

جامعة الشهيد حمه لخضر -الوادي-  
كلية العلوم الاجتماعية والانسانية  
مخبر التنمية الاجتماعية وخدمة المجتمع

الملتقى الوطني: الأمن السيبراني ورهانات الأمن الشامل في الجزائر

استمارة المشاركة

المشاركين	المشارك الأول	المشارك الثاني
اللقب والاسم	قواسمية العلمي	ثابت أميرة
الرتبة العلمية	طالب دكتوراه	طالبة دكتوراه
جامعة الانتماء	جامعة الشهيد حمه لخضر - الوادي-	جامعة الشهيد حمه لخضر - الوادي-
مخبر الانتماء	مخبر التنمية الاجتماعية وخدمة المجتمع	مخبر التنمية الاجتماعية وخدمة المجتمع
التخصص	علم الاجتماع التنظيم والعمل	علم الاجتماع الحضري
البريد الالكتروني	<a href="mailto:elalmi-gouasmia@univ-eloued.dz">elalmi-gouasmia@univ-eloued.dz</a>	<a href="mailto:tabet-amira@univ-eloued.dz">tabet-amira@univ-eloued.dz</a>
عنوان المداخلة	الأمن السيبراني: قراءة في المفهوم، وأهم التحديات التي تواجهه	
محور المداخلة	المحور الخامس: معوقات وتحديات الأمن السيبراني	

## ملخص:

نعيش اليوم في ظل عصر التحولات الرقمية والتطورات التكنولوجية، أو كما يسميه البعض: التحول الرقمي، ورغم ان هذا التحول الرقمي ساعد الدول والمجتمعات في شتى القطاعات والمجالات، إلا أنه في نفس الوقت يشكل تهديدا واضحا لأمنها وأمن سكانها، وهو ما أدى الى ظهور ما يسمى بالأمن السيبراني، والذي يعمل على محاولة التصدي لكل الهجمات التي يمكن ان تتعرض لها الدولة او الافراد، خاصة الهجمات الالكترونية.

وعليه هدفت هذه الورقة البحثية الى محاولة التطرق الى الامن السيبراني من خلال تناول قراءة في

المفاهيم، إضافة الى معرفة أهم التحديات التي تواجهه.

الكلمات المفتاحية: الأمن، الأمن السيبراني، المجتمع، المخاطر.

## Abstract:

Today we live in an era of digital transformations and technological developments, or as some call it: digital transformation. Although this digital transformation has helped countries and societies in various sectors and fields, at the same time it constitutes a clear threat to their security and the security of their population, which has led to the emergence of what It is called cybersecurity, which attempts to confront all attacks that the state or individuals may be exposed to, especially electronic attacks.

Accordingly, this research paper aimed to attempt to address cybersecurity by examining the concepts, in addition to identifying the most important challenges facing it.

**Keywords:** security, cybersecurity, society, risks.

## مقدمة

تحاول مختلف الدول والمجتمعات تحقيق أقصى استفادة ممكنة من التطورات التكنولوجية

التي يشهدها العالم حاليا، وذلك في مختلف المجالات، بغية تحقيق التقدم والتطور والازدهار ومحاولة مواكبة التقدم الموجود في الدول المتقدمة، خاصة ان التطورات التكنولوجية ساعدت الدول والافراد في تسيير مختلف أمورهم، ولكن هذا لا يعني ان لهذه التطورات التكنولوجية سلبيات، اذ انه يمكن لهذه التطورات التكنولوجية ان تساهم في القيام بالهجمات السيبرانية على الدول والافراد وهو ما يشكل خطرا كبيرا أكثر من ذي قبل، ومن اجل مواجهة هذه الهجمات السيبرانية، ظهر ما يسمى بالأمن السيبراني.

وبناء على هذا نطرح التساؤلات التالية:

1- ما المقصود بالأمن السيبراني؟

2- ماهي أبعاد الأمن السيبراني؟

3- ماهي أهم التحديات التي تواجه الأمن السيبراني؟

## أهداف الدراسة

تهدف هذه الدراسة الى تحقيق جملة من الاهداف، التي نذكرها كمايلي:

1- محاولة التعرف على مفهوم الأمن السيبراني.

2- محاولة الكشف عن أبعاد الأمن السيبراني.

3- التعرف على أهم التحديات التي تواجه الأمن السيبراني.

## 1- تعريف الأمن السيبراني

يعرف الأمن السيبراني على أنه: مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الإستغلال واستعادة المعلومات الإلكترونية ونظم الإتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. (عطية، 2019، صفحة 104)

كما عرف الأمن السيبراني على أنه: مجموعة من الممارسات التي تهدف الى حماية الانظمة والشبكات والبرامج من الهجمات الرقمية، أي كان نوعها، وهذه الممارسات تتنوع بين تدابير احتياطية استباقية قبل وقوع الضرر أي بمعنى تدابير وقائية، وتدابير علاجية بعد وقوع الضرر. (محمد توفيق و شيرين ، 2023 ، صفحة 766)

كما يعرف الامن السيبراني على أنه: تأمين كل الفضاء السيبراني الموجود والمتربط شبكيا من البنية التحتية لتقنية المعلومات، التي تشمل الانترنت وشبكات الاتصالات، وأنظمة الحاسب

الآلي والأجهزة المتصلة بالإنترنت، الى جانب المعالجات وأجهزة التحكم المرتبطة بها. (حميدي و طايلب ، 2022، صفحة 4)

كما يعرف الأمن السيبراني بانه: النشاط الذي يؤمن حماية الموارد البشرية والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع الى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث لا تتحول الأضرار الى خسائر دائمة. (بارة ، 2017 ، صفحة 257)

## 2- أهمية الامن السيبراني

وللدلالة على أهمية الأمن السيبراني في عالمنا المعاصر أن مجرمي الانترنت يركزون في هجماتهم على البنية التحتية الحيوية لأنه في حالة عدم حدوث هجوم ناجح عليها لا يمكنهم من الحصول على ربح مالي أو سياسي ، مستغلين في ذلك نقاط الضعف في هذه البنية كون بعضها يستعمل أنظمة حماية الكترونية تجارية ، ومع المعرفة الجيدة بالتقنية يمكن للمهاجم استغلال الثغرات الموجودة في هذه الأنظمة ، وما زاد من تعقيد الأمور أن الحوادث في الفضاء السيبراني تواجه دائما مشكلة إسناد المسؤولية فمن الصعب تتبع مرتكبي الحادث ، علاوة على ذلك إن التهديدات السيبرانية يصعب التنبؤ بها واتخاذ التدابير الوقائية في الوقت الملائم (سلمان، 2021، صفحة 159)

كما يقوم الأمن السيبراني بتقييم المخاطر من اجل التخطيط للتعافي من الكوارث و ووضع استراتيجيات للإنعاش في حال حدوث الكوارث ، كما تكمن أهمية الأمن السيبراني في حماية الشبكات من مختلف الهجمات الالكترونية والفيروسات ومكافحة التجسس ، كما يعمل على خلق جدار للحماية ومنع الغير المصرح به من الدخول إلى الشبكات والمواقع الخاصة ، كما يعمل الأمن السيبراني على تطوير مختلف أنظمة منع التسلسل وتحديد التهديدات سريعة الانتشار ، مثل

الهجمات التي لا تستغرق يوماً أو سفراً وشبكات الخاصة بتوفير وصول الأمن عن بعد. (جابوري، 2020، صفحة 73)

كما يمكن توضيح أهمية الأمن السيبراني في النقاط التالية:

- التقليل من مخاطر التهديدات الامنية والاختراقات المحتملة للبيانات الى جانب الحفاظ على سرية المعلومات.
  - احلال الحماية الامنية اللازمة للملفات الشخصية والحساسة لمنع الوصول غير المصرح اليها.
  - ضمان استمرارية عمل المؤسسات المؤمنة وتجنب تعطيل مصالحها المتصلة بالاستخدام السيبراني لشبكة الانترنت، مع تقليل وقت التوقف عن الخدمات الرقمية خاصة الحساسة منها.
- (حميدي و طاييب ، 2022 ، الصفحات 9-10)

### 3- أبعاد الامن السيبراني

تتمثل أبعاد الأمن السيبراني فيمايلي:

#### 3-1- البعد العسكري

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني، بما يسمح بسهولة تبادل المعلومات وتدفعها، وسرعة اتخاذ القرارات العسكرية، ومن ثم تحقيق الاهداف عن بعد ومن دون شك فإن عدم استغلال هذه التقنية والتسلح بها، أو تأمينها بشكل جيد من أي اختراق خارجي سيؤدي بالضرورة الى شن هجمات الكترونية مضادة على شبكات القوات العسكرية ومن ثم تدمير قواعد البيانات.

#### 3-2- البعد الاجتماعي

تعتبر الشبكة الدولية للمعلومات مجالا مفتوح لجميع الافراد، حيث يمكن لجميع المتعاملين السيبرانيين ان يستفيدوا من البنية التحتية والخدمات المتاحة لهم دون تحمل المخاطر الامنية، وهنا يجب التموه الى ضرورة التحسيس بأخلاقيات الأمن السيبراني.

### 3-3- البعد القانوني

هناك اساليب ممارسة عديدة في استخدام تقنية المعلومات كإنشاء المدونات، والتجمعات على الانترنت والحق في حماية ملكية البرامج المعلوماتية والابلاغ عن المخالفات والجرائم السيبرانية، وهذا ما أدى الى ظهور ترسانة قانونية تتوافق مع التغيرات الحاصلة.

### 3-4- البعد السياسي

لقد اصبح بإمكان المواطن ان يتحول الى لاعب اساسي وبإمكانه الاطلاع على خلفيات القرارات السياسية عبر الكم الهائل من المعلومات التي يسهل عليه الوصول اليها عبر الانترنت، وهنا نشير الى التسريبات للوثائق الحساسة مثلا والتي تثير مشكلات عويصة، وايضا دور شبكات التواصل الاجتماعي في تنظيم الدعايات السياسية والانتخابية وتنظيم التظاهرات الافتراضية، وافتعال الاحتجاجات الالكترونية، واصبح الفضاء السيبراني ملاذا للتجنيد من طرف التنظيمات الارهابية وغيرها. (طمطامي ، 2022/2021، الصفحات 25-26)

### 4- عناصر الأمن السيبراني

لأمن السيبراني مجموعة من العناصر الواجب توفرها حتى يستطيع القيام بدور على الوجه السليم، ويمكن توضيح أهم هذه العناصر كمايلي:

#### 4-1- التقنية

تلعب التقنية والتكنولوجيا دورا كبيرا في حياة الاشخاص والمؤسسات، حيث انها تعمل على توفير لحماية الفائقة لهم امام الهجمات السيبرانية، وتشمل حماية الاجهزة بمختلف أنواعها الذكية

والحاسوبية والشبكات وذلك بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

#### 4-2- الأشخاص

يستوجب الأمر لزوماً على الأشخاص من مستخدمي البيانات والأنظمة في مؤسسة ما، العمل على استخدام مبادئ حماية البيانات والمعلومات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانب القيام بنسخ احتياطي للبيانات.

#### 4-3- الأنشطة والعمليات

يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة. (طمطامي ، 2022/2021، الصفحات 19-20)

#### 5- أهداف الأمن السيبراني

يسعى الأمن السيبراني إلى تحقيق جملة من الأهداف التي يمكن ذكرها كمايلي:

- تأمين الفضاء الإلكتروني بما فيه الخدمات الرقمية.
- الحفاظ على سرية المعلومات وقصر النفاذ على الجهات المصرح لها فقط.
- الحفاظ على سلامة البيانات والبرامج وعدم فساد حالتها.
- الحفاظ على توافر تقديم الخدمات بشكل مستمر وبدون انقطاع أو تدهور .
- احترام الخصوصية الرقمية للمستخدمين والمتعاملين الرقميين.
- ضمان الصدق في التصرفات الإلكترونية والاستدلال على الفاعل من خلال تتبع الأثر.
- تطوير السياسات والاجراءات الامنية اللازمة للمنظمات والدول ونمو اقتصادها.

- خلق الثقة في التطبيقات والخدمات المقدمة خاصة في المعاملات التجارية والمالية الكترونيا.  
- الوصول الى الوضع الامثل لأداء نظام المعلومات جنبا الى جنب مع مستوى اداء الامن المطلوب.

- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام شبكات الانترنت المختلفة. (بوداود، دحو ، و صواق ، 2021 ،  
صفحة 836)

## 6- تحديات الامن السيبراني

يواجه الامن السيبراني مجموعة من التحديات التي تعيقه، ويمكن لنا ان نذكر اهم هذه التحديات في النقاط التالية:

- التشفير له نقاط ضعف، حيث يمكن كسر كلمات المرور .  
- ظهور تقنيات جديدة وبالتالي نقاط ضعف جديدة.  
- تصاعد عدد الحروب السيبرانية وعمليات التجسس السيبراني، نتيجة لزيادة تهديدات الدول فيما بينها.

- عدم مسايرة وتكيف القوانين التشريعية مع سرعة تطور الجرائم السيبرانية، وهو ما يجعلها غير قادة على مكافحتها.

- الإنسان: إن اكبر واطور تحديات الأمن السيبراني هو العنصر البشري والمتمثل فيما يلي:

- ✓ التمكن من التحكم في ردود الفعل العاطفية.
- ✓ السياسة الأمنية معقدة وتستند إلى أحكام بشرية.
- ✓ أنظمة الأمن هي من تصميم الإنسان وهذا الأخير هو الذي يسيروها ويثبت معاييرها ويستعملها.

✓ إساءة استخدام الحقوق: حتى نظام أو تطبيق جيد وموثوق به يمكن أن يتعرض للهجوم من قبل الأشخاص الذين ينتهكون حقوقهم.

✓ الموارد البشرية: يعد نقص المختصين في مجال امن منظومات الأمن تحديا حقيقيا للشركات. (بوقرص، 2022، الصفحات 73-74)

كما أن هناك بعض العوامل الأخرى التي ساعدت على تنامي التهديدات السيبرانية من بينها:

- تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية مع تصاعد ادوار الشركات متعددة الجنسيات ، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء السيبراني .

- تزايد اعتماد الدول على الأنظمة الالكترونية في جميع منشاتها الحيوية، الأمر الذي جعل من الممكن الأضرار بمصالحها من خلال الهجمات الالكترونية في حالات العداء

- قلة تكلفة الحروب السيبرانية مقارنة بنظيرتها التقليدية ، مع إمكانية شن الهجوم في أي وقت، بحيث لا يتطلب تنفيذه سوى وقت محدود.

- توظيف الفضاء السيبراني في تعظيم قوة الدول ، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة ، وبالتالي يظهر ما يسمى الاستراتيجية السيبرانية للدول.

- اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون ، سواء من الدول أو غير الدول في الحروب السيبرانية ، فقد تشن الهجمات الالكترونية عبر أجهزتها الأمنية الدفاعية ، كما قد تلجا إلى تجنيد القراصنة أو موالين لشن هجمات ضد الخصوم دون أي ارتباط رسمي. (كلاع، 2022، صفحة 300)

وبناء على هذه التحديات التي تواجه الأمن السيبراني، حاولنا تقديم بعض التوصيات او الحلول التي بإمكانها التقليل من هذه التحديات، وتتمثل هذه الحلول حسب وجهة نظرنا فيمايلي:

- سن قوانين صارمة مناسبة وتتكيف مع التطورات الحاصلة في مجال الأمن السيبراني والهجمات السيبرانية.

- قيام المؤسسات والشركات بتأمين نشاطاتهم الالكترونية بكلمات مرور قوية يصعب اختراقها من قبل الهاكرز.

- القيام بعقد اتفاقيات تعاون دولية في مجال الأمن السيبراني.

- القيام بتطوير الأجهزة المكلفة بضمان الامن السيبراني للدول.

- القيام بإنشاء فرق خاصة بالأمن السيبراني في المؤسسات والشركات.

## خاتمة

لقد ساعد التحول الرقمي والتطورات التكنولوجية في تحسين حياة الافراد والمجتمعات والدول في العديد من المجالات والجوانب، إلا انها لها آثار سلبية تتلخص أساسا في الهجمات السيبرانية، وهو ما ألزم وجود الأمن السيبراني، هذا الأخير الذي يلعب دورا كبيرا في ضمان حماية أمن الافراد والمجتمعات والمؤسسات والشركات وأمن الدول، على الرغم من وجود بعض التحديات التي تعترضه.

وقد توصلت هذه الدراسة الى النتائج التالية:

1- الامن السيبراني: مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الإستغلال واستعادة المعلومات الإلكترونية ونظم الإتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

2- تتمثل أبعاد الامن السيبراني في البعد الاجتماعي، البعد السياسي، البعد القانوني، البعد العسكري.

3- يواجه الأمن السيبراني مجموعة من التحديات التي تشكل خطرا عليه وتعيقه على أداء دوره المنوط به، ومن بين هذه التحديات نجد:

- التشفير له نقاط ضعف، حيث يمكن كسر كلمات المرور.
- ظهور تقنيات جديدة وبالتالي نقاط ضعف جديدة.
- تصاعد عدد الحروب السيبرانية وعمليات التجسس السيبراني، نتيجة لزيادة تهديدات الدول فيما بينها.
- عدم مسايرة وتكيف القوانين التشريعية مع سرعة تطور الجرائم السيبرانية، وهو ما يجعلها غير قادة على مكافحتها.
- الإنسان: إن اكبر واطغر تحديات الأمن السيبراني هو العنصر البشري.

## قائمة المراجع

- ادريس عطية. (2019). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري . *مجلة مصادقية* ، العدد 01 ، صفحة 104.
- اسماعيل جابوري. (2020، 12). دور الامن السيبراني في مواجهة التهديدات الالكترونية دراسة حالة الجزائر . *مجلة تحولات* ، صفحة 73.
- بومدين بوداود، سليمان دحو ، و عبد القادر صواق . (2021، 06 07). النمذجة البنائية لمساهمة ابعاد الامن السيبراني للبيانات في تحقيق رضا المستهلك الالكتروني من خلال تعزيز الثقة كمتغير وسيط. *مجلة ادارة الاعمال والدراسات الاقتصادية*، العدد 01، صفحة 836
- حياة حميدي، و نسيمة طايلب . (2022). مدخل مفاهيمي حول الأمن السيبراني . *مدار للدراسات الاتصالية الرقمية* ، العدد 02، صفحة 4.
- ساعد بوقرص. (2022). الامن السيبراني : مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات. *مجلة الابحاث في الحماية الاجتماعية*، العدد 01، الصفحات 73-74.
- سالم طمطامي . (2022/2021). *الصحافة الالكترونية والامن السيبراني - دراسة حالة الجزائر*-. كلية العلوم الانسانية والاجتماعية والعلوم الاسلامية ، قسم العلوم الانسانية . أدرار : جامعة احمد دراية .
- سمير بارة . (2017). الأمن السيبراني في الجزائر: السياسات والمؤسسات. *المجلة الجزائرية للأمن الانساني* ، العدد 04 ، صفحة 257.
- شريعة كلاع. (2022، 4 27). الامن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني. *مجلة الحقوق والعلوم الانسانية*، الصفحات 292-314.
- صلاح الدين محمد توفيق ، و عيد موسى شيرين . (2023). متطلبات تحقيق الامن السيبراني بالجامعات المصرية في ضوء التحول الرقمي من وجهة نظر اعضاء هيئة التدريس - جامعة بنها أتمودجا-. *المجلة التربوية* ، الجزء 2، صفحة 766.
- مصطفى ابراهيم سلمان. (2021). الامن السيبراني واثره في الامن الوطني العراقي . *مجلة العلوم القانونية والسياسية* ، صفحة 159.