ملخص :

أصبح الفضاء السيبيراني في العقود القليلة الماضية يجمع الكثير من الثقافات والشعوب عبر العالم حتى شبه العالم كله " **بالقرية الصغيرة** " وذلك نظرا للتطور الهائل في مجال التكنولوجيا الرقمية بوجه عام وتكنولوجيا الاتصال والحوسبة والإنترنت بشكل خاصّ، مما خلق مشكلات كبيرة في مجال أمن المعلومات والدول، الأمر الذي دفع الدول إلى وضع استراتيجيات أمنية للحيلولة دون الوصول إلى معلوماتها الاقتصادية والعسكرية، أو ما بات يعرف بالأمن السيبيراني والذي يهدف عموما إلى، حماية الأمن المعلوماتي للدول وبالتالي أمنها القومي، وكذلك القدرة على التعافي من الهجمات السيبيرانية أو الجرائم الإلكترونية أو الكوارث والمشكلات التي تصيب الشبكات والمعلومات، من هنا جاءت هذه الدراسة لتسلط الضوء على مفهوم الأمن السيبيراني وكذلك التهديدات والتحديات التي تواجهه خاصة في بلدنا الجزائر.

الكلمات المفتاحية : الأمن، الأمن السيبيراني، السيبيرانية.

summary :

In the past few decades, cyberspace has come to bring together many cultures and peoples across the world, to the point that the entire world has been compared to a “small village.” This is due to the tremendous development in the field of digital technology in general and communication technology, computing, and the Internet in particular, which has created major problems in the field of information and state security. Which prompted countries to develop security strategies to prevent access to their economic and military information, or what has become known as cybersecurity, which generally aims to protect the information security of countries and thus their national security, as well as the ability to recover from cyber attacks, cybercrimes, or disasters and problems that affect networks. And information, Hence, this study came to shed light on the concept of cyber security as well as the threats and challenges it faces, especially in our country, Algeria.

Keywords: security, cyber security, cyber.

أولا : الأمن السيبيراني مدخل مفاهيمي

1-مفهوم الأمن

1-1- المعنى اللغوي للأمن

الأمن هو المقابل- المضادّ- للخوف والفزع، فهو الطمأنينة والاطمئنان إلى عدم توقع المكروه، كما ربط الإسلام الأمن بالإيمان فالإيمان هو: اطمئنان القلب بالانتماء إلى الخالق والرازق والمنعم والراعي والحافظ- أي الاطمئنان بالمعية الإلهية العاصمة من أي خوف أو فزع أو اغتراب في الدنيا والآخرة، ومن ثم فالإيمان هو أنجع السبل لتحقيق الأمن بالنسبة للإنسان وبالنسبة للعلاقات بين البشر.[1]

وفي هذا السياق قال تعلى : ﴿ وَعَدَ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَعَمِلُوا الصَّالِحَاتِ لَيَسْتَخْلِفَنَّهُمْ فِي الْأَرْضِ كَمَا اسْتَخْلَفَ الَّذِينَ مِنْ قَبْلِهِمْ وَلَيُمَكِّنَنَّ لَهُمْ دِينَهُمُ الَّذِي ارْتَضَى لَهُمْ وَلَيُبَدِّلَنَّهُمْ مِنْ بَعْدِ خَوْفِهِمْ أَمْنًا يَعْبُدُونَنِي لَا يُشْرِكُونَ بِي شَيْئًا وَمَنْ كَفَرَ بَعْدَ ذَلِكَ فَأُولَئِكَ هُمُ الْفَاسِقُونَ ﴾[2]

وقال تعالى: ﴿ فَلْيَعْبُدُوا رَبَّ هَذَا الْبَيْتِ * الَّذِي أَطْعَمَهُمْ مِنْ جُوعٍ وَآمَنَهُمْ مِنْ خَوْفٍ ﴾[3]

تعريف رونيه ديكارت :" متى كان الأمل قويا جدًا لدرجة أنه يطرد الخوف تمامًا، ويغير طبيعته ويسمى الأمن أو التأمين "[4]

من خلال هذه التعريفات يتضح بأن مفهوم الأمن هو مفهوم معاكس للخوف.

1-2- المعنى الاصطلاحي للأمن

يرى وولتر ليبمان walter lippman"أن الأمة تبقى في وضع آمن إلى الحد الذي لا تكون فيه عرضة لخطر التضحية بالقيم الأساسية إذا كانت ترغب في تفادي وقوع الحرب وتبقى قادرة لو تعرضت للتحدي على صون هذه القيم عن طريق انتصاراتها في حرب كهذه"[5]

ورى أرنولد وولفرز arnold walfers "يقصد بالأمن من وجهة النظر الموضوعية عدم وجود تهديد للقيم المكتسبة أما من وجهة النظر الذاتية فيعني عدم وجود مخاوف من تعرض هذه القيم للخطر"[6]

اما مفهوم الأمن الواسع فيشمل كل ما يحقق الاستقلال السياسي للدولة وسلامة اراضيها، وضمان الاستقرار السياسي والاقتصادي والاجتماعي الداخل، فهو يشمل تحقيق الأمن ببعديه الداخلي والخارجي، أي أنه "تأمين كيان الدولة والمجتمع من الأخطار التي تتهددها داخليا وخارجيا وتأمين مصالحها وتهيئة الظروف المناسبة اقتصاديا واجتماعيا لتحقيق الأهداف والغايات التي تعبر عن الرضا العام في المجتمع"[7]

2- مفهوم الأمن السيبيراني

2-1- مفهوم السيبيرانية

2-1-1- السيبيرانية لغة : وهي مأخوذة من كلمة " سيبر" وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبيرانية تعني " **فضاء الأنترنت**"، وهي كلمة مشتقة من الكلمة اليونانية "**kybernets**" التي وردت في بدايات مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة. [8]

أما قاموس "**أكسفورد**" الإنجليزي" **OXFORD** " **فيعرفها على أنها** "**دراسة فاعلية العمل البشري بمقارنتها بفاعلية الآلات الحاسبة تتصل بسمات وخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي**"[9]، فيما يعرفها قاموس الأمن المعلوماتي بأنها : "هجوم الفضاء الإلكتروني يهدف إلى السيطرة على المواقع الإلكترونية أو بنى محمية إلكترونيا لتعطيلها أو تدميرها أو الإضرار بها"[10]

2-1-2- المفهوم الاصطلاحي للسيبيرانية : ويرجع أصل اللفظ إلى منتصف القرن ال 20، مع عالم الرياضيات الأمريكي "wieners narbert"، الذي استخدمها للتعبير عن التحكم الآلي، حيث عرف السيبرنيتيقية على أنها "التحكم والتواصل عن الحيوان والآلة "، كما ذكر في الكتاب ذاته أنها :"علم نقل الرسائل بين الإنسان والآلة أو بين الآلة والآلة"، من هنا تبلورت السيبيرانية وتم توظيفها للتعبير عن العمليات الآلية والعلاقات بين الأجهزة الإلكترونية والإنسان.[11]

ورأى "وينر" أنه يمكن تطبيق هذا النظام على نطاق واسع في مختلف المجالات ليس العملية فقط بل الانسانية أيضا وبالتالي فالمصدر الاصطلاحي الحديث لكلمة سيبيرانية وهو "علم القيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل"[12]

2-2- الأمن السيبيراني

يعرّف الأمن السيبيراني بأنه : النشاط الذي يؤمن حماية الموارد البشرية والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانيات الحد من الخسائر والأضرار، التي تترتب في حالة تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ماكان عليه في أسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة.[13]

هو استراتيجية عمل تقوم بها الدول أو بعض الهيئات المختصة في حماية الأنظمة والبرامج من الهجمات الرقمية التي تهدف عادة إلى الوصول إلى المعلومات الحساسة وإعادة تغييرها أو إتلافها أو ابتزاز هذه الدول والمؤسسات من أجل ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية العادية.[1514]

كما يعرف الأمن السيبيراني على أنه: جميع الإجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به، ويشمل كذلك حماية الأجهزة والبيانات.[16]

كما عرّف بعض الفقهاء الأمن السيبيراني بأنه : "أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت وهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها لمواجهة التحديات، ومنع التعديات، او للحد من آثارها في أقسى وأسوأ الأحوال "[17]

وقد عرّفه فريق العمل المشترك المعني بتعليم الأمن السيبيراني بجامعة "جورج واشنطن" أنه : نظام قائم على الحوسبة يشمل التكنولوجيا والأشخاص والمعلومات والعمليات المؤكدة، ويشمل إنشاء وتشغيل وتحليل واختبار أنظمة الكمبيوتر الآمنة، إنها دورة دراسة متعددة التخصصات بما في ذلك الجوانب القانونية والسياسية والعوامل البشرية ولأخلاق وإدارة المخاطر.[18]

ثانيا : أبعاد الأمن السيبيراني

يشتمل الأمن السيبيراني على جملة من الأبعاد المرتبطة ببعضها ارتباطا وثيقا وهي كالآتي :[19]

1- الأبعاد العسكرية :

تكمن الميزة النسبية للقوة السيبيرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وكذا السرعة وإعطاء الأوامر العسكرية والقدرة على إيصال الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن الشبكات الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي، قد يتسبب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات، ومن ثم التجسس على الأمن العسكري للدول، وتعطيل قوة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الاتصال في ما بين الوحدات العسكرية وتطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل أنظمة الدفاع الجوي أو التوجيه الإلكتروني فضلا عن إمكانية فقدان السيطرة على وحدات القيادة.

2- الأبعاد الاقتصادية :

يرتبط الأمن السيبيراني ارتباطا وثيقا بالاقتصاد فالتلازم واضح بين اقتصاد المعرفة وتوسيع استخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كل المستويات، كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث في إدارة كلفة إنتاجها بأفضل الشروط، يضاف إلى ذلك دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق الخدمات الإلكترونية، إذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي وتتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع آمنة، وقد وضعت بعض الدول تشريعات خاصة بحماية أموالها وما يمكن أن يثيره هذا الأمر من صعوبات، وما يتطلبه من تشريعات للحد من بعض الجرائم الاقتصادية والمالية الخطيرة العابرة للحدود كتبييض الأموال والتهرب من الضريبة، فالأمن السيبيران يضمن تقديم الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الإقبال عليها بما يترجم عمليا بتطوير أسس اقتصاد سليم.

وكمثال على ذلك، يشير تقرير صادر عن شركة "emarkater" إلى أن حجم التجارة الإلكترونية بلغ 1.5 تريليون دولار عام 2014 مقارنة بعام 2013 الذي بلغت فيه 1.2 تريليون دولار، ونظراً لارتفاع

معدل الجرائم السيبرانية المنظمة والخطيرة، فإن ذلك يمثل تهديداً صريحاً لنمو الاقتصاد الرقمي ما لم تقم الدول بتعظيم معايير الأمن السبراني بما يضمن الحد من هذه الجرائم.[20]

3- الأبعاد الاجتماعية :

تساهم شبكات التواصل الاجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكالها المختلفة، كذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة لتطوير المجتمع، مما يتيح الفرصة للإطلاع على الأفكار والمعلومات وبما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء الإلكتروني والمجتمع الذي يرتكز عليه، كما أن انفتاح مجتمع ما على المجتمعات الأخرى، يؤسس لتبادل أفكار وخبرات وتكوين آفاق للتعاون والتكامل.

4- الأبعاد السياسية :

يتمثل البعد السياسي للأمن السيبيراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية، التي تعني حقها وواجبها في السعي إلى تحقيق رفاه شعبها، في وقت تؤثر موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان الفرد أن يتحول إلى لاعب أساسي في اللعبة السياسية كما أصبح بإمكانه الاطلاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها، وبالمقابل لا يتوانى العاملون في الشأن السياسي من الاستفادة مما تقده هذه التقنيات للوصول إلى أكبر شريحة ممكنة من الأفراد والترويج لسياساتهم في العالم، ومدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات والمبادئ والمواقف التي تروج لها.

5- الأبعاد القانونية :

تعد العلاقة بين القانون والتكنولوجيا علاقة تبادلية فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية وغير القانونية منها، ولكن في الوقت الحالي تفتقد الجريمة السيبيرانية في الوقت الحالي للأطر القانونية الصارمة للتعامل معها، ولعل ذلك يعود لعوامل مثل طبيعة الجريمة الإلكترونية في حد ذاتها وصعوبة تحديد هوية

مرتكبي تلك الجرائم ومرونة التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب ذلك فإن الجرائم السيبيرانية غير مقيدة بحدود الدول، الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها.[21]

ولعل من أبرز الممارسات القانونية في مجال الأمن السيبراني هو ضمان بعض الحقوق في هذا المجال كحق النفاذ إلى الشبكة العالمية للمعلومات، وأيضاً توسعت بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات على الإنترنت، وأيضاً الحق في حماية ملكية البرامج المعلوماتية.

ثالثا : المبادئ الأساسية للأمن السيبيراني

استنادا إلى توجيهات الخبراء الإقليميين والأطر الدولية والإقليمية بشأن الأمن السيبيراني، فقد حددت جمعية الإنترنت ISOC المبادئ الأساسية التالية لتأمين شبكة الإنترنت:[22]

أ- **الوعي** : يتعين على جميع الجهات المعنية في كل من القطاعين العام والخاصّ، فهم المخاطر التي تهدد أمنها، ومدى تأثير تلك المخاطر عليها وعلى الآخرين في النظام البيئي الخاص بالبنية التحتية لشبكة الإنترنت.

ب-**المسؤولية** : يجب على جميع الجهات المعنية تحمل مسؤولية مواجهة المخاطر الأمنية في إطار أدوارها ومؤسساتها، مع الأخذ في الاعتبار الآثار المترتبة على اتخاذ إجراء ما أو التقاعس في تنفيذه.

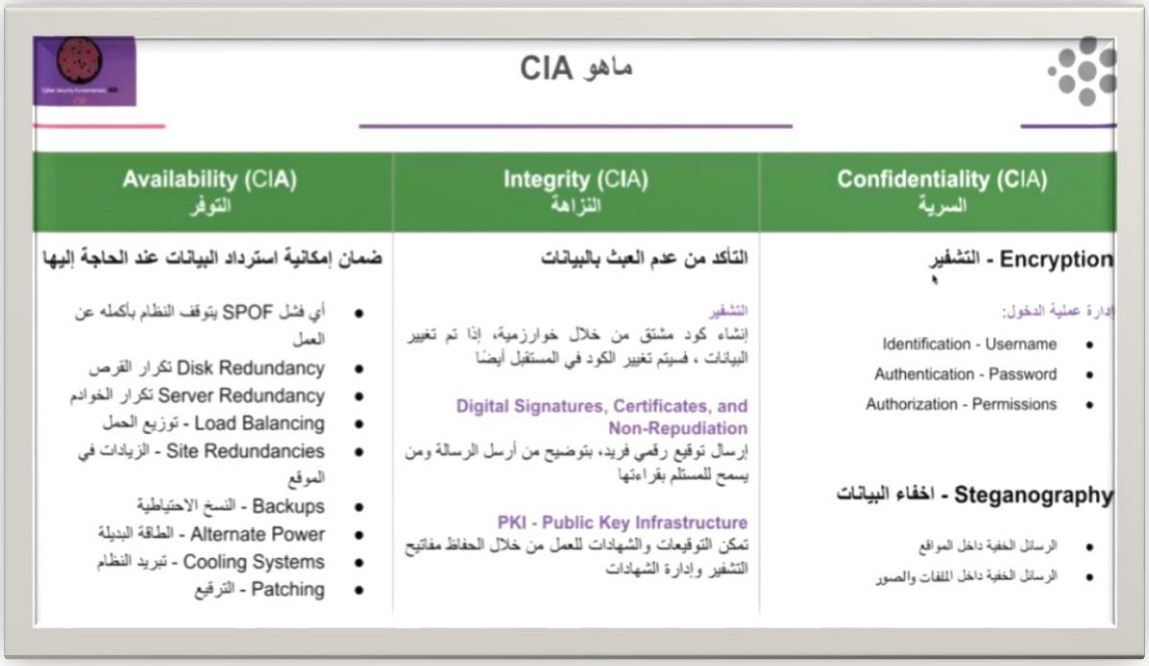
ت-**التعاون** : يجب إشراك جميع الجهات المعنية، بما في ذلك الأطراف المعنية خارج الحدود، في حوار مستمر حول الأمن السيبيراني لمواجهة التهديدات الجديدة والمستمرة مواجهة فعّالة.

كما أنه هناك ثلاث معايير أساسية اتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار إليها بمثلث أو ثلاثي "**CIA**" وهي السرية والأمانة والتوافر[23]

- **السرّيّة C**: ويقصد بها عدم كشف المعلومات لغير أطرافها بما يوفر الخصوصية والسرية للمعلومات المتداولة على الفضاء الرقمي.
- **الأمانة** (النزاهة) I : وتعني عدم التلاعب بالمعلومات أو حذفها أو تعديلها بحث يضمن المستخدم دقة نقل ما يريد من معلومات دون تدخل في أثناء النقل أو التخزين أو المعالجة.

- **التوافر A:** أما في ما يخص التوافر فهو استمرار توفر المعلومة للشخص أو الجهة التي يسمح لها المستخدم بالاطلاع عليها عند الحاجة.

المصدر : حسن الحسين، اساسيات الأمن السيبيراني



المصدر : حسن الحسين، اساسيات الأمن السيبيراني

رابعا : أنماط التهديدات السيبيرانية

تتعدد أشكال التهديدات السيبيرانية وتختلف من حيث الطبيعة والمصادر والأهداف كالتجسس وسرقة المعلومات وشن الحروب وبالتالي بات العديد من الفواعل الدوليين يلجؤون إلى آليات إلكترونية لتحقيقها، وعلى الرغم من تعدد صور وأشكال الهجمات الإلكترونية، غير أنه من الممكن تقسيمها إلى المجموعات الرئيسية التالية :[24]

1- خطر الكوارث الطبيعية أو (العرضية للكابلات البحرية)

تعد الكابلات (**Submarine cable**) جزءا هاما لتوفير خدمة الاتصالات بين دول العالم في مجال الإنترنت، وشبكات الكمبيوتر وغيرها، فمنذ عام 2005 اصبحت الكابلات البحرية مأهولة على مجال الاتساع والانتشار، أما على نطاق التقدم والتطور، تحولت إلى تقنيات أخف وزنا واصغر حجما، كما تعرضت تلك الكابلات إلى عدد من المشكلات التي تؤثر سلبا على أعمال البنى التحتية بالضرر، حيث لا تقع في مياه المحيط العميق.

2- التجسس الإلكتروني

يعد أحد أنواع التجسس التقليدي، باستخدام وسائل التكنولوجيا الفائقة، ومعظم الهجمات السيبيرانية المتطورة التي تقع ضمن هذه الفئة، حيث يتم الحصول على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية اقتصادية، أو استراتيجية أو عسكرية. فالتجسس السيبيراني هو ذلك التجسس الذي يعتمد على استخدام التقنيات الإلكترونية للحصول على معلومات، ويختلف التجسس السيبيراني من حث النوع، فهناك التجسس عن طريق الأفراد، ومن خلال الشبكات السلكية أو التجسس من خلال الأقمار الصناعية.

3- الجريمة السيبيرانية

وهي المخالفات التي ترتكب ضد الأفراد أو مجموعات من الأفراد بدافع الجريمة قصد إيذاء سمعة الضحية بأذى عقلي أو مادي مباشر أو غير مباشر باستخدام شبكات الاتصال مثل الإنترنت (غرف الدردشة، البريد الإلكتروني، الموبايل)، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو

مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة **السيبيرانية**".

4- الإرهاب السيبيراني

يعتبر الإرهاب السيبيراني تهديدا واضحا للأمن القومي للدول والذي يتضح من خطورة توظيف التقنيات الذكية في تنفيذ هجمات إرهابية سيبيرانية، سواء عبر الفضاء السيبيراني أو استخدام الروبوتات وطائرات دون طيار في شن تلك الهجمات أو استخدام الطابعات ثلاثية الأبعاد في تصنيع الأسلحة.[25]

وكان "**باري كولين Barry collin**" من أوائل الذين استخدموا مصطلح الإرهاب السيبيراني **(cyber terrorism)**، في ثمانينيات القرن الماضي والتي خلص فيها إلى صعوبة وضع تعريف شامل للإرهاب التكنولوجي، ولكنه تبنى تعريفا للإرهاب السيبيراني بأنه " هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب"[26]

اضحت الأسلحة السيبيرانية بطبيعة الحال من أهم أدوات حروب الجيلين الرابع والخامس، وهي ليست حكرا على الدول بالطبع، إذ تقوم التنظيمات المتطرفة باستخدام بعض آلياتها فهي مجرد فيروسات وديدان وبرمجيات خبيثة يتم تصميمها عبر أكواد وبرامج كمبيوتر لشن هجمات إلكترونية على أهداف عسكرية ومدنية، تؤدي إلى تدمير النظم والبرمجيات أو المكونات المادية من أجهزة ومعدات أو إلحاق خلل وظيفي أو فني بها، بما قد يؤدي في النهاية إلى تدمير البنية التحتية للدول أو اختراق الأنظمة العسكرية والتجسس على الأفراد والمعلومات وأنظمة الاتصالات وغيرها من الأعمال التخريبية التي تهدد أمن الدول.[27]

ووفقا لوزارة الدفاع الأمريكية فإن الإرهاب السيبيراني يقصد به " عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث الخوف تجاه تلقي الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل إلى لأجندة سياسية أو اجتماعية أو فكرية معينة، وتتعدد استخدامات التنظيمات الإرهابية للتكنولوجيا ومخرجاتها سواء لأغراض

التجنيد أو الدعاية الدينية المتطرفة، أو للتمويل من مصادر خفية يصعب تعقبها، أو في صناعة الأسلحة وتنفيذ العمليات الإرهابية".[28]

خامسا : تحديات الأمن السيبيراني

بالإضافة إلى مخاطر الفضاء السيبيراني الكثيرة والمتعددة فللأمن السيبيراني هو الآخر تحديات كثيرة، وهذا ما يؤكد بأن الخطر صفر أو الأمن 100% في ميدان الأمن السيبيراني غير موجودان وذلك مهما اتخذت من احترازات وتقنيات، ومن هنا سنحاول ذكر وباختصار أهم تحديات الأمن السيبيراني:[29]

1- **الإنسان** : إن أكبر وأخطر تحديات الأمن السيبيراني هو العنصر البشري والمتمثل في ما يلي :

- التمكن من التحكم في ردود الفعل العاطفية
- السياسة الأمنية معقدة وتستند إلى أحكام بشرية
- أنظمة الأمن هي من تصميم الإنسان والإنسان هو الذي يسيرها ويُثبت معاييرها ويستعملها
- إساءة استخدام الحقوق: حتى نظام أو تطبيق جيد وموثوق به يمكن أن يتعرض للهجوم من قبل الأشخاص الذين ينتهكون حقوقهم.
- الموارد البشرية : يُعد نقص المتخصصين في مجال أمن منظومات الأمن تحديا حقيقيا للشركات والدول.

2- المنظمات تخاطر عند استعمالها للفضاء السيبيراني

3- التشفير له نقاط ضعف وكلمات المرور يمكن كسرها.

4- الابتكار في خدمة الهجمات السيبيرانية ولهذا فإن المراقبات التقليدية للمخاطر يجب أن تتكيف مع التهديدات الحالية والمستقبلية.

5- ظهور تقنيات جديدة وبالتالي نقاط ضعف جديدة وباستمرار وحتى للشركات التي لديها موارد لا بأس بها

6- توسُّع وتطور رقعة الهجومات السيبيرانية وذلك راجع للإرتفاع المذهل لعدد الأشياء المتصلة بالإنترنت، وكذا عدد مستخدمي الإنترنت من جهة وتهديدات الدول في ما بينها، والذي أدى إلى تصاعد الحروب السيبيرانية والتجسس السيبيراني من جهة أخرى.

7- المرونة السيبيرانية باعتبارها ميزة الشركات التي تتمتع بالقدرة على الاستعداد والتكيف مع التهديدات المتطورة وكذلك استرداد قدراتها بسرعة من الهجمات السيبيرانية، في هذا الإطار يلاحظ عدم إقامة تدريبات حل الأزمات لعدد كبير من الشركات.

8- القوانين التشريعية في ميدان الأمن السيبيراني والتي من المفروض أن تكون متطورة وسريعة تساير وتتكيف مع تطور الجرائم السيبيرانية من أجل مكافحتها في الوقت المناسب.

سادسا : التقنيات المستخدمة في الأمن السيبيراني للدول

أكد البروفيسور سعدي سلامي أن " التقدم المتسارع الذي يشهده العالم في مجالات الذكاء الاصطناعي والتطور التكنولوجي ساعد كثيرا في تحقيق التفوق والريادة والتنمية المستدامة، لكنه خلق في المقابل تحديات جمة ولاسيما على صعيد تحقيق الأمن السيبراني وتعزيز الدفاعات السيبرانية للدول والمجتمعات التي تنامت خطورتها كذلك، من خلال التكنولوجيات الحديثة[30] والمتمثلة في :

1- **التعلّم العميق : Deeplearning**

ويتم عن طريق تعليم الحواسيب باستخدام معالجة البيانات الضخمة عبر أنظمة الشبكات الاصطناعية المتعددة الطبقات، ويشكل خطرا على أمن البنية التحتية للمعلومات التابعة للدول، كما يمكن استخدامه في المقابل لتأمين الشبكات والقواعد المعلوماتية.[31]

2- **اللسانيات الحاسوبية : computeriezed lunguistic**

وهي التي تسهل جمع المعلومات بكل اللغات، وعملية التعلم الآلي، والتعلم العميق، من خلال المحاكاة، مما يهدد الأمن المعلوماتي للدول، من خلال التعرف البصري على الحروف (بالإنجليزية OCR)، والقواميس الإلكترونية التي تعد قواعد بيانات ضخمة، والترجمة الإلكترونية، وتقنية التعرف الصوتي وغيرها التي تساعد في عملية استعادة المعلومات والمحاكاة[32]

3- **الذكاء الاصطناعي والاقتصاد الرقمي :**

من خلال جمع البيانات الضخمة من قواعد البيانات ومواقع الإنترنت، ومواقع التواصل الاجتماعي، باستخدام تقنيات الذكاء الاصطناعي، وجمع المعلومات الشخصية، ومقارنتها، وتكوين ملفات عن

الأشخاص، واستهدافهم بالإعلانات التجارية، بالإضافة إلى الحوكمة الاقتصادية، ورقمنة الإدارات والمؤسسات وغيرها.[33]

4- الحوسبة السحابية : Cold computing

وذلك من خلال فضاء منفصل لحماية وتأمين البيانات، من خلال إنشاء شبكات لامركزية، واستخدامها بشكل مباشر وشفاف دون وسيط، وقد عمد الكثير إلى إلى التوجه نحو استخدامها، خاصة في المعاملات المالية وأثبتت نجاعتها في حماية البيانات من الاختراق، إلا أن لها عيوب، وتتمثل في عدم معرفة هوية صاحب الحوسبة، وأيضا إمكانية تعرض البيانات للضياع، أو الحذف وعدم إمكانية الدخول إليها أو استرجاعها.[34]

5- الواقع المعزز : Augmented reality

ويقصد به استخدام الآلة التي تعزز الوجود الإنساني، وتحاكي ذكاءه، وتعمل من خلال بياناته الخاصّة.

6- الحاسوب الكومومي : Quantum computer

هي حواسيب متطورة جدا، وهي اختصار " **لكوانتم بت**"، حيث تتميز بقدرتها على تخزين كم هائل من المعلومات في أكثر من 0 و 1 خلافا لما يستخدمه نظام الحاسوب التقليدي، حيث (Qubits) يمكن أن تكون 0 أو 1 أو عدد غير متناهي من الأرقام في حالات مختلفة. وتقوم أجهزة الحاسوب الكمية بتوفير طاقة هائلة، والتي بدورها ستحل العمليات الحسابية بوقت أقل وجهد وطاقة أقل، وتعد سبب ناجح في تطوير تقنيات الذكاء الاصطناعي وجميع التطورات التكنولوجية، ومن الجدير بالذكر أن هذه التقنية ساعدت في حل المشاكل الرياضية الصعبة والمستعصية ومعالجة أفضل للمعلومات بشكل أدق وأسرع. ومن المهم ذكره الإنترنت الكمي، وسيكون هذا النوع من الإنترنت غير قابل للاختراق أو السرقة، حيث سيعمل على تقنية التشابك الكمي، وهو ما يعرف بعدم إرسال أي من المعلومات عبر هذه الشبكات وإنما يقوم بعكسها عبر الفوتونات، وبالتالي يضمن عدم تسريب أي من المعلومات والبيانات وحمايتها من السرقة[35]

سابعا : التهديدات السيبيرانية التي تواجهها الجزائر[36]

وقد أجمل "سمير بارة " أخطر التهديدات الإلكترونية التي تواجهها الدول في أربع أنواع: تعطيل الخدمة، إتلاف المعلومات أو تعديلها، التجسس على الشبكات، تدمير الأصول والمعلومات.

وفي ذات السياق كشف العميد " **تيتوش نبيل يوسف** " **رئيس** " دائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية " في تصريح لمجلة "الجيش"، التابعة لوزارة الدفاع الجزائرية، عن إحباط مصالحه لـ : مليون و 242 ألف و 801 محاولة هجوم إلكتروني، وقرصنة سنة 2022/2021 ومن مختلف مناطق العالم، إستهدفت مواقع إلكترونية جزائرية[37]، وقال قائد أركان الجيش، الفريق السعيد شنقريحة: "عرفت بلادنا الجزائر، العديد من الهجمات السيبرانية، التي استهدفت مواقع حكومية، وأخرى تابعة لمؤسسات اقتصادية وحيوية استراتيجية، وازدادت هذه الهجمات حدة وكثافة في الآونة الأخيرة، مع خروج بلادنا من أزمتها ودخولها مرحلة بناء الجزائر الجديدة"[38].

كما حذرت وزارة الدفاع الجزائرية مما سمته "خطورة مواقع وتطبيقات التواصل الاجتماعي"، وشددت على أنها باتت "**ملاذا آمنا لشبكات إجرامية منظمة**"، وكشفت عن إحباطها "جميع" الهجمات السيبرانية استهدفت مواقع حكومية وأخرى تابعة لمؤسسات اقتصادية وحيوية استراتيجية، تضاعفت بشكل كبير منذ 2021.[39]

كما يمكم إيجاز هذه التحديات في ما يلي:[40]

1- تزايد عدد المشتركين في شبكة الإنترنت ومواقع التواصل الاجتماعي في الجزائر، الذي فاق 10 ملايين مشترك سنة 2021، مما يزيد من المخاطر والتهديدات المفروضة، الأمر الذي ينعكس سلبا على عملية اكتشاف هوية مرتكبي الجرائم السيبيرانية.
2- انتشار تكنولوجيا الإنترنت فائقة السرعة، والذي يفرض تحديا أمام سرعة متابعة الجناة، والتسلح بالأجهزة والبرامج الملائمة لها.
3- الإنترنت اللاسلكي(wif,3g,4g,5g) أيضا شكل عائقا أمام محاربة الجريمة الإلكترونية
4- عمليات التخفي أثناء استعمال شبكة الإنترنت (proxy) والذي يصنف ضمن أكبر التحديات التي تواجهها أجهزة مكافحة الجريمة الإلكترونية.

5- نقص عامل التنسيق بين الدول والحكومات، نظرا لخصوصية الجريمة السيبيرانية، وسرية المعلومات التي لا يمكن كشف طبيعتها، ولا كشف البرامج التي تستخدم لحمايتها وتقاسمها مع الدول الأخرى، مما يمكن مرتكبي هذه الجرائم من النفاذ إلى أنظمة المعلومات بسهولة.

6- صعوبة تكييف القوانين الرادعة للجريمة الإلكترونية، وتفعيلها، وتطبيقها بالتزامن مع التطور الحاصل في مجال التكنولوجيا والهويات الافتراضية، والبرمجيات، والتقنيات التي تتجدد باستمرار، والاحترافية في التخفي، والبرمجيات والتقنيات التي تتجدد باستمرار، والفيروسات القادرة على التخفي أيضا.

بالإضافة إلى عوامل تشترك فيها الجزائر مع دول العالم الثالث والمتمثلة في :

- التجربة الفتية للجزائر في مجال تكنولوجيا الاتصال والمعلوماتية.
- استحواذ الدول المتقدمة على التكنولوجيا، واحتكارها للتقنيات الحديثة، مما يؤدي إلى عدم التمكن من التنبؤ بالتهديدات التي تواجهها، حيث نوه العميد " تيتوش نبيل" أن هناك " بعض الصعوبات"، والتي ربطها بتنفيذ العقود مع الشركاء الأجانب بفعل جائحة كورونا.

ثامنا : آليات تصدي الجزائر للتهديدات السيبيرانية

تولي الدولة الجزائرية مكانة كبيرة للأمن السيبيراني، ضمن الاستراتيجية الأمنية العامة للدولة، من حيث تسخير كل الإمكانية والتدابير اللازمة، التي من شأنها توفير أكبر حماية للبنية التحتية المعلوماتية، وتحقيق أمن سيبيراني مناسب للتحولات الرقمية الجارية، وعملية عصرنة قطاعات الدولة، التي تفرض تحديات كبيرة أمام تحقيق الأمن اللازم لمختلف أجهزة الدولة ومواطنيها، ويأتي ذلك بمجموع آليات وإمكانيات سخرتها الدولة، والتي أقر بها العديد من الفاعلين والمسؤولين، خاصة مسؤولي الأمن السيبيراني على مستوى جهاز الجيش الوطني الشعبي، وبعض الأشخاص المختصين في مجال الأمن والجريمة الإلكترونية، حيث كشف العميد تيتوش على مجموعة من الآليات التي عملت الجزائر على تفعيلها ومن بينها يذكر بوزنان : (http://2022https//al-ain.com/article/algeria-thwart-cyber-attack-2012 2022)

تزود مخابر "دائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية " والضباط العاملين بـ " أحدث الوسائل والأجهزة التعليمية الممتدة في مجال التكوين، من بينها محاكيات متخصصة بمعايير دولية لاستعمال واستخدام وسائل الحرب الإلكترونية"[41]

- تعزيز المدرسة العليا للإشارة بأكاديمية " سيسكو"، التي تقدم حاليا تكوين عالي المستوى في تسيير وتأمين الشبكات.
- تجهيز الدائرة العسكرية بوسائل وتجهيزات جد متطورة تستجيب للمعايير الدولية، مما يؤهلها اليوم إلى إنتاج كميات معتبرة من المعدات التي من شأنها تلبية احتياجات المستخدمين بشكل فعال.
- توفير ورشتين ميكانيكيتين مجهزتين بآلات تحكم عالية الدقة، تستخدم لتصنيع الأجزاء وقطع الغيار الميكانيكية اللازمة في مجال التصليح والصيانة .
- ومن المرتقب – بحسب المسؤول ذاته – إبرام دائرة الحرب الإلكترونية بالجيش الجزائري عقود تطوير بالشراكة مع كبرى الشركات العالمية، في مجال تكنولوجيا الإعلام والاتصال.

كما قامت الدولة الجزائرية بإنشاء عدة مؤسسات وهيئات مختصة في مجال مكافحة الجريمة الإلكترونية والإرهاب السيبيراني وهي كالآتي :[42]

1- **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني** : والذي تأسس سنة 2008، حيث عالج العديد من القضايا المتعلقة بالتهديد الإلكتروني وقضايا الاختراق والهاركز التي تؤرق أنظمة المؤسسات الأمنية والاقتصادية بالخصوص.
2- **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني ببوشاوي بالجزائر العاصمة** : والتي تختص في التحري والتحقيقات المتعلقة بالجرائم والجنح والجنايات والتي تعتمد على وسائل تقنية عالية الدقة.
3- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للأمن الوطني** : التي أنشأت سنة 2011، والتي عالجت هي أيضا الكثير من الجرائم خاصة تلك المتعلقة بوائل التواصل الاجتماعي، وبعدها تم إلحاقها لمديرية الشرطة القضائية سنة 2015، قصد التحري أكثر في الجرائم التي تهدد الأمن الوطني؛ كالتهديد وجرائم المساس بالنظام العام والاعتداء على الحياة الخاصّة للمواطن والإرهاب والجريمة الإلكترونية وقضايا تحريض القصر على الفسق والدعارة، وجرائم المساس بأنظمة المعلومات والهاكرز، إهانة هيئات نظامية ورموز الدولة والنصب والاحتيال والتحرش الجنسي ضد القصّر.
4- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:** حيث تشكلت هذه الهيأة بمقتضى المرسوم الرئاسي رقم : 261-15، وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت

إشراف ومراقبة لجنة مديرية يترأسها وزير العدل، وتضم اساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، حيث كلفت هذه الهيئة باقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للإتصالات الإلكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، وقد نص على إنشاء هذه الهيأة المادة 13 من القانون 09/04 المؤرخ في أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال إنشاء هيئة وطنية وتنظيمها وكيفيات سيرها عن طريق التنظيم.[43]

خاتمة :

من خلال ما تناولناه في هذه الورقة البحثية، فإن الأمن السيبيراني أصبح ضرورة ملحة في ضوء التطور الهائل والمتسارع في مجال تكنولوجيا الإعلام والاتصال، وخاصة في ما تعلق بأمن المعلومات سواء ما تعلق بالجانب الاقتصادي أو العسكري أو الأمني، إذ أصبح الفضاء السيبيراني وسيلة للتجسس على الدول، وخلق مشكلات إجتماعية واقتصادية وأمنية، لذلك أصبح من الضروري على بلدنا الحذو حذو الدول المتقدمة في هذا المجال وخلق فضاء سيبيراني آمن من خلال بنية تكنولوجية قوية ومتطورة خاصة في ما تعلق بالإنترنت والحاسبات كما يجب أن تعتمد في ذلك على الخبرات المحلية بغية الوصول إلى درجات عليا من السرية والأمن حفاظا على أمننا القومي ومكتسباتنا الاقتصادية والأمنية.

المراجع :

[1] - محمد عمارة ، مقومات الأمن الإجتماعي في الإسلام ، القاهرة،مصر، مكتبة الإمام البخاري ، الطبعة الأولى،2009، ص:09.
[2]- سورة النور، الآية رقم : 55.
[3] - سورة قريش، الآية : 3-4.
[4] - Thierry Balzacq, ''Qu'est-ce que la sécurité nationale?'', La revue internationale et stratégique, n°:52, hiver 2003-2004,p.36
[5] - جون بيليس، سميث ستيف، عولمة السياسة العالمية، ترجمة مركز الخليج للأبحاث، دبي، الطبعة الأولى، 2004، ص:414.
[6] - المرجع نفسه، نفس الصفحة.
[7] - سليمان عبد الله الحربي، مفهوم الأمن: مستوياتُه وصيغُهُ وتهديداتهُ، (دراسة نظرية في المفاهيم والأطر)، المجلة العربية للعلوم السياسية، العدد 19، 2008، ص:11.
[8] - إدريس عطية، مكانة الأمن السيبيراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد 01، العدد 01، ديسمبر 2019، ص: 103.
[9] - المرجع نفسه، نفس الصفحة.
[10] - نفس المرجع، نفس الصفحة.
[11] - ليلى بن برغوث، الأمن السيبيراني وحماية خصوصية البيانات الرقمية في الجزائرفي عصر التحول الرقمي والذكاء الاصطناعي، المجلة الدولية للإتصال الاجتماعي، جامعة عبد الحميد بن باديس، مستغانم، المجلد 10، العدد 01، ص: 446.
[12] - إدريس عطية، المرجع السابق، نفس الصفحة.
[13] - بارة سمير، الأمن السيبيراني في الجزائر(السياسات والمؤسسات)، المجلة الجزائرية للأمن الإنساني، العدد الرابع، جويلية 2017، ص: 257.
[14] - وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبيراني(التجربة الماليزية نموذجا)، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 23، العدد 01، 2022، ص: 161.
[15]
[16] - منى عبد الله السمحان، متطلبات تحقيق الأمن السيبيراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد 111، جويلية 2020، ص : 7.
[17] - خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبيراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد 38، جويلية 2022، ص ص : 993-994.
[18] - المرجع نفسه، ص ص: 994-995.
[19] - إدريس عطية، مرجع سابق، ص : 105.
[20] - فارس قره، الأمن السيبراني - Cyber Security، الموسوعة السياسية، نشر في: 28-08-2019، https://political-encyclopedia.org/dictionary/.
[21] - فارس قره، الأمن السيبراني، مرجع سابق.
[22] - بن علية جدو، تحديات الأمن السيبيراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، السنة السابعة، المجلد 07، العدد02، جويلية 2022، ص : 303.
[23] - نفس المرجع، ص ص:303-304.
[24] - إدريس عطية، مرجع سابق، ص: 109.
[25] - مسيكة محمد، الفضاء السيبيراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، المجلد07، العدد04، ديسمبر 2022، ص ص: 455-456.
[26] - المرجع نفسه، نفس الصفحة.
[27] - إيهاب خليفة، مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع،ط1، القاهرة، 2019، ص: 124.
[28] - مسيكة محمد، مرجع سابق، ص : 456.
[29] - ساعد بو قرص، الأمن السيبيراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، جوان 2022، ص ص: 72/73.
[30] - https://www.akhbardzair.dz/ 30-08-2021
[31] - ليلى بن برغوث، المرجع السابق، ص: 450.
[32] - المرجع نفسه، نفس الصفحة.
[33] - ليلى بن برغوث، المرجع السابق، ص: 450.
[34] - المرجع نفسه، نفس الصفحة.
[35] - صهيب الجويفل، https://mawdoo3.com/، 15 أغسطس 2023.
[36] - ليلى بن برغوث، مرجع سابق، ص: 449.
[37] - https://al-ain.com/article/algeria-thwart-cyber-attacks-2012 /الأربعاء 5/1/2022 10:27
[38] - https://al-ain.com/article/algeria-thwart-cyber-attacks-2012 /الأربعاء 5/1/2022 10:27
[39] - https://al-ain.com/article/algeria-thwart-cyber-attacks-2012 /الأربعاء 5/1/2022 10:27
[40] - ليلى بن برغوث، مرجع سابق، ص: 451.

[41] - ليلى بن برغوث، مرجع سابق، ص: 452.
[42] - سمير قلاع الضروس، الأمن السيبيراني الوطني: قراءة في أهم الاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر، مجلة الرواق للدراسات الاجتماعية والانسانية، المجلد 08، العدد 02، 2022، ص ص : 259-260.
[43] - إدريس عطية، مرجع سابق، ص : 114.