا من اصدار مذكرات التفتيش والتحري، وحتى الوصول الى المصادرة والحجز وجمع الادلة. كذلك، حيث إن تعريف الجريمة السيبرانية يسمح للسلطات القضائية، بتعيين النصوص الملائمة، وايجاد التفسيرات الصحيحة، ويسمح للسلطات السياسية، برسم خطوط التعاون مع البلدان الآخر. ونقول هذا، دون ان ننسى، الصعوبة التي تنشأ عن ان بعض الاعمال الجرمية، في بلد ما، يمكن الا تكون كذلك، في بلد آخر، ما يستدعي، معالجة خاصة، ومقاربة مشتركة، من البلدان المعنية، بالتعاون لمكافحة الجريمة السيبرانية، والحد من تأثيرها على الثقة والامن، في المجال السيبراني. فالخطوة الاولى نحو مكافحة الاعمال الجرمية والسيطرة عليها هو تعريف واضح لها.

*** أهداف الدراسة**

تهدف هذه الدراسة إلى معرفة وتعزيز دور المؤسسات في تعزيز مفهوم الامن السيبراني وحماية المعاملات الالكترونية، وحصر التدابير الاحتياطية اللازمة لتجنب تلك المخاطر والسيطرة عليها ومكافحتها من خلال هذه المؤسسات والدوائر والوزارات، وتقديم حلول لتعزيز مفهوم الامن السيبراني.

*** منهج الدراسة**

اعتمد الباحث في دراسته هذه على المنهج الموضوعي.

*** مصطلحات الدراسة**

تستخدم الدراسة مفاهيم ومصطلحات علمية فيما يلي تحديد موجز لها: -

الجريمة هي أي فعل ضارّ يأتيه المواطن ويكون لهذا الفعل أثر ضار على غيره من المواطنين ورد فيها نص قانوني يحدد أركانها ونموذج وقوعها وعقابها.

وتكون الجريمة الإلكترونية كل فعل ضار يأتيه المواطن عبر استعماله المواد الإلكترونية وهي فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية وهي الجريمة التي تلعب فيها بيانات الحاسب والبرامج المعلوماتية دوراً مهما وهي سلوك غير مشروع يرتكب باستخدام الحاسب.

الجريمة الالكترونية أيضاً هي نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه .

يمكن تعريف **جريمة الحاسوب**: هي الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسوب بعمل غير قانوني مثل سرقة النقود او البيانات أو تدميرها أو استخدام وقت الحاسوب بشكل غير قانوني، أو استخدام الحاسوب لإنجاز أغراض شخصية ليس لها علاقة بالعمل المكلف به الشخص.

الامن السيبراني: التعريف الاصطلاحي مأخوذة من كلمة (سيبرCyber) ، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي.

الأمن السيبراني (التعريف الاجرائي): أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها.

الشبكة : هي مجموعة من الحاسبات المتصلة مع بعضها بوسائط نقل بغرض المشاركة بمواردها .

شبكة الانترنت : عبارة عن مجموعة هائلة من الشبكات المتصلة فيما بينها و المنتشرة حول العالم تتيح المشاركة في المعلومات الرقمية و قواعد البيانات .

التحول الرقمي : هو عملية تطبيق التقنيات الرقمية لتجديد طريقة انجاز الاعمال وابداع قيمة جديدة وتقديمها .

الاعتداء :هو السب و القذف والتشهير و بث أفكار و أخبار من شأنها الاضرار الأدبي أو المعنوي بالشخص أو الجهه المقصودة .

*** الإطار النظري والدراسات السابقة**

من المعلوم أن الامن السيبراني قد وصل الى جميع المسائل الاقتصادية، والاجتماعية والسياسية، والانسانية، وذلك انطلاقا من تعريفه على انه قدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم، بأمان، من جهة أولى، ومن جهة ثانية من كونه يرتبط ارتباطا وثيقا بسلامة مصادر الثروة في العصر الحالي، ونعني بها، البيانات، والمعلومات، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكون حوله الانتاج، والابداع، والقدرة على المنافسة. من هنا لا بد من التوقف عند ابعاد الامن السيبراني، وان نستعرضها كما يلي:

*** الابعاد العسكرية**

من المعلوم، ان بدايات الانترنت، قد طورت بشكل أساسي في بيئة عسكرية، لتضاف اليها فيما بعد البيئة الاكاديمية، بما تمثل من أبحاث تخدم تطوير القدرات العسكرية، والانجازات العلمية، التي تدخل في تحديد تفوق بلد على آخر، حيث كان التنافس على أشده، بين الولايات المتحدة الاميركية والاتحاد السوفياتي، في مجال الوصول الى الفضاء الخارجي، وتطوير الاسلحة النووية. والامثلة كثيرة التي يمكن سوقها، في هذا المجال، لتوضيح خطورة الهجمات السيبرانية والابعاد العسكرية للأمن السيبراني، حيث يمكن ايراد ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وإيران، كمثال على بعض الهجمات والاختراقات، التي ترجمت ماديا، سواء باندلاع صراع مسلح لاحق، كذلك الذي وقع بين روسيا وجورجيا، أو بانقطاع الاتصال بالإنترنت في استونيا، بين الدولة والمواطنين، والتشويش على الادارات الحكومية.

كذلك نذكر هنا ما حدث في إيران من اختراقات أنظمة المنشآت النووية وتحقق امكانات التلاعب بها، مع ما يعنيه هذا من تعرض الامن القومي، للدولة المعنية، ومن تعريض السلام الدولي للاهتزاز. في هذا المجال ايضا، يمكن ايراد، الاختراق الذي حصل في البرازيل، والمملكة المتحدة، للبنية التحتية للطاقة، حيث انقطع التيار الكهربائي، ما طال بآثاره السلبية الملايين من الاشخاص، والمؤسسات والمصالح، وما يمكن ان يعني من وصول، الى موارد الطاقة كافة .نذكر هنا في هذا السياق ما حدث في ايلول 2007 عندما وجه خبراء اميركيون، خطابا مفتوحا الى الرئيس الاميركي، جورج بوش محذرين اياه، من خطر الهجمات السيبرانية على البنية التحتية الاميركية، التي تضم الى الدفاع، امدادات الطاقة الكهربائية، والمياه، والاتصالات السلكية واللاسلكية، ، والنقل، والانترنت والخدمات الصحية.

وهنا يمكن ان نتخيل النتائج الكارثية، التي يمكن ان تتجسد فيها تهديدات الأمن السيبراني الذي يوضح جدية الامر، وحاجتنا الى العمل معا، لتحقيق هذا الامن، لاسيما وان كلفة التقاعس، وانتظار وقوع الكارثة، يجعل نتائجها أكثر دراماتيكية.

*** الابعاد الاجتماعية**

تسمح طبيعة الانترنت المفتوحة لكل مواطن، عبر المدونات والشبكات الاجتماعية بشكل خاص، بان يعبر عن تطلعاته السياسية، وطموحاته الاجتماعية، وميوله الشرائية

حتى بأشكالها كافة. كذلك، تشكل مشاركة جميع شرائح المجتمع ومكوناته، وسيلة لإغناء هذا المجتمع، وتطويره، بما تتيحه من فرص للاطلاع على الافكار، والمعلومات، المختلفة، وبما تكونه من حاجة لدى الجميع، في الحفاظ على استقرار الفضاء السيبراني، والمجتمع الذي يرتكز اليه. والمعلوم، ان انفتاح المجتمعات على بعضها يؤسس لتبادل خبرات، وافكار، وتكون حاجات جديدة، وآفاق تعاون وتكامل.

يضاف الى هذا، ما يقدمه الانترنت، من امكانات وقدرات، للمجالات العلمية، والثقافية، والخدماتية، حيث تسمح بالوصول الى مناطق بعيدة، والى فئات محددة، ككبار السن، والمرضى، وغيرهم من ذوي الاحتياجات الخاصة. هذا بالإضافة الى الدور الذي يمكن ان تؤديه، في تبادل المعلومات، في اوقات الازمات الانسانية والكوارث، بحيث تتأمن المساعدات وتوزع بالسرعة المطلوبة. ولا تقف الابعاد الاجتماعية، عند حدود توفير اطمئنان المواطن الى حياته اليومية، والافادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها، الى صيانة القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات، اضافة الى العادات والتقاليد.

ولهذا فإن التشديد من قبل المنظمات والهيئات الدولية، على نشر ثقافة الامن في الفضاء السيبراني، وضرورة تعاون المجتمع، بكل مكوناته، وذلك لتحقيق الامن السيبراني وضمانه. فمما لا شك فيه، ان المخاطر السيبرانية، تطاول المجتمع كله، سواء، بسبب ارتكاز الخدمات الحيوية، كالطاقة، والنقل، والصحة، والاتصالات، وغيرها، على ما تقدمه تقنيات الاتصالات والمعلومات، من امكانات، او من خلال ما يضخ من محتوى في الفضاء السيبراني. فالمحتويات غير المشروعة، وغير المرغوب بها، ذات تأثير سلبي أكيد، على اخلاقيات مجتمع معين، وعلى ارتفاع نسبة الممارسات الجرمية نذكر منها: الاباحية، والترويج للاتجار بالممنوعات، والدعارة، والارهاب، والتجنيد لقضايا تمس الامن والسلام الدوليين. وعليه، لا بد من بناء مجتمع مسؤول ومدرك لمخاطر الفضاء السيبراني، قادر على التعامل بحد أدنى من قواعد السلامة، ومدرك للعواقب القانونية، التي يمكن ان تترتب على التصرفات، والتي تعرض سلامة الغير، وسلامة رؤوس الاموال للخطر.

*** الابعاد السياسية**

بشكل أساسي، تتمثل الابعاد السياسية للأمن السيبراني في حق الدولة في حماية نظامها السياسي، وكيانها، ومصالحها الاقتصادية، التي تعني، حق الدولة وواجبها في السعي الى تحقيق رفاه شعبها، في الوقت الذي تؤثر التقنيات، في موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان المواطن، ان يتحول الى لاعب أساسي، في اللعبة السياسية. كما انه بإمكانه الاطلاع، على خلفيات ومبررات القرارات السياسية، التي تتخذها حكومته، عبر الكم الهائل من المعلومات، التي يمكنه الوصول اليها، او التي يمكن ان توزع وتنشر على الانترنت، مع باقي الاجهزة التي توصل بها. بالمقابل، العاملون في الشأن السياسي، لا يتوانون عن الافادة مما تقدمه هذه التقنيات، حتى تصل الى أكبر شريحة ممكنة من المواطنين، والترويج لسياساتهم، في العالم. واضافة الى مدى

التأثير الذي يتركه هذا الامر، بغض النظر عن السياسات والمبادئ والمواقف التي يروج لها وصحتها. مثال ذلك فقد استخدم اوباما خلال حملته الانتخابية، الشبكات الاجتماعية بشكل كثيف. كما تركت التسريبات للوثائق الديبلوماسية السرية، عبر الويكيليكس، أثرا سلبيا على العلاقات الدولية، وعلى مصداقيتها.

*** الابعاد الاقتصادية**

ان التلازم واضح بين الامن السيبراني والاقتصاد. بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات، ايضا بالقيمة التي تمثلها البيانات والمعلومات المستخدمة والمخزنة، على كل المستويات. كذلك فإن تقنيات المعلومات والاتصالات تتيح تعزيز التنمية الاقتصادية للبلدان، من خلال افادتها، من فرص الاستخدام، التي تقدمها الشركات الدولية، وكبرى الشركات، التي تبحث عن ادارة كلفة انتاجها، بشروط أفضل. الا ان هذا يطرح مسائل مختلفة، منها ما يتعلق بحماية مقدم الخدمة، وبحماية المستهلك على الانترنت. اضافة الى ذلك دخول العالم، عصر المال الالكتروني، في بيئة تقنية متحركة، خصوصا بعد إطلاق خدمات المحفظة الالكترونية، حيث تتزايد استثمارات المصارف، والمؤسسات المالية، في مجال المال الرقمي. والشركات تتنافس على اصدار تطبيقات تسمح بطرق دفع آمنة، وتسمح بحفظ المال في المحفظة الالكترونية، وبالإيفاء ايضا من خلالها، وبإمكانية استخدامها كرصيد افتراضي. وقد وضعت بعض الدول تشريعات خاصة بهذا المال، وهذا الامر يمكن ان يثير صعوبات كثيرة، ويتطلب تشريعات، للحد من بعض الجرائم الاقتصادية والمالية الخطرة، والعابرة للحدود، مثل تبييض الاموال، والتهرب من الضريبة.

ويرى المسؤولون ان هناك رابط بين الامن والنمو الاقتصادي، بشكل واضح فالأمن السيبراني، يضمن ركون الجمهور، الى الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما انه يضمن الاقبال عليها، بما يترجم عمليا عن طريق تطويرا اقتصاد سليم. والدليل الاوضح، على هذه القيمة، هو استهداف هذه المعلومات، من خلال عمليات التجسس الصناعي والعسكري التقليدية، او من خلال الاعتداء على الملكية الفكرية. عدا عن التأثيرات المالية السلبية التي يتركها الاعتداء على نظم المعلومات، وتعطيلها، بالإضافة الى سرقة نتائج أبحاثا معلومات أخرى إلا ان الابعاد الاقتصادية، يمكن ان تقدر خسائر عدم استخدام تكنولوجيا المعلومات بمليارات الدولارات، كالذي حصل، نتيجة تفشي فيروس الحب، والذي كانت بداية انطلاقه من الفيليبين، في العام 2000.

*** الابعاد القانونية**

يرتب النشاط الفردي والمؤسساتي والحكومي نتائج قانونية في الفضاء السيبراني، وموجبات تستدعي ايجاد القواعد الخاصة، بحل النزاعات التي يمكن ان تنشأ عنها. لذا، لا بد من مراعاة عدد من التحولات التي رافقت ظهور مجتمع المعلومات. فقد اضيفت حقوق اخرى الى الحقوق الأساسية، والحريات الانسانية المعترف بها، في الدساتير، والتشريعات الدولية، مثل حق النفاذ الى الشبكة العالمية للمعلومات، بالإضافة الى توسع بعض المفاهيم، حتى شملت أساليب

الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، مثل الحق في انشاء المدونات الالكترونية، والحق في انشاء التجمعات على الانترنت، والحق في حماية ملكية البرامج المعلوماتية. كذلك ظهرت موجبات جديدة، ذات انعكاسات اقتصادية نذكر منها على سبيل المثال: موجب الاحتفاظ ببيانات الاتصالات، والابلاغ عن مخالفات وجرائم خاصة بالمحتوى. ويبقى المحور الاساس، في حماية الاشخاص الطبيعيين والمعنويين، على السواء، في ضرورة حماية البيانات، خصوصا الشخصية والحساسة منها، بالإضافة الى حماية الحق في الخصوصية.

نضيف الى هذا، ما يتوقع من تحولات في السياسات الخاصة بالقطاعات الصناعية والتجارية، مع ضرورة اعادة صياغة هذه القطاعات، بما ينسجم مع استخدام الشبكات الاجتماعية بشكلها الواسع، والمسائل القانونية التي يجب أن يتم تثار، على وذلك لحماية المستهلك، والخصوصية، والبيانات الشخصية، وحقوق العمال، والملكية الفكرية. فمن المؤكد بأن السنوات القادمة تشهد تصاعدا في أعداد الاعمال الجرمية، والممارسات غير القانونية، التي تمارس في فضاء المعلومات أو الفضاء السيبراني، ما يعني ازدياد عدد القضايا التي سترفع امام المحاكم، الامر الذي يستدعي، تهيئة واعداد البيئة التنظيمية والتشريعية، وايضا بناء قدرات هيئات المكافحة والحكم.

ولا شك بان النزاعات القانونية ستطال: الاعلان، الذي يرتكز الى اطياف مستخدمي الانترنت، انطلاقا من اهتماماتهم البحثية، او المواقع التي يزورونها، والاختراقات، والتسريبات للبيانات الشخصية، والمالية، سواء منها المقصودة او غير المقصودة، ومسؤوليات الجهة التي تملكها، او تديرها، والحق في تصحيح البيانات الشخصية، ومحوها، وتعديلها.

*** مستلزمات المواجهة**

ان العامل المحفز لتصاعد نسبة المخاطر هو ارتباط البنى التحتية الخاصة بتقنيات المعلومات والاتصالات، بالإضافة الى الاعتماد المتزايد عليها من قبل الدول والافراد والمؤسسات الامر الذي يفرض اتخاذ تدابير واجراءات، تضمن ادارة فاعلة للمخاطر التقنية وايضا السيبرانية، والتي تعتمد على منهجية تتناسب مع الابعاد الواسعة لهذا الارتباط، ما ينطبق على البلدان اجمع. فالبلدان النامية، مثلا، يجب ان تحرص على أمنها السيبيري، وذلك لحماية نفسها، وايضا دفعا لاستبعادها، عن المجال السيبراني، باعتبارها مصدرا للخطر.

لذلك، من هنا لا بد ان تنطلق الحلول في هذا المجال، بدءا من فهم الطبيعة الخاصة لتقنيات المعلومات والاتصالات، خصوصا الجزء الخاص بتجاوزها للحدود، وللمجتمعات، والانظمة، بالإضافة لطبيعة البنى التحتية نفسها، ما يعني الطبيعة غير الملموسة للبيانات، وامكانات تناقلها، واختراق الانظمة التي تحوي هذه البيانات. ويعني هذا، فهما مشتركا، للإمكانات التي تقدمها تقنيات المعلومات والاتصالات، بوجهيها السلبي والايجابي، وادراكا لضرورة ايجاد ارضية مشتركة، حتى يمكننا مواجهة تحديات بناء الثقة في مجتمع المعلومات، انطلاقا من تحقيق بيئة آمنة.

على صعيد آخر، فان الابعاد الخاصة بالأمن السيبراني تفرض ارساء قواعد الحماية، على فهم وتصور

شاملين واضحين، للمكونات التقنية وايضا للموارد البشرية، بحيث لا تسقط المخاطر التي يتسبب بها البشر، سواء اكانت مجرد اخطاء غير مقصودة، ام اعمالا جرمية. وقياسا عليه فإن المبادئ الاساسية، في بناء الامن الكلاسيكي هي: تحديد التهديدات والمخاطر، وضع خطة ورسم استراتيجية وبناء قدرات الدفاع، ايضا اعداد خطط مواجهة، واتخاذ خطط احترازية. وذلك، يستلزم بناء الامن السيبراني، من خلال اجراءات ردع حقيقية، يحكمها ويواكبها إطار تشريعي وتنظيمي، وهيكلية خاصة، وبناء قدرات، وآليات تحقيق، وملاحقة، ومحاكمة، الامر الذي يستدعي ادراج قواعد خاصة بمكافحة الجريمة السيبرانية، واعلان المسؤوليات المترتبة مدنياً، وجزائياً، ومهنياً.

*** الجريمة السيبرانية**

على ضوء ما تقدم، نجد بان المخاطر السيبرانية تصدر بشكل أساسي، عن اعمال قصدية، او غير قصدية، وتزيد خطورتها، إذا قابلها قلة وعي وإدراك لهذه المخاطر، بالإضافة الى اساليب وطرق الوقاية.

وعليه، فإن مواجهة المخاطر السيبرانية تتطلب ايجاد التعريف المناسب، الذي يحدد التصرفات التي يمكن ان تشكل مصادر حتمية للمخاطر السيبرانية، كتلك التي تسبب الاساءة والأذى، والتي يتبعها بالتالي، تحديد مسؤولية القائمين بها، وايضا تحديد السلوك الواجب اتباعه، ما يعني عدم الالتزام به، ام امتناعا او اهمالا، ترتب مسؤولية هو الآخر. ويستدعي هذا الامر، معرفة معنى الجريمة السيبرانية، التي تشكل الخطر الاساس الذي تجب مكافحته. والتعريف ضروري، حتى يتمكن اختصاصيو المعلومات، من تحديد الافعال حتى يتلافوا من ارتكابها، وتلك التي لا بد من التبليغ عنها، كما يسمح للسلطات المعنية بالمكافحة، من التحرك على أساسها، بدءا من اصدار مذكرات التفتيش والتحري، وصولا الى المصادرة والحجز وجمع الادلة. ايضا، يسمح تعريف الجريمة السيبرانية، للسلطات القضائية، بتعيين النصوص الملائمة، وايجاد التفسيرات الصحيحة، وللسلطات السياسية، برسم خطوط التعاون مع البلدان الآخر. ونقول هذا، من دون ان ننسى، الصعوبة التي تنشأ عن ان بعض الاعمال الجرمية، في بلد ما، قد لا تكون كذلك، في بلد آخر، الذي يستدعي، معالجة خاصة، ومقاربة مشتركة، من البلدان المعنية، بالتعاون من أجل مكافحة الجريمة السيبرانية، والحد من تأثيرها على الثقة والامن، في المجال السيبراني. فإن تعريف الاعمال الجرمية، هو الخطوة الاولى، لمكافحتها والسيطرة عليها.

ومن مبدأ" لا جريمة ولا عقاب دون نص" فإن العديد من البلدان، وضعت نصوص قانونية، خاصة بهذا النوع الجديد من الجرائم، والتي يمكن ان تشمل مروحة واسعة من الاعمال غير المشروعة أو الشرعية، خصوصا التي تستخدم اجهزة الكومبيوتر والشبكات كوسيلة لتنفيذ الجريمة، او التي تستخدمها كهدف لها، بدءا من عمليات اختراق الانظمة المعلوماتية وانظمة الاتصالات، حتى تصل الى الهجمات التي تعطل الخدمات. كذلك، فإن الجريمة السيبرانية تشمل فئة الجرائم التقليدية، التي تنفذ عبر المجال السيبراني. الا ان عدم وجود تعريف شامل للمخاطر والجريمة، اضافة الى تنوع التعريفات الوطنية، والطبيعة العالمية يجعل من الافضل، ان

ننطلق من التعريفات التي اعتمدها الهيئات والمنظمات الدولية المتخصصة، لهذا التعريف، بالرغم من كونها، تعريفات لا نهائية وغير محددة كفاية. ففي ورشة عمل متخصصة بالمسائل التي تثيرها الجرائم المتصلة بالشبكات، قسمت هذه الجرائم، الى مجموعتين الاولى، حسب المدلول الاضيق، الذي يشير الى كل تصرف غير شرعي موجه بالوسائل الالكترونية، نحو أمن انظمة المعلومات، والبيانات التي تحويها، بينما المجموعة الثانية ضمنت حسب المدلول الاوسع، كل تصرف غير شرعي يرتكب من خلال الانظمة المعلوماتية، او بطريقة متصلة بها، ويشمل جرائم غير المشروعة كالحيازة او عرض الخدمات وتوزيع المعلومات، بواسطة انظمة معلومات او شبكات معلومات.

من جهتها فإن الاتفاقية الاوروبية لمكافحة الجريمة السيبرانية عمدت الى ايراد ما تعتبره اعمالا غير شرعية، تحت عناوين مثل الجرائم ضد سرية الانظمة والبيانات، وسلامتها، وتوفرها، والجرائم المتصلة بالأجهزة، والجرائم الخاصة بالمحتوى، والجرائم الخاصة بالملكية الفكرية والحقوق المجاورة أو الاعتداء عليها.

*** المحتوى غير المشروع**

على الرغم من ان الارتباط وثيق بين نشر المحتوى غير المشروع والجرائم الالكترونية، فإننا نرى بان إبرازه ضرورة كنقطة مستقلة. وذلك ان ما هو غير مشروع على المستوى التقليدي، يبقى غير مشروع في الفضاء السيبراني لذا لا بد من النظر الى المحتوى غير المشروع، واحد من المخاطر التي ترتبط مباشرة بأمن المجتمع والدولة، على حد سواء، ما جعل تنظيم وتشريع ما يمكن تداوله من معلومات، بواسطة اي من وسائل النشر، مسألة لصيقة بمهمات الدولة الاساسية في حماية المجتمع، وحماية النظام القائم فيه. وبما ان مهمات الدولة لم تتغير، يبقى المحتوى غير المشروع، على الشبكة العالمية للمعلومات، وعلى كافة وسائل النشر الالكترونية، في طليعة المسائل، التي يجب تأطيرها وتنظيمها. مما يدعونا الى التوقف على المحتوى غير المشروع على أكثر من مستوى، وهنا، نكتفي بالمستوى الاعلامي، ومستوى حماية الاطفال والشباب والثقافة التي ترتبط بهم جميعا. فممارسة النشر والاعلام الالكتروني، عبر المواقع الاعلامية الرسمية، او عبر المدونات، والصفحات الشخصية على المواقع الاجتماعية، حولت مواقع كثيرة، على الشبكة العالمية للمعلومات، الى منابر اعلامية، تطرح مختلف الآراء وتناقش التوجهات والسياسات المختلفة.

وفي نفس السياق يتم طرح بث بعض أنواع المعلومات مثل الصور، والخدمات على الانترنت، مشاكل خاصة مثل حماية الشباب والاطفال، من المحتوى غير المشروع أو الضار. ونذكر على سبيل المثال: عروض خدمات الدعارة، وبيع المشروبات الروحية، والاستشارات الطبية غير المشروعة، والمواد الطبية الممنوعة، والفلك، والميسر، والخطابات التي تحث على العنصرية والكراهية، والمواقع الخاصة ببدع ومعتقدات تحرض على الانتحار أو على القتل، هذا عدا، عن المواد الاباحية التي تستخدم الاطفال هدف وتستغلهم. اضافة الى ما تقدم، فإن غياب تعريف عالمي، أو حتى اقليمي، للمحتوى غير المشروع، حسب فعالية المكافحة

في الفضاء السيبراني، فإننا ندرك، خطر هذا النقص وانعكاساته العملية. وعليه، فإن العمل، الى الوصول وايجاد أرضية مشتركة، ومبادئ عملية تمكن من مكافحة المحتوى غير المشروع. وهنا فان التقنيات يمكن أن تلعب دورا أساسيا، خصوصا من خلال تطوير برامج الترشيح والفلترة، بناء على تعليمات خاصة ومحددة لهذا المحتوى غير المشروع، تمنع وصوله، على الاقل الى الاوطان التي تعتبره كذلك. وتبدو الحاجة ملحة، لمعالجة المدلول الواسع والمتزايد، للمحتوى غير المشروع، حتى في بعض التشريعات الوطنية، والتي يمكن للسلطة أن تتصرف بالتفسير والقياس، الى درجة عالية، ما يشير الى امكانات واسعة للاعتداء على حرية التعبير والحريات المرتبطة بها، كحق الخصوصية، والتعبير عن الرأي.

*** تحديث نماذج العمل**

نضيف الى التحديات التقليدية، التي طرحها دخول تقنيات المعلومات والاتصالات، منذ بداياته، على الآليات التقليدية، للعمل والتحرك، داخل المجتمع، كقواعد اقراره، وتوقيت اصداره، وحدود تطبيقه، تبرز تحديات جديدة، تستدعي حركة خاصة، يمكن ان تطال، تحديث نماذج وآليات العمل.

فلتقنية المعلومات والاتصالات تغيرات سريعة، وحركة دائمة التغيير، وللفضاء السيبراني، سمة عالمية، وطبيعة عالية التقنية، الامر الذي لا يتناسب مع حركة القانون البطيئة، ولا مع الإطار السيادي، الذي يبنى على اساسه. من هنا، فانه يجب على القانونيين الرد على تحديات اقلها ايجاد نماذج تشريعية جديدة، وخطة عمل، وهيئات، تستطيع التعامل مع متطلبات السلامة والامن. وفي أقرب وقت، قواعد جديدة، للتعامل مع مسائل الحوسبة السحابية، والخدمات التي تقدمها شركات خارجية واجنبية، غريبة عن المؤسسات والادارات، مالكة الانظمة المعلوماتية، في القطاعين العام والخاص.

في هذا السياق، فانه يتم طرح مسائل عديدة، منها: اعادة النظر في آليات اصدار واقرار التشريع، والهيئات المخولة بإصدار واقتراح هذه التشريعات واصدار القوانين والانظمة، واعداد برامج وتأهيل وتدريب السلطات المعنية بالمكافحة والتحقيق، اضافة الى استحداث ادارات خاصة، تختص بالمواضيع الاجرائية والادارية الخاصة بقطاع المعلومات والاتصالات، ومعالجة المعلومات. وهذه بعض الافكار في هذا المجال، مثل:-

اولا: الالتفات نحو اقرار القواعد التي تحكم تقنيات الاتصالات والمعلومات، من خلال مراسيم بدلا من القوانين، وذلك لأنها أكثر قربا من الواقع العملي، ولا تتطلب وقتا طويلا، لوضعها موضع التنفيذ.

ثانيا: ايجاد هيئات تشريعية منتخبة، ذات صلاحيات تماثل صلاحيات المجالس النيابية، تلتزم التشريع في مجال الاتصالات والمعلومات، مع مراعاة التداخلات التي يمكن ان تطرأ مع القوانين. فتقنية المعلومات التي اقتحمت جميع مجالات نشاطات الانسان، تحولت الى قطاع تجاري، وخدماتي ايضا، ولا بد لتنظيمها وتنظيم القواعد القانونية الخاصة بها، ان تتأثر بالقطاعات التي دخلتها. ونورد على سبيل المثال، ما يفرض من اجراءات ومواصفات، على البرامج المعلوماتية الخاصة بالأسواق المالية، بحيث تضمن الشفافية، والاطلاع على

المعلومات، ومصداقيتها، كما القوة الثبوتية للتقارير الصادرة عنها.

ثالثا: تشكيل هيئات متخصصة، تتابع بشكل خاص عمليات التشريع والتنظيم في مجال الامن السيبراني، من المجالس النيابية، ولكن شرط التزامها بآلية عمل تؤمن سرعة اقرار القوانين، وتحديثها، في الوقت المناسب.

رابعا: خلق اصول اجرائية خاصة بالتبليغ والانذار، عن الاختراقات وتسرب المعلومات

في ذات الوقت، فإن القضاء مدعوا، للإجابة عن مسائل تقليدية، وتطبيق قواعد كلاسيكية معروفة، على الاوضاع الجديدة، كتحديد صاحب المصلحة في الادعاء في حالات تسرب البيانات، وتقرير ما إذا كان خطر سرقة الهوية بارتفاع، يعطي الشخص الحق في اللجوء الى القضاء. وما هي امكانية الادعاء على الجهة التي تسربت البيانات من انظمتها، في حال عدم وجود رابطة كالعقود، وهل يمكن عندها ان تتم الملاحقة، بسبب التخلف، عن اعتماد معايير الحماية الضرورية. كذلك، هل يمكن اعتبار عدم الالتزام بمعايير الحماية، خرقا لقانون حماية المستهلك، ومستخدم الشبكة، الى ما هنالك من مسائل تتعلق بالضرر، الذي على اساسه يمكن المطالبة بتعويض، وكيفية تحديد هذا التعويض.

*** تعزيز الامن عن طريق التعاون**

في هذا المجال، يجب ايجاد الإطار التشريعي والتنظيمي الحاضن، الذي يشجع مبادرات التعاون، وذلك لان استمرارية عمل تقنيات المعلومات والاتصالات، والانترنت، بالإضافة الى استقرار الفضاء السيبراني، يستدعيان سياسات لمعالجة الثغرات الامنية، ومن اجل مواجهة الاخطار والحد من آثار الاعمال الجرمية. وبالتالي، لا بد من دعم الجهود الى وضع مقاييس ومعايير دولية، كما لا بد من دعم اقرار الاطر القانونية والتنظيمية، والاستفادة من أفضل الممارسات والتجارب الناجحة، التي تعزز الثقة في الفضاء السيبراني، وتؤمن بيئة تدعمه، وذلك لنمو النشاط الاقتصادي، والاجتماعي، في الفضاء السيبراني. وفي نفس الإطار، لا بد من الابتعاد عن السياسات، التي تتعارض وطبيعة عمل الانترنت المفتوحة، وامكاناتها التي تشكل أرضية للإبداع، والنمو الاقتصادي والاجتماعي، لان لا تتحول هذه السياسات، الى أدوات تسبب في اعاقة الانسياب الحر للمعلومات، والوصول اليها، تحت ذريعة تحقيق الامن والحماية.

وهنا لا بد لسياسات الامن أن تعزز المبادرات الفردية، والجماعية، العاملة على تحقيق الامن والحماية. فان نجاح خطط الحماية والامن السيبراني، يفرض ترابطا وتكاملا، بين استراتيجيات الامن وسياساته، كما انه يفترض، امكانية وصول الجمهور اليها، على المستويات، الإقليمية والعالمية والوطنية ايضا. كذلك، هنالك حاجة لمشاركة الجميع، في وضع الحلول، بحيث تأتي هذه الاخيرة، ناجعة، ومؤسسة لتفاهم اجتماعي وسياسي، بشكل يعزز فرص نجاحها وفعاليتها. كما انه، يجب لمتخذي القرار، ان يأخذوا مقترحات القطاعات المهنية، والاختصاصيين، والمجتمع المدني، وغيرهم، بعين الاعتبار، عند صياغة التشريعات، ووضع الاطر التنظيمية.

*** البنية الادارية وتطويرها**

ان الثقة في الفضاء السيبراني، ترتبط بقدرة الاجهزة المعنية، على ضبط الامور، كما ترتبط، بوضوح المسؤوليات، والمرجعيات المعنية، بإقرار الحقوق وحمايتها، وايضا بالقدرة على ردع، وملاحقة لكل عمل جرمي، او تصرف يهدد استقرار المعاملات، والفضاء السيبراني. وتتطلب المكافحة الفاعلة، اجهزة متخصصة، وعناصر تتميز بكفاءتها وقدرتها على الاحاطة، بجوانب كيفية ادارة انظمة المعلومات، وطرق معالجة البيانات، والحقوق المتصلة بها. اضافة الى ذلك، ضرورة وجود مرجعية قانونية، تشرف على توثيق الحقوق، وارساء قواعد متينة تعزز الثقة في العاملين في مجال معالجة المعلومات، والانظمة المتصلة بها، والحقوق الناشئة عنها، في سجلات خاصة، ذات قيود موثوقة.

من هنا، يجب اعطاء عملية بناء قدرات الاجهزة الامنية، ودوائر تنفيذ القانون، اهمية خاصة. كما لا بد من ايجاد اجهزة ادارية متخصصة، تتولى اعطاء شهادات خاصة للأشخاص الذين يتولون مراقبة المعلومات، وحفظها، ومعالجتها، وتسجيلهم في سجلات خاصة، وتلزمهم بقواعد وقوانين لحماية المعلومات والانظمة.

فإن تشجيع الاستثمار، والابداع، والاختراع، في اسواق العمل المتصلة بوسائل الاتصالات، يرتكز على تحديد الحقوق والموجبات بشكل واضح، كما يرتكز على آليات محددة، لحماية الحقوق الناتجة عن هذا النشاط، كما كان عليه الحال، عند اقرار قوانين الملكية الفكرية، وحقوق المؤلف، والعلامات التجارية، والسجلات التي تثبت ملكيتها، في عصر ما قبل الانترنت. وفي ذلك أيضا، للحفاظ على حقوق المستخدمين، لاسيما حقهم في تطبيق القوانين المرعية الاجراء.

*** حماية الانسياب العالمي الحر للمعلومات وتعزيزها**

يرتكز اقتصاد الانترنت، كما نموها، بشكل اساسي، على الانسياب الحر للمعلومات. وإذا كانت الدول المختلفة، مدعوة الى وضع سياسات تعزز هذا الانسياب، وتشجعه، وتدعمه، وفي المقابل فإنها مدعوة ايضا، لتامين الإطار القانوني الذي يوفر حماية الحق في الخصوصية، والبيانات الشخصية، والحريات الفردية، وبعض الفئات العمرية، مثل الاطفال والشباب، والملكية الفكرية. ومن هنا، ضرورة الالتفات الى الامن السيبراني، وارساء قواعد ثابتة له. ويتصل انسياب المعلومات، بالطبيعة المفتوحة للإنترنت، التي تتكئ بدورها، على مقاييس ومعايير تقنية عالمية. وترد في هذا الإطار ايضا، سياسات المنافسة، والاسواق المفتوحة، والتنوع، والخدمات العابرة للحدود، التي تؤمن خدمات، بكلفة معقولة، تسهم في اتاحة الانترنت للجميع.

*** الالتزام بقواعد أخلاقية**

يمكن للحكومة، ان تقر قواعد قانونية، تقوم بدعم وتشجع الالتزام بأخلاقيات وقواعد سلوك معينة، يرافق ذلك آليات محاسبة ومسؤولية خاصة، كما هو معمول به، في إطار تنظيم بعض المهن، كالتجارة، والمحاماة، والصحافة، والطب والمصارف، وغيرها. حيث يمكن لهذه القواعد، ان تساهم في، مكافحة التصرفات اللامشروعة، ولا اخلاقية، كالغش والخداع، والممارسات غير المهنية، ويمكن، ان تدعم الحريات

العامة، وتحصن الحقوق المعترف بها، في القوانين التي تراعي الاجراء.

*** الحفاظ على الخصوصية**

يعتبر الحفاظ على الخصوصية أحد أساسيات تعزيز الثقة، في الفضاء السيبراني، والافادة من طاقات تقنيات المعلومات والاتصالات، على المستويات جميعها: الاجتماعية، والاقتصادية، والثقافية. فالتحديات الحالية، التي تطرحها وسائل معالجة البيانات وجمعها، واستخدامها، واستثمارها، لا بد وان تكون لها انعكاسات سلبية، على استخدام الانترنت، وعلى التقنيات المتصلة بها، سواء التجارية، او الاجتماعية، او الحكومية. وهنا لا بد للأطر التشريعية والتنظيمية، من ان تمكن المستخدمين، من فهم ما يجري من ممارسات تطال بياناتهم الشخصية، والمعلومات التي يضعونها على الانترنت. كما لا بد من تمكين المستخدمين، من ممارسة حقوقهم، في ادارتها، بالطريقة التي تطمئنهم الى امكانية الحفاظ على خصوصيتهم، وعلى حقوقهم الفكرية، والصناعية والادبية. وهنا في هذا المجال، يمكن للتشريعات، ان تسترشد بالقواعد الدولية، والمبادئ التي سبق اقرارها، عالميا، كجزء اساسي للمحافظة، على نمو واستقرار، الفضاء السيبراني.

*** الامن السيبراني في المملكة الاردنية الهاشمية**

للمملكة جهود كبيرة لتعزيز الأمن السيبراني فقد أصدرت «قانونا مؤقتا لسنة (2010) لمكافحة جرائم أنظمة المعلومات» في البلاد، التي تضع أدنى حد من المعايير الواجب الالتزام بتطبيقها في مختلف الجهات الوطنية، وذلك لتقليل مخاطر التهديدات السيبرانية، مما يسهم في تعزيز أمن المملكة السيبراني، وأمن مصالحها الحيوية والاقتصادية ومقدراتها.

وتناولت هذه التشريعات تحديد الأفعال الجرمية المرتكبة عبر شبكة الانترنت والتي تعتبر جرائم معلوماتية كما تناولت العقوبات لكل منها.

وكما يهدف القانون إلى تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للشبكات والحاسبات الالية وحماية المصلحة العامة والآداب والاخلاق العامة وحماية الاقتصاد الوطني.

كما يحدد الأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني، لحماية الشبكات والأنظمة والبيانات الإلكترونية، وتعمم هذه على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها، حيث إن هذا الاختصاص لا يخلي أي جهة عامة أو خاصة أو غيرهما من مسؤوليتها تجاه أمنها السيبراني بشكل لا يتعارض مع اختصاصات ومهام الهيئة الواردة في تنظيمها.

كما يتضمن هذا القانون انه على جميع الجهات الحكومية أن ترفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، وأن تلتزم بسياسات وأطر ومعايير وضوابط وإرشادات تتعلق بهذا الشبن .

وحيث ان تطبيق هذه الضوابط إلزامي للجهات الحكومية، والجهات والشركات التابعة لها، إضافة إلى جهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها. وتشجع الهيئة الجهات الأخرى في الاردن على الاستفادة من هذه الضوابط لتطبيق أفضل

الممارسات في كل ما يتعلق بتحسين الأمن السيبراني وتطويره داخل تلك الجهات.

وترتكز الضوابط التي تم اعتمادها على مكونات أساسية تتمحور حول حوكمة وتعزيز وصمود الأمن السيبراني، وإلى الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، بالإضافة الى أنظمة التحكم الصناعي.

*** الدراسات السابقة**

أولاً: الدراسات العربية

أجرى سليمان مهجع العتري دراسة حول جرائم نظم المعلومات وتوصلت الدراسة إلى أن حجم استخدام منفذ شبكة الانترنت وبرامج الاختراق الموجودة بها (4.25%) من مؤسسات عينة الدراسة. وتوصلت الدراسة أيضاً إلى أن برامج الحماية تعد وسيلة ضبط وتحقيق هامة بشكل دائم، وتساعد بما نسبته (94.2%) في تحديد نوع الجريمة، وما نسبته (95.1%) في تحديد توقيت ارتكاب الجريمة. وكشفت الدراسة عن أنه بالإمكان الاعتماد على عنوان (IP)بما نسبته (94.2%) وعلى برامج الحماية (91.4%) ووسائل تتبع المخترقين (74.9%). وتُبرز دراسة (العتري) أهمية وسائل الحماية في ضبط الجريمة الإلكترونية وذلك يتوافق مع هذه الدراسة في موضوع حماية الشبكات من المخاطر حيث أكدت على ضرورة تركيب برامج وأجهزة الحماية وإعدادها الإعداد المناسب والقيام بالتحديث المستمر لتقوم بصد جميع الهجمات وتسجيلها من خلال تفعيل خصائص تسجيل الأحداث وتسجيلها.

أجرى عبد الله بن محمد ناصر السحيباني دراسة بعنوان ''كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات''، وقد تناول تصميم برامج شبكة الاتصال والبرامج التطبيقية في المصارف. وأوصى (السحيباني) بضرورة قيام المصارف التجارية بزيادة التركيز على استخدام الرقم السري لدخول المباني وغرف الحاسب الآلي، وإشعار العاملين بوجود مراقبة مستمرة عليهم وصيانة أجهزة الحاسب الآلي داخل المصرف، وإجراء تجارب لاختبار طرق الاستجابة عند حدوث طارئ أو كارثة، وضرورة إصدار سياسات لأمن المعلومات، وضرورة توظيف متخصصين في أمن المعلومات. وتضيف هذه الدراسة على دراسة السحيباني تفصيل الإعدادات التشغيلية لأجهزة الحماية وتتفق معها في جميع ما ورد فيها مع اختلاف عينة الدراسة.

ثانياً: الدراسات الأجنبية

أجرى شيخ فاروق عمارة دراسة بعنوان " The Control of Firewalls using Active Networks"حول ضبط جدران الحماية باستخدام الشبكات النشطة تتمحور حول مشكلة تغيير إعدادات جدران الحماية المبنية على تصفية حزم البيانات بوضع برامج صغيرة مسبقة التعريف داخل تلك الأجهزة التي تمكِّن من تعديل أو إعادة توجيه حزم البيانات بفتح أو إغلاق المنافذ تبعاً لمحتوى الحزم باستخدام تقنيات الشبكة النشطة (Active Network).ومن توصياته التوجه نحو نموذج عام لبرمجة الشبكة يتمتع بخصائص ذكية أهمها: خاصية التنقل، وخاصية الحماية، وخاصية الفعالية. وتختلف هذه الدراسة عن

دراسة (عمارة) بتناولها الأخطار المحتملة على الشبكات وتدابير تجنبها وضمنت جدران الحماية كواحد من أهم تدابير الوقاية. ((Emarah,2007 .

أجرى نور بك باشا إدريس وبحراني دهران شانموجان، دراسة بعنوان "Hybrid Intelligent Intrusion Detection" حول نظام هجين للكشف الذكي عن التجسس على شبكات الحاسب، وقد طرح الباحثان مشكلة عدم كفاية نظام كشف التجسس (IDS) لمنع التجسس على شبكات الحاسب الآلي كونها محدودة الإمكانات وتتركز قدرتها على المراقبة وتحتاج للتحديث اليومي لظهور برمجيات تجسس يومياً، ومن أهم توصيات دراستهما: ضرورة استخدام النظام الهجين واستخدام جهاز عالي الأداء من حيث المعالجة. وتتوافق دراسة إدريس مع ما ذكره الباحثان في دراستهما هذه في أهمية جدران الحماية الذكية المعروفة بالاختصار (UTM) وضرورة استخدامها على بوابات شبكات الحاسب الآلي، واختلفت دراسة إدريس عن هذه الدراسة في اقتصارها على جدران الحماية وعدم تطرقها إلى نواحي الحماية الأخرى التي غطتها هذه الدراسة من منظور الحماية من المخاطر المحتملة (Idris and Shanmugam : 2007) .

اجرت دينيتا ماهونو (Dieta mhono 2017) دراسة هدفت الى تصميم برنامج لزيادة الوعي لدى طلاب جامعة تالين لتكنولوجيا المعلومات في السنة الأولى من غير تخصص تكنولوجيا المعلومات حيث استخدمت عينة من 17 طالبة حيث حقق البرنامج نجاحا في زيادة الوعي لدى طلاب جامعة تالين في تكنولوجيا المعلومات

*** النتائج**

أظهرت النتائج ان للمؤسسات دور كبير في تعزيز مفهوم الامن السيبراني، واظهرت انه ولا بد من ايجاد الاطار التشريعي والتنظيمي التربوي المؤيد لتوضيح مخاطر الامن السيبراني على المجتمع ، حيث أن استمرارية عمل تقنيات المعلومات والاتصالات، وفي مقدمها الانترنت، وان استقرار الفضاء السيبراني، يستدعيان سياسات لمعالجة الثغرات الامنية، أيضا انه لا بد من دعم الجهود التربوية والتعليمية الآيلة الى وضع مناهج توعوية لأهمية الامن السيبراني ، كما لا بد من دعم اقرار الاطر القانونية والتنظيمية، والافادة من أفضل الممارسات والتجارب الناجحة، التي تعزز الثقة في الفضاء السيبراني، وتؤمن بيئة داعمة، لنمو النشاط الاقتصادي، والاجتماعي، والتربوي في الفضاء السيبراني.

كما وأن المعلمين وأساتذة الجامعات يؤيدون ان ترتبط الثقة في الفضاء السيبراني، بقدرة الاجهزة المعنية، على ضبط الامور، كما ترتبط، بوضوح المسؤوليات، والمرجعيات المعنية، بإقرار الحقوق وحمايتها، وبالقدرة على الردع، والملاحقة لكل عمل جرمي، او تصرف يعرض استقرار المعاملات، والفضاء السيبراني. وتتطلب المكافحة الفاعلة، اجهزة متخصصة، وعناصر تتميز بالكفاءة، والقدرة على الاحاطة، بجوانب كيفية ادارة انظمة المعلومات، وطرق معالجة البيانات، والحقوق المتصلة بها. يضاف الى ذلك، ضرورة وجود مرجعية، تشرف على توثيق الحقوق، وارساء قواعد

متينة للثقة في العاملين في مجال معالجة المعلومات، والانظمة المتصلة بها، كما الحقوق الناشئة عنها، في سجلات خاصة، ذات قيود موثوقة.

*** المراجع**

أولاً– المراجع العربية

سورة الأنبياء الايه (47).

الدكتور محمد علي قطب ،الجرائم المعلوماتية و طرق مواجهتها ، عمان : وزارة الداخلية ،الاكاديمية الملكية للشرطة

د. عبد الله عبد العزيز اليوسف، (2004)، أساليب تطوير البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، الرياض، جامعة نايف العربية للعلوم الأمنية.

محمد حجازي، (2005): جرائم الحاسبات والانترنت (الجرائم المعلوماتية)، مصر: عضو مجلس ادارة المركز المصري للملكية الفكرية.

م. زكريا أحمد عمار، (1429)، الحلقة العلمية الدليل الرقمي والتحقيق في الجرائم الالكترونية: جامعة نايف العربية للعلوم الامنية.

آبادي، الفيروز، (1987): القاموس المحيط، بيروت: مؤسسة الرسالة، ص1219

البشري، محمد أمين (2004): التحقيق في الجرائم المستحدثة، الرياض: جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث.

السحيباني، عبد الله (1996): كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

شمدين، عفاف (2003): الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات، دمشق.

الشهري، فايز بن عبد الله (2001): استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي: دراسة وصفية على عينة من المواقع الأمنية العربية على شبكة الإنترنت، مجلة البحوث الأمنية، الرياض: كلية الملك فهد الأمنية، مركز الدراسات.

العتزي، سليمان (2003): وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

النقروز، على (2017) جرائم نظم المعلومات، دار السناء للنشر، الاردن، عمان

ثانياً– المراجع الأجنبية

Emarah, S. (2007) : The Control of Firewalls using Active Networks, Information Technology and national security Conference, Riyadh.

Brenton, C& Hunt, C. (2003) Mastering – Network security, SYBEX Inc. US.

Cisco System, Inc. Cisco Networking Academy Program: First – Year

Companion Guide , Cico Press, Indianapolice, (USA, 2001).

Idris, N & Shanmugam, B (2007): Hybrid Intelligent Intrusion Detection System, Information Technology and national security Conference, Riyadh.