عنــوان المداخلـة: آليات تحقيق الأمن السيبراني في ظل تحديات التحول الرقمي

1- د. يوسفي علاء الدين، المركز الجامعي بريكة، الجزائر

alaeddine.youcefi@cu-barika.dz

2- د. عباس ميدون، جامعة باتنة 1، الجزائر

abbes-h@hotmail.fr

الملخــص:

لقد أصبح الاهتمام بتحقيق الأمن السيبراني أولوية كل دولة من دول العالم لما له من أهمية في الحفاظ على المعلومات و البيانات من السرقة و القرصنة و التصدي لمختلف التهديدات الالكترونية كالتجسس و الإرهاب الالكتروني .و لتحقيق الأمن السبيراني ينبغي اتباع آليات و أساليب مختلفة تقنية و تعليمية و إعلامية و تشريعية كاستخدام تقنيات و برامج حماية متقدمة للبريد الالكتروني و للحسابات الرسمية، مضادة للفيروسات قادرة على التصدي للهجمات الالكترونية و إدراج أنظمة مكافحة جرائم الفضاء السيبيراني ضمن المناهج التعليمية لكافة المراحل التعليمية، لتعزيز ثقافة الأمن الرقمي، وسن التشريعات الدقيقة الشاملة التي تناسب مقاومة الهجمات السيبرانية من خلال صياغة قوانين تنظم و تواكب التقدم التكنولوجي، والتعاون المستمر بين الأفراد والأجهزة الأمنية لكل دولة و كذلك التعاون بين الدول لرصد وتتبع عمليات الاختراق و القرصنة المعلوماتية .

كلمات مفتاحية: آليات، الحماية، الأمن السيبراني، التحول الرقمي

Abstract :

The interest in achieving cyber security has become a priority for every country globally because of its importance in preserving information and data from theft and piracy and addressing various electronic terrorism.To achieve cyber security , we must adopt mixed technical, educationl, media , and legislative mechanismes and methods , anti-virus technique , and programs for e-mail and official accounts capableof addressing electronic attacks. The inclusion of anti-cybercrime systems within the educational curricula for all academic levels will enhance. The culture of digital security and enactment accurate and comprehensive legislation that suits will the resistance to cyber-attacks through the formulation of laws that regulateand will keep pace with technological progress and the continuous cooperation between individuals and the security services of each country , as well as cooperation between countries to monitor and track hacking and information piracy.

Keywords: mechanisms, protection, cyber security, contemporary changes

1.مقدمــة :

أصبح استخدام تكنولوجيا المعلوماتية في عصرنا الحالي أمرا ضروريا في مختلف المجالات، ما أدى إلى تقريب المسافات و تلبية حاجيات الأفراد بسرعة فائقة بفضل هذه الأجهزة المعلوماتية، و مختلف أجهزة الاتصالات،

لكن هذا لم يمنع من ظهور بعض المشاكل التي تهدد مصالح الأفراد والدول أثناء استخدام تجهيزات الحاسوب و الانترنت و أجهزة الاتصالات المختلفة، أين ظهر ما يسمى بالهجمات و التهديدات الالكترونية التي ينفذها مجرمو المعلوماتية للاستيلاء على المعلومات والبيانات وسرقتها، أو لاستغلالها في التجسس والإرهاب غيرها من الأهداف التي يسعون إليها.

إن تحقيق الأمن السيبراني أصبح من أولويات الدول لحماية الشبكات والبرامج والأجهزة والبيانات من الهجمات والقرصنة والتخريب وتدمير الشبكات، وهذا ما يتطلب اتباع أساليب مختلفة للوقاية من هذه التهديدات السيبرانية و التصدي لأي محاولة اختراق للشبكة في الوقت المناسب. ما يجعلنا في هذه المداخلة نركز عن أساليب تحقيق الأمن السيبراني والوقاية من الهجمات والتهديدات الالكترونية.

من خلال ما تقدم يمكن طرح الإشكالية التالية:

في ظل تحديات التحول الرقمي وزيادة حدة الجرائم المالية والاقتصادية، ما هي أهم آليات تحقيق الأمن السيبراني؟

1.1- : مفهوم الأمن السيبراني :

يشير مصطلح الأمن السيبراني الذي أتى من لفظ الكلمة اللاتينية السيبر (Cyber)، و معناها الفضاء المعلوماتي، و منه يعني مصطلح الأمن السيبيراني " أمن الفضاء المعلوماتي " من كل جوانبه، و هو عبارة عن تعبير شامل عن العالم الافتراضي الذي يحوي كل ما يتعلق باستخدامات و آليات و تطبيقات و تجهيزات تقنية المعلومات و الحاسب الآلي، و الترابط فيما بينها من خلال شبكات الحاسب و الاتصالات و الإنترنت[1] .

الأمن السيبراني هو " عبارة عن مجموعة من الوسائل التقنية و التنظيمية و الإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، و سوء الاستغلال واستعادة المعلومات الإلكترونية و نظم الاتصالات و المعلومات، و تعزيز حماية و سرية و خصوصية البيانات الشخصية و اتخاذ جميع التدابير اللازمة لحماية المواطنين و المستهلكين من المخاطر في الفضاء السيبراني "[2]

كما يعرفه (إدوارد أمورسو) Edward Amoroso على أنه : " وسائل من شأنها الحد من خطر الهجوم على البرمجيات، أو أجهزة الحاسوب أو الشبكات، و تشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة و كشف الفيروسات ووقفها و توفير الاتصالات المشفرة .[3]

الأمن السيبراني حسب تعريف الاتحاد الدولي للاتصالات في تقريره حول (اتجاهات الإصلاح في الاتصالات للعام 2010، 2011)، هو " مجموعة من المهمات، مثل تجميع وسائل، وسياسات و إجراءات أمنية، و مبادئ

---

[1]محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون و الكومبيوتر و الانترنت المنعقد في الفترة من 1 إلى 3 ماي، بكلية الشريعة و القانون بدولة الإمارات، 2000، ص 39.

[2]منى الأشقر جبور، الأمن السيبراني : التحديات و مستلزمات المواجهة، المركز العربي للبحوث القانونية و القضائية، 2012، ص 16.

[3]أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات و التخطيط، بيروت، 2016، ص 6.

توجيهية، و مقاربات لإدارة المخاطر، و تدريبات و ممارسات، و تقنيات يمكن استخدامها لحماية البيئة السيبرانية، و موجودات المؤسسات و المستخدمين ..[1](ITU ,2008)

2.1-الفواعل في مجال القوة السيبرانية:

يحدد جوزيف.س.ناي ثلاثة أنواع من الفاعلين الذين يملكون القوة السيبرانية:

– الدول : و التي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية و تطوير البنية التحتية و ممارسة السلطات داخل حدودها .[2]

–الفاعلون من غير الدول : و يستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة و مساعدة أجهزة استخباراتية متطورة، و لكن يمكنهم اختراق المواقع الالكترونية و استهداف الأنظمة الدفاعية.

– الأفراد (القراصنة): الذين يمتلكون معرفة تكنولوجية عالية و القدرة على توظيفها، و عادة ما تكون هناك صعوبة في الكشف عن هوياتهم، و من الصعب ملاحقتهم. .[3]

2 – التهديدات السيبرانية:

1.2 – تعريفها :

هي استغلال الحاسبات و تكنولوجيا المعلومات في تخريب و تدمير البنية المعلوماتية للخصوم، بل و تعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الالكتروني لمكاتب رؤساء الدول و التجسس عليهم وفق خطة ممنهجة .

إذا التهديدات السيبرانية أو الهجمات السيبرانية هي التي تهدد أمن المجتمع و أمن الاقتصاد الوطني و الجانب الأمني و العسكري للدول، كما أن للتهديدات السيبرانية أهداف مسطرة، حيث تمس كلا من الجانب المعنوي و الجانب المادي و على جميع الأصعدة .[4]

يعد أمن الحاسب و تقنية المعلومات مطلبا حيويا للمحافظة على خصوصية و سلامة و تصرفات الأفراد و الهيئات، لأنه بدونه ستنهار الثقة في التعامل مع القطاعات التي تقدم خدماتها بالاعتماد على معالجة البيانات و المعلومات، إذ قد يؤدي ذلك إلى توقف نشاط الفرد أو الهيئة، أو إلى حدوث نتائج كارثية يصعب إزالة آثارها لاحقا، و تكون مكلفة ماليا و معنويا .

2.2- أبرز التهديدات السيبرانية :

---

[1] ITU , Cybersecurity, Géneva : internationaltélécummunication Union (ITU),2008. P 125.

[2] Joseph .s Nye : JR ; Cyberpower , Harvard Kennedy School,2010. P 11.

[3] حسن بن أحمد الشهري. الأنظمة الالكترونية الرقمية المطورة لحفظ و حماية سرية المعلومات من التجسس، مركز النور للأبحاث الالكترونية، 2010، ص 11.

[4] نفس المرجع، ص 14.

هناك أشكال عديدة من التهديدات السيبيرانية و تختلف من حيث المصادر و الأهداف كالتجسس و سرقة المعلومات، و يمكن تلخيصها فيما يلي:

2.2 .1 .– التجسس الالكتروني : و يتم باستخدام وسائل التكنولوجيا الفائقة، و تهدف الهجمات السيبرانية في هذا الصدد إلى الحصول على معلومات سرية بطرق غير مشروعة .(فالتجسس السيبراني هو ذلك التجسس الذي يعتمد على استخدام التقنيات الالكترونية في الحصول على معلومات، و يختلف التجسس السيبراني من حيث النوع، فهناك التجسس عن طريق الأفراد، و من خلال الشبكات السلكية أو التجسس عن طريق الأقمار الصناعية.[1]

2.2.2– الجريمة السيبرانية :

زادت الجرائم الالكترونية بشكل كبير، نتيجة لتطور تكنولوجيا الاتصال و بروز العولمة الرقمية، فعلى الرغم من حقيقة أن الإنترنت يساعد في إجراء الأنشطة الاقتصادية و الاجتماعية المختلفة، إلا أن هناك مجموعة من المخاطر التي يتم ارتكابها عبر تلك الشبكة من سرقة البيانات و الوصول غير القانوني للمعلومات الشخصية، و غيرها من التهديدات[2]. فالجريمة السيبرانية هي "المخالفات التي ترتكب ضد الأفراد أو مجموعة من الأفراد بدافع الجريمة قصد إيذاء سمعة الضحية بأذى مادي أو عقلي للضحية مباشر، أو غير مباشر باستخدام شبكات الاتصال مثل الانترنت (كغرفة الدردشة، البريد الالكتروني، و الهاتف النقال) . فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، و الأفعال المتعلقة بمحتويات الكومبيوتر جميعها تقع ضمن الجرائم السيبرانية ".[3]

- **أهم الجرائم السيبرانية :**

يمكن اعتبار العمل الجرمي المحدد قانونا جريمة سيبرانية عندما يستهدف الهجوم :

- أمن المعلومات، أي مصداقيتها، و توافرها، و صحتها، و تندرج في هذا الإطار عمليات اختراق الأنظمة، عبر سرقة كلمة السر، أو التصيد، أو التضليل و الاحتيال و عمليات تدمير البيانات و سرقتها .
- سلامة الأشخاص، كما هو حال التربص و الترصد للأطفال، بغية الاعتداء عليهم، واستدراجهم، بهدف استغلالهم جنسيا، كما تندرج هنا عمليات استدراج الأشخاص، في إطار عمليات الاتجار بالرقيق، أو تجارة الأعضاء البشرية، أو إنتاج المواد الإباحية، أو تقديمها .
- الأموال من خلال عمليات الغش، و الاحتيال والتزوير، و الابتزاز، تبييض الأموال .

---

[1]أمجد المنيف، الإرهاب الإلكتروني – معركة حديثة، المجلة العربية، العدد 7 . يوليو 2015.، ص 02.

[2]أميرة محمد محمد سيد احمد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي، مجلة البحوث الإعلامية، كلية الإعلام جامعة الأزهر، العدد 58 الجزء الرابع، القاهرة، 2021، ص 178.

[3]إدريس بن الطيب عطية. الظاهرة الإرهابية في زمن ما بعد الحداثة، دراسة تحليلية في الأشكال و الأساليب و الإجراءات المضادة، المجلة العربية للدراسات الأمنية و التدريب، المجلد 31، العدد 63، الرياض، 2015، ص 24.

- المحتوى، كتوزيع مواد إباحية عن الأطفال، بث الكراهية التمييز العنصري، عرض خدمات المرتزقة، الترويج للإرهاب .
- أمن الدولة وسيادتها مثل التجسس، و إفشاء معلومات سرية .
- الملكية الفكرية، و التي يدخل فيها سرقة البرامج و القرصنة، و الاستعمال غير الشرعي لإنتاج محمي بالملكية الفكرية.[1]

3.2.2.الإرهاب السيبراني : هو ذلك الاستخدام للموارد المعلوماتية، المتمثلة في الإعلام و أجهزة الحاسوب و شبكة الانترنت و الفضائيات من أجل أغراض التخويف أو الإرغام لأغراض سياسية، أو الإقناع الفكري و التثقيف السلبي و العدواني . (و يمكن أن يتسبب الإرهاب المعلوماتي في إلحاق الشلل بأنظمة القيادة و السيطرة و الاتصالات أو قطع شبكات الاتصال و الوحدات و القيادة المركزية و تعطيل أنظمة الدفاع الجوي.[2]

2 .2 .4- الحروب السيبرانية : تعتمد هذه الحروب على فريق من المختصين في المعارك الالكترونية، حيث كل منهم يتميز بمسؤولياته و مهاراته الخاصة لترسيخ القدرة على القتال و التحكم بها و إبرازه ضمن الفضاء السيبراني، و يقوم مشغلو الحروب السيبرانية بالتخطيط للنشاطات الهجومية و الدفاعية و إدارتها و تنفيذها عبر الفضاء السيبراني .[3]

3.2 -أنماط التهديدات السيبرانية :

تقسم التهديدات السيبرانية التي تواجهها الدول و الأفراد إلى أربعة أنماط رئيسية و هي :

1.3.2-هجمات الحرمان من الخدمة : حيث يتم إطلاق حزمة كبيرة من الطلبات و المهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها و الاستجابة لها، مما يؤدي إلى توقفه بصورة جزئية أو كلية أو إبطاء عمله، و هذا ما يسبب ضررا للمستخدم النهائي، و هي تستعمل كثيرا ضد مواقع الإنترنت أو البنوك، أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية .[4]

2.3.2- إتلاف المعلومات أو تعديلها : و يقصد به الوصول إلى معلومات الضحية عبر شبكة الانترنيت أو الشبكات الخاصة، و القيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد أو خرائط سرية .[5]

---

[1]منى الأشقر جبور. السيبيرانية هاجس العصر، المركز العربي للبحوث القانونية و القضائية، بيروت .2017، ص 50.

[2]عادل عبد الصادق. خطر الحروب السيبرانية عبر الفضاء الالكتروني، مجلة الأهرام للكمبيوتر و الانترنت والاتصالات، 2017، ص 32.

[3]عزيز ملحم بربر. أمن الشبكات و الانترنت، جامعة نايف العربية للعلوم الأمنية، القاهرة، 2008، ص 04.

[4]محمد مختار. هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية ؟"، مفاهيم المستقبل، العدد 6، مركز المستقبل للأبحاث و التطوير، 2015، ص 50.

[5]نفس المرجع، ص 51.

3.3.2- التجسس على الشبكات : و يقصد به الدخول غير المصرح و التجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات، و الهدف منه الحصول على معلومات قد تكون خطط عسكرية أو أسرار حربية، اقتصادية، مالية، أو سياسية، مما يؤثر سلبا على مهام الخصم.

4.3.2- تدمير المعلومات : و يتم في هذه الحالة مسح و تدمير كامل للأصول و المعلومات و البيانات الموجودة على الشبكة، يصطلح عليه " تهديد لسلامة المحتوى " و يعني بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين ..[1]

ولعل ما سبق ذكره يقودنا إلى أن هناك تهديدات سيبرانية تؤدي إلى ما يلي :

1. تدمير المواقع على الشبكة المعلوماتية.
2. اختراق البريد الإلكتروني.
3. الاعتداءات على سرية الخطابات والمراسلات.
4. التشهير بالأشخاص.
5. سرقة بطاقات الائتمان.
6. نسخ البرامج.
7. إتلاف البرامج والمعلومات.
8. تزوير المستندات.[2]

3- أبعاد الأمن السيبراني :

تشمل خمسة أبعاد نذكرها فيما يلي :

1.3 - الأبعاد العسكرية : حيث تظهر القوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني، بما يسمح بسهولة تبادل المعلومات و تدفقها، و كذا السرعة في إعطاء الأوامر العسكرية و القدرة على الوصول إلى الأهداف عن بعد و تدميرها، و قد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الالكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي، و هذا قد يؤدي إلى شن هجمات إلكترونية مضادة على شبكات القوات المسلحة و أجهزة الاستخبارات، و من ثم التجسس على الأمن العسكري للدولة، و تعطيل قدرتها على النشر السريع لقواتها، أو قطع أنظمة الاتصال فيما بين الوحدات العسكرية و تعطيل شبكات الكومبيوتر، كما يمكن أن يتم شل و تعطيل عمل أنظمة الدفاع الجوي أو التوجيه الالكتروني و التسبب في فقدان السيطرة على وحدات القيادة.[3]

---

[1] محمد مختار، مرجع سابق، ص 52.

[2] آمنة محمد المختار، أميمة حميد الأحمدي. الضوابط الشرعية للمعلوماتية، المعلوماتية والتعليم، مكتبة دار الزمان، جامعة طيبة، الرياض، 2005، ص 468.

[3] حمدون توريه. الأمن السيبراني في البلدان النامية، الاتحاد الدولي للاتصالات، الأردن، 2006، ص 15.

2.3 – الأبعاد الاقتصادية : أصبح الفضاء الالكتروني جاذبا لقطاعات المجتمع كافة، أفراد ا و جماعات و زاد الاعتماد بصورة أساسية على التكنولوجيا الرقمية في تخزين البيانات و المعلومات، بالإضافة لاستخدام الحاسب الآلي في تطوير الصناعات و تحريك الاقتصاد، و أصبحت المعاملات المالية والاقتصادية محوسبة، و باتت شبكات البنوك و البورصات و شركات الأسواق المالية مرتبطة ببعضها البعض بنظم و شبكات إلكترونية، فأصبحت الإنترنت هي أساس المعاملات المالية و الاقتصادية و باتت تشكل محورا رئيسيا للتطور الاقتصادي في القرن الحادي والعشرين، و هو ما أثار الحديث عن أهمية تحقيق الأمن السيبري في المجال الاقتصادي.[1]

3.3 – الأبعاد الاجتماعية : تساهم شبكات التواصل الاجتماعي في فتح المجال للأفراد للتعبير عن تطلعاتهم و طموحاتهم الاجتماعية بأشكالها المختلفة، حيث تؤدي مشاركة شرائح المجتمع في استخدام الإنترنت إلى الاطلاع على الأفكار و المعلومات، و هذا ما يفرض ضرورة استقرار الفضاء الالكتروني، لأن انفتاح المجتمع على مجتمعات أخرى يؤسس لتبادل خبرات و أفكار و تكوين آفاق للتعاون و التكامل.[2]

4.3– الأبعاد السياسية : للدولة حق في حماية نظامها السياسي و مصالحها الاقتصادية لتحقيق رفاه شعبها ، حيث تساهم هذه الوسائل المعلوماتية الحديثة في مساعدة الأفراد على الاطلاع على خلفيات و مبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها، و بالمقابل لا يتوانى العاملون في الشأن السياسي من الاستفادة مما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة من الأفراد و الترويج لسياستهم في العالم، و مدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات و المبادئ و المواقف التي تروج لها[3]

هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني كالتسريبات المختلفة للوثائق الحساسة، التي سببت مشكلات في علاقات الدول ببعضها البعض، مما حتم على الدول إعادة النظر في سياستها الخارجية في ظل هذه التسريبات . كما لا يجب إغفال الدور البارز لشبكات التواصل الاجتماعي في تحقيق أهداف سياسية، كتنظيم حملات انتخابية أو تظاهرات افتراضية، و حركات احتجاجية الكترونية، هذا فضلا عن قيام بعض الدول مثل الولايات المتحدة ببث رسائل سياسية على مواقع التواصل الاجتماعي لتحقيق أهدافها، كقيام الجيش الأمريكي بتطوير برنامج إلكتروني يعمل على تدشين حسابات شخصية على مواقع التواصل الاجتماعي بلغات مختلفة، بهدف بث رسائل من خلالها تدعم الرؤية الأمريكية على مواقع التواصل الاجتماعي، و من ناحية أخرى وجدت الكثير من الحركات الإرهابية في هذه المواقع.[4]

---

[1]عبد الفتاح بيومي. مبادئ الإجراءات الجنائية في جرائم الكومبيوتر و الإنترنت، دار الكتب القانونية، مصر، 2007، ص 198.

[2]نوران شفيق. أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني، المكتب العربي للمعارف، القاهرة، 2014، ص 40.

[3]عادل عبد الصادق، مرجع سابق، ص 27.

[4]عبد الإله أحمد هلالي. اتفاقية بودابست لمكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2008، ص 129.

5.3- الأبعاد القانونية : تعد العلاقة بين القانون و التكنولوجيا علاقة تبادلية، فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها من خلال وضع أطر و تشريعات للأعمال القانونية و غير القانونية منها، و لكن بصورة عامة تفتقد الجريمة السيبرانية حاليا للأطر القانونية الصارمة للتعامل معها، و لعل هذا يعود حاليا لعوامل، مثل طبيعة الجريمة الالكترونية ذاتها، و صعوبة تحديد هوية مرتكبي تلك الجرائم، و مرونة تلك التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب كون الجرائم السيبرانية غير مقيدة بحدود الدول الأمر الذي يقتضي تفعيل التعاون الدولي لمكافحتها .[1]

4.- أهداف الأمن السيبراني:

يهدف الأمن السيبراني إلى حماية جميع العمليات التي نقوم بها باستخدام الانترنت و التكنولوجيا و مختلف وسائل الاتصال و حماية البيانات و التطبيقات و حفظ المعلومات الوطنية للدولة و للأفراد، و المحافظة عليها، يعني منع أي دخول عليها غير مرخص أو العبث بها و التي لابد أن يكون هناك نظام قوي يحمي هذه الخدمات و المعلومات التي توفرها و تزودنا بها هذه التكنولوجيا المتطورة عبر الفضاء الالكتروني.[2]

هناك أخطار معلوماتية متعددة يجب أخذها بعين الاعتبار عند بناء و تطوير تجهيزات و أنظمة المعلوماتية، حيث أن هذه الأخطار تمس سرية المعلومات، ووحدة و تجانسها، أو خطر عدم توفرها عند الطلب و عند الحاجة لمالكها، و هناك خطر منع الخدمة الذي يمنع استخدام الموارد و البرمجيات و التجهيزات المعلوماتية و تؤدي إلى انهيار النظام و منع الاستفادة منه، و خطر التسلل و الاختراق و الذي ينجم عنه دخول أشخاص غير مصرح لهم إلى الأنظمة و الموارد المعلوماتية و التحكم فيها أو استغلالها للهجوم على موارد و أنظمة أخرى، و خطر سرقة المعلومات الذي يمكن حدوثه بسبب ثغرات في الأنظمة أو التجهيزات أو باستخدام برامج خاصة مما يتيح لغير صاحب الشأن الاطلاع على البيانات المختزنة أو المرسلة و سرقتها أو العبث بها .[3]

إن مصطلح الأمن السيبراني يصف جميع الأمور المتعلقة بحفظ هذه الخدمات و البيانات و تدفق سيرها و الذي يحوي كل ما يتعلق باستخدامات و آليات و تطبيقات و تجهيزات تقنية و تدفق البيانات و المعلومات ، و البرامجيات، و الترابط فيما بينها من خلال شبكات الحاسب و الاتصالات و الانترنت . و منه فهدف الأمن السيبراني هو تعزيز حماية جميع ما يتعلق بالدولة الكترونيا وأفرادا لحماية هذه الأنظمة الالكترونية و أنظمه تقنية المعلومات و أنظمة التقنيات التشغيلية و جميع مكوناتها المحيطة بالمجتمع من أجهزة و برمجيات و معدات و جميع ما يؤثر على تقدم هذه الخدمات.[4]

---

[1]عبد الإله أحمد هلالي، نفس المرجع السابق، ص 135.

[2]مراد ماشوش. الجهود الدولية لمكافحة الإجرام السيبراني، جامعة الحسن الأول، كلية العلوم القانونية و الاقتصادية و الاجتماعية، مختبر البحث قانون الأعمال، المغرب، 2018، ص 50.

[3]نفس المرجع، ص 55.

[4]محمد بن أحمد بن علي المقصودي. الجرائم المعلوماتية : خصائصها و كيفية مواجهتها قانونيا، المجلة العربية للدراسات الأمنية، مج 33، العدد 70، جامعة نايف العربية للعلوم، الرياض، 2017، ص 13.

إن تأمين البنى التحتية لأمن المعلومات و البيانات الخاصة بالمواطنين، و حماية شبكة المعلومات و الاتصالات أمر لا بد منه لما لها من دور في تدفق البيانات بين المواطنين و الدولة و مختلف الأطراف ، لأن تعرض هذه الشبكة للتدمير و الاختراق و التخريب سيؤدي إلى قطع الاتصالات، و منه إلى توقف مختلف الخدمات الالكترونية، ما يتسبب في تعطل مختلف المصالح عن أداء مهامها . فالفضاء السيبيراني هو " المجال المادي و غير المادي الذي يتكون و ينتج من عناصر هي : أجهزة الكومبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل و التحكم، و مستخدمو هذه العناصر. [1] و تهدف الحماية إلى جعل المجرمين يحجمون عن خططهم، أو منعهم من تحقيقها، و إلى ضمان حد مقبول من الأخطار، و ذلك عبر وضع خطة تتلاءم و المحيط التقني، البشري، التنظيمي، و القانوني .

5- أساليب تحقيق الأمن السيبراني :

إن المحافظة على المعلومات و البيانات من أهم ما تحرص عليه الهيئات والمنظمات على مستوى الأفراد، بل على مستوى الدول أيضاً، إذ يمكن تعويض فقدان الأجهزة والبرامج، لكن يصعب تعويض فقدان البيانات والمعلومات أو التلاعب بها، فالمعلومات والبيانات تعد من أهم ممتلكات أي منظمة، لذا يتم السعي للمحافظة على البيانات، والمعلومات قدر الإمكان حتى لا يصل إليها أشخاص غير مصرح لهم، ويتم إتباع مجموعة من الإجراءات التي تضمن سلامة هذه المعلومات.[2]

هناك عدة أساليب يمكن اللجوء إليها لتحقيق الأمن السيبراني و التصدي للهجمات الالكترونية تشمل جوانب تقنية و إعلامية و تعليمية و أمنية نذكرها فيما يلي :

- استخدام تقنيات و برامج حماية متقدمة للبريد الالكتروني و للحسابات الرسمية، مضادة للفيروسات قادرة على التصدي للهجمات الالكترونية، و رفع كفاءة معايير الأمن و الأنظمة، و تطوير البرمجيات المقاومة للهجمات السيبرانية من خلال تزويد أنظمة أمن المعلومات بأحدث الأساليب و التقنيات و خصوصا تقنيات الذكاء الاصطناعي .
- الاعتماد على التشفير لاكتشاف الهجمات المحتملة و تتبعها، و رصد آلية كيفية تطويرها و إنشاء نظام الإنذار المبكر لرصد الهجمات الالكترونية المتوقعة، واتباع سياسة فعالة و قوية لتشفير البيانات و المعلومات الحساسة
- الاعتماد على نظام الحوسبة السحابية التي تعمل على الحماية من فقدان البيانات . فباستخدام التطبيق لن تفقد البيانات في حالة تعطل أو توقف الجهاز.

[1] ITU , Cybersecurity, Géneva : internationaltélécummunication Union (ITU),2008. P 12.

[2] آمنة محمد المختار، أميمة حميد الأحمدي، مرجع سابق، ص 478.

- استضافة الخبراء و المتخصصين في مجال الأمن السيبراني في مختلف وسائل الإعلام، و التوعية الدائمة لمستخدمي المنصات الرقمية للتعرف عن الطرق المحتملة التي يلجأ إليها القراصنة لاختراق الأنظمة و البيانات الحساسة و الكشف عن الأساليب و الحيل و التقنيات التي يستخدمونها .

- سن التشريعات الدقيقة الشاملة التي تناسب مقاومة الهجمات السيبرانية من خلال صياغة قوانين تنظم و تواكب التقدم التكنولوجي المتسارع للحد من التهديدات و المخاطر السيبرانية . .[1]

- إدراج أنظمة مكافحة جرائم الفضاء السيبراني ضمن المناهج التعليمية لكافة المراحل التعليمية ، لتعزيز ثقافة الأمن الرقمي، و التي من شأنها دعم الاستخدام الآمن لتكنولوجيا الاتصال و تطوير مهارات الطلاب البحثية لتكوين إطارات مهنية متخصصة في مجال إدارة الأمن السيبراني، و تعزيز الوعي الأمني لديهم، بما يتماشى مع التطور التكنولوجي في مجال الحوسبة السحابية و إدارة البيانات، و عقد شراكات واتفاقيات دولية بين الجامعات بهدف زيادة تأهيل المختصين للتعامل مع تلك الجرائم الالكترونية .

- إخضاع المواقع الالكترونية المشتبه فيها للرقابة المشددة، لإعداد خطط المواجهة، واتخاذ التدابير الاحترازية بشكل دوري، و تقوية و تحديث أنظمة التشغيل، و رفع كفاءة المبرمجين، لتصميم برامج و أنظمة يصعب اختراقها..[2]

- عقد ورش تدريبية باستمرار عن الذكاء السيبراني الاستراتيجي و كيفية توظيفه في مختلف القطاعات الحيوية للتصدي لمختلف التهديدات السيبرانية المحتملة. .[3]

- استخدام كلمات السر للدخول إلى الحاسب الآلي، وتغييرها كل فترة بحيث تعتمد طول الفترة على أهمية البيانات، كما أن بعض أنظمة التشغيل لا تسمح باستخدام كلمة السر نفسها مرة أخرى، وتجبرك على تغييرها بعد فترة محددة من قبل المشرف على نظام التشغيل.

- عمل طرائق تحكم داخل النظام تساعد في منع محاولات الدخول غير النظامية مثال ذلك: عمل ملف يتم فيه تسجيل جميع الأشخاص الذين وصلوا أو حاولوا الوصول إلى أي جزء من البيانات يحوي رقم المستخدم، ووقت المحاولة وتأريخها، ونوع العملية التي قام بها وغير ذلك من المعلومات المهمة.

---

[1] أميرة محمد محمد سيد احمد. استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي، مجلة البحوث الإعلامية، كلية الإعلام جامعة الأزهر، العدد 58 الجزء الرابع، القاهرة، 2021، ص179.

[2] نفس المرجع، ص 180.

[3] نفس المرجع، ص 181.

- تشفير البيانات المهمة المنقولة عبر وسائل الاتصالات كالأقمار الصناعية أو الألياف البصرية بحيث يتم تشفير البيانات ثم إعادتها إلى وضعها السابق عند وصولها إلى الطرف المستقبل، ويتم اللجوء إلى تشفير البيانات والمعلومات إذا كانت مهمة لأن عملية التشفير مكلفة.

عدم إلقاء مستهلكات المعلومات، أو شريط تحبير الطابعة، لأن مثل هذه المخرجات قد تحتوي على معلومات مهمة تصل إلى أشخاص غير مصرح لهم بالاطلاع عليها، لذا يجب تمزيق المخرجات بواسطة الآلات خصوصاً قبل إلقائها.

- توظيف أشخاص تكون مهمتهم المتابعة المستمرة لبرمجيات الحاسب الآلي، للتأكد من أنها تعمل بشكل صحيح، ولاسيما البرمجيات المالية التي غالباً ما يكون التلاعب بها من قبل المبرمجين أو المستخدمين وذلك عن طريق أخذ عينات عشوائية لمخرجات البرمجية في فترات مختلفة، كما يقومون بفحص ملف المتابعة للتعرف على الأشخاص الذين وصلوا إلى البيانات أو حاولوا الوصول إليها.

- عمل نسخ احتياطية من البيانات تخزن خارج مكان الجهاز.[1]

- استخدام وسائل حديثة تضمن دخول الأشخاص المصرح لهم فقط إلى أقسام مركز الحاسب الآلي، كاستخدام أجهزة التعرف على بصمة العين، أو اليد، أو الصوت.

- التعاون بين الدول في مجال حماية و تأمين الفضاء السيبراني و الدفاع و الردع ضد الإرهاب و مواجهة التحديات الأمنية السيبرانية .[2]

6 – الاتفاقيات الإقليمية و الدولية لأمن الفضاء السيبراني :

1.6– الاتفاقيات الاقليمية :

تنسجم الاتفاقيات الإقليمية مع متطلبات مواكبة سرعة تطور التهديدات السيبرانية، و يسجل في هذا المجال عدد من المبادرات نذكر منها :

- في عام 2002، وضعت مجموعة بلدان الكومنولث قانونا نموذجيا لمكافحة الجريمة السيبرانية، بالإضافة إلى قانون الإثبات الرقمي .

- في عام 2009، بادرت المجموعة الاقتصادية لغرب إفريقيا إلى إقرار توصية لمكافحة الجريمة السيبرانية، شكل الإطار القانوني لعمل الدول الأعضاء .

[1] آمنة محمد المختار، أميمة حميد الأحمدي، مرجع سابق، ص 480.

[2] أميرة محمد محمد سيد احمد، مرجع سابق، ص 181.

- جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2011، لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية و الحفاظ على أمنها و سلامة مجتمعاتها .

- تعتبر اتفاقية بودبست2001 (الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية) خطوة رائدة على مستوى التعاون بين الدول، و هي الوحيدة من حيث المدى و حجم الدول المنضمة إليها، حيث دخلت حيز التنفيذ عام 2004، و تعتبر أداة إقليمية ملزمة لمكافحة الجريمة السيبرانية، عبر تحقيق الانسجام بين القوانين الوطنية، و قد شددت على ضرورة تحسين تقنيات التحقيق و البحث و زيادة التعاون بين الدول.[1]

6.2- الاتفاقيات الدولية :

أما على المستوى الدولي فقد لعبت هيئة الأمم المتحدة عبر القرارات الصادرة عنها التي تدعم الأمن و السلامة في الفضاء السيبراني، و توعية الوعي العالمي بالأمن السيبراني دورا في جذب انتباه الدول الأعضاء إلى أهمية التحديات السيبرانية . و من أهم القرارات الصادرة عن الهيئة :

- قرار صادر سنة 1990، حول قانون جرائم المعلوماتية .
- قرار صادر سنة 1991، حول مكافحة الاستخدام الجرمي لتقنيات الاتصالات و المعلومات.
- عام 2001، إنشاء مجموعة من الخبراء الحكوميين GGE، بدأت عملها في 2004، لمناقشة الأخطار القائمة المحتملة في مجال أمن المعلومات، و الإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات و المعلومات العالمية .
- عام 2003، صدر قرار خاص حول الأمن السيبراني، ركز على القدرة على مكافحة الجريمة السيبرانية.[2]
- عام 2010، صدر قرار حول الأمن السيبراني، و ملحق حول ضرورة أن تلجأ الدول، لمعرفة مدى تناسب أطرها التشريعية و قدرتها على مكافحة الجريمة السيبرانية .

تبقى هذه الجهود، و القرارات، رغم قيمتها على المستوى الدولي غير كافية و غير فاعلة، نظرا لعدم إلزاميتها القانونية، و عدم إتاحتها إمكانية العقاب.

الخاتمة:

من خلال محاور هذه المداخلة يمكن القول أن تحقيق الأمن السيبراني أصبح غاية كل دولة لتأمين شبكاتها المعلوماتية و بياناتها من مخاطر الهجمات السيبيرانية، و لكن هذا لن يتحقق إلا باتباع أساليب الوقاية كاستخدام تقنيات و برامج حماية متقدمة للبوارید الالكترونية و للحسابات الرسمية مضادة للفيروسات قادرة على التصدي

[1] منى الأشقر جبور. السيبيرانية هاجس العصر، المركز العربي للبحوث القانونية و القضائية، بيروت، 2017، ص 103.

[2] عادل عبد الصادق، مرجع سابق، ص 334.

للهجمات الالكترونية، و تطوير البرمجيات المقاومة للهجمات السيبرانية من خلال تزويد أنظمة أمن المعلومات بأحدث الأساليب و التقنيات، و القيام بعمل شفرات لاكتشاف الهجمات المحتملة و تتبعها، و التصدي لها، وسن التشريعات الدقيقة الشاملة التي تناسب مقاومة الهجمات السيبرانية من خلال صياغة قوانين تنظم و تواكب التقدم التكنولوجي المتسارع للحد من التهديدات و المخاطر الالكترونية، و إدراج أنظمة مكافحة جرائم الفضاء السيبراني ضمن المناهج التعليمية لكافة المراحل التعليمية، لتعزيز ثقافة الأمن الرقمي، و التي من شأنها دعم الاستخدام الآمن لتكنولوجيا الاتصال و تطوير مهارات الطلاب البحثية لتكوين إطارات مهنية متخصصة في مجال إدارة الأمن السيبراني.

التوصيـات :

1- التعاون بين دول المعمورة في مكافحة التهديدات و الجرائم السيبيرانية .

2- تنظيم حملات تحسيسية و توعوية ببرمجة ملتقيات و محاضرات و أيام دراسية وطنية و دولية، و المشاركة في حصص تلفيزيونية و إذاعية و غيرها من الحصص الإعلامية لتنبيه جميع شرائح المجتمع بأخطار الهجمات السيبرانية .

3- التعاون مع مصالح الأمن من طرف المواطنين لرصد و تتبع عمليات الاختراق و القرصنة المعلوماتية .

4- تشفير جميع التعاملات الالكترونية لحماية البيانات و التطبيقات المختلفة من الهجموم و الاختراق الالكتروني .

5- الاعتماد على نظام الحوسبة السحابية التي تعمل على الحماية من فقدان البيانات في حالة تعطل أو توقف الجهاز.

6- التكوين المستمر للمختصين في الأمن المعلوماتي، و رفع كفاءاتهم العلمية في هذا المجال و هذا قصد ضمان الحماية الدائمة لشبكة المعلومات من أي هجوم و التعرف على كل مستجد فيما يخص التقنيات المتعلقة بالتصدي للهجمات السيبرانية .

قائمة المراجع :

1- آمنة محمد المختار، أميمة حميد الأحمدي، الضوابط الشرعية للمعلوماتية، المعلوماتية و التعليم، مكتبة دار الزمان، جامعة طيبة، الرياض، 2005.

2- إدريس بن الطيب عطية، الظاهرة الإرهابية في زمن ما بعد الحداثة، دراسة تحليلية في الأشكال و الأساليب و الإجراءات المضادة، المجلة العربية للدراسات الأمنية و التدريب، المجلد 31، العدد 63، الرياض، 2015.

3- أمجد المنيف، الإرهاب الإلكتروني – معركة حديثة، المجلة العربية، العدد 7 . الرياض، يوليو 2015.

4- أميرة محمد محمد سيد احمد. استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي، مجلة البحوث الإعلامية، كلية الإعلام جامعة الأزهر، العدد 58 الجزء الرابع، القاهرة .2021.

5- أوس مجيد غالب العوادي . الأمن المعلوماتي السيبراني، مركز البيان للدراسات و التخطيط، بيروت .2016

6- حسن بن أحمد الشهري .الأنظمة الالكترونية الرقمية المطورة لحفظ و حماية سرية المعلومات من التجسس، مركز النور للأبحاث الالكترونية. القاهرة، 2010.
7- حمدون توريه، الأمن السيبراني في البلدان النامية، الاتحاد الدولي للاتصالات . 2006.
8- عادل عبد الصادق، الإرهاب الالكتروني و القوة في العلاقات لدولية : نمط جديد و تحديات مختلفة، مركز الدراسات السياسية و الاستراتيجية، القاهرة. 2009
9- عادل عبد الصادق. خطر الحروب السيبرانية عبر الفضاء الالكتروني، مجلة الأهرام للكمبيوتر والانترنت والاتصالات، القاهرة، 2017.
10- عبد الإله أحمد هلالي. اتفاقية بودابست لمكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة. 2008
11- عبد الفتاح بيومي . مبادئ الإجراءات الجنائية في جرائم الكومبيوتر و الإنترنت، دار الكتب القانونية، مصر. 2007
12- عزيز ملحم بربر، أمن الشبكات و الانترنت، جامعة نايف العربية للعلوم الأمنية، الرياض. 2008
13- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون و الكومبيوتر و الانترنت المنعقد في الفترة من 1 إلى 3 ماي، بكلية الشريعة و القانون بدولة الإمارات . 2000
14- محمد بن أحمد بن علي المقصودي. الجرائم المعلوماتية : خصائصها و كيفية مواجهتها قانونيا، المجلة العربية للدراسات الأمنية، مج 33، العدد 70، جامعة نايف العربية للعلوم الرياض، 2017.
15- محمد مختار. هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية ؟"، مفاهيم المستقبل، العدد 6، مركز المستقبل للأبحاث و التطوير . القاهرة، 2015.
16- مراد ماشوش . الجهود الدولية لمكافحة الإجرام السيبراني، جامعة الحسن الأول، كلية العلوم القانونية و الاقتصادية و الاجتماعية، مختبر البحث قانون الأعمال . المغرب، 2018.
17- منى الأشقر جبور . الأمن السبيراني : التحديات و مستلزمات المواجهة، المركز العربي للبحوث القانونية و القضائية، القاهرة، 2012.
18- منى الأشقر جبور. السيبيرانية هاجس العصر، المركز العربي للبحوث القانونية و القضائية، بيروت . 2017.
19- نوران شفيق . أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني، المكتب العربي للمعارف، القاهرة. 2014.
20- Joseph .s Nye : JR ; Cyberpower , Harvard Kennedy School,2010.
21-ITU , Cybersecurity, Géneva : internationaltélécummunication Union (ITU),2008.
22-The internationaltélécummunication Union, (ITU)Toolkit for cybercrime légesla-tion ,Geneva ,2010.