معوقات وتحديات الأمن السيبراني

Obstacles and challenges of cybersecurity

أ.بوديار عبد الحميد
جامعة سكيكدة
a.boudiar@univ-skikda

أ.ميهي وئام
جامعة تيبازة
wiam.mihi39@gmail.com

الملخص

في ظل التوجه الدولي نحو الحكومة الإلكترونية أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد التهديدات الأمنية الإلكترونية،والجزائر كغيرها من الدول سعت منذ انتهاجها للإدارة الإلكترونية حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية.

لقد أصبح الأمن المعلوماتي السيبراني ركن أساسي ضمن المنظومة الأمنية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزته كاالامن الوطني،و الدرك الوطني الجزائري باعتباره مسؤول أمني داخلي تحقيقه في ظل تنامي الجريمة الرقمية، وكذا نظرا للاستغلال المتنامي للشبكة العنكوبتية للأهداف إجرامية،والتي تؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة خاصة على المعلومات

الشخصية.

وعليه جاءت هذه الورقة البحثية لمعالجة وتحليل معوقات وتحديات الأمن السيبراني.

الكلمات المفتاحية:الانترنت،المعلوماتية،الأمن السيبراني،الجريمة الالكترونية.

Abstract

In light of the international trend towards e-government, the issue of cyber information security has become one of the major challenges at the regional and global levels, especially with the increase in electronic security threats. Algeria, like other countries, has sought since its adoption of electronic management to protect its information system through many security devices and cells.

Cyber information security has become an essential pillar within the contemporary security system, which the National Defense, through its agencies such as the National Security, and the Algerian National Gendarmerie, as an internal security official, must achieve in light of the growing digital crime, as well as in view of the growing exploitation of the spider network for criminal targets, which has a negative impact. On the safety of sensitive national information infrastructure, especially information

Personal.

Accordingly, this research paper came to address and analyze the obstacles and challenges of cybersecurity.

Keywords: Internet, informatics, cybersecurity, cybercrime.

- بيان إشكالية الدراسة:

على الرغم من الإيجابيات الهائلة التي تحققت بفضل تقنية المعلومات، فإن تلك الثورة المعلوماتية المتصاعدة قد صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام، ومن بين تلك الانعكاسات المستحدثة، ظاهرة الجريمة

الرقمية، والتي تصاعدت أخطارها بدورها مما افرز نوعًا جديدًا من الجرائم العابرة للقارات، التي لم تعد أخطارها وأثارها محصورة في نطاق دولة بعينها مما أثار بعض التحديات القانونية أمام الأجهزة المعنية بمكافحة الجريمة. وقد انتشرت في الآونة الأخيرة كلمة الأمن السيبراني، ومع سماع هذه الكلمة كثيرا من خبراء مجال أمن المعلومات ظهرت علي السطح أسئلة كثيرة منها، ما هو الأمن السيبراني و ماهي معوقات وتحديات الأمن السيبراني؟

1- نشأة الأمن السيبراني:

البداية، كانت الشبكات الإلكترونية محدودة ومستخدمة بشكل أساسي في القطاع العسكري والحكومي والأكاديمي، ومع زيادة استخدام الإنترنت وانتشاره في العالم بدأت تظهر تهديدات جديدة تتعلق بأمن المعلومات والبيانات.

في التسعينات، مع تزايد استخدام الإنترنت في الأعمال التجارية والحياة اليومية للأفراد، أصبح هناك اعتماد كبير على البنية التحتية الرقمية ونقل المعلومات الحساسة عبر الشبكات، وهذا أدى إلى زيادة التهديدات السيبرانية مثل الاختراقات الإلكترونية والاختراقات الهجومية وسرقة المعلومات والبرمجيات الخبيثة والاحتيال الإلكتروني.

مع تصاعد التهديدات السيبرانية، أصبح هناك حاجة ملحة لتطوير استراتيجيات وأدوات للحماية من هذه التهديدات، وهكذا بدأت مجالات الأمن السيبراني تتطور وتتخذ شكلًا مستقلاً ومتخصصًا.

2- مفهوم الأمن السيبراني : معنى كلمة سيبراني (cyber) تطلق كلمة سيبراني على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني يعني الفضاء الإلكتروني ،وهويعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالوتسآب، والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها (كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم (https://www.mah6at.net)/.

- يقصد كذلك بالأمن السيبراني - : حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات ويش ار إليها " ICT " وذلك اختصار and Information Communication Technologiesوالقول بالأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيا وتنظيميا وإداريا في منع الوصول غي ر المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال إتباع التدابير والإجراءات اللازمة لحماية البيانات.

أ- الأمن السيبرانى لغويا : الأمن السيبراني مكون من لفظتين :الأمن، والسيبراني الأمن :هو نقيض الخوف، أي بمعنى السلامة .والأمن مصدر الفعل أَمِن أَمناً وأَماناً وأَمنَةً :أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِن من الشر، أي سلِم منه . السيبراني :مصطلح السي برانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وكلمة" cyber" لفظة يونانية الأصل مشتقة من كلمة " kybernetes"بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم" governor". وأشار بعض المؤرخين الي أن أصلها يرجع إلى عالم

الرياضيات الأمريكي (1894-1964) Wieners Norbert وذلك للتعبير عن التحكم الآلي .

ب-الأمن السيبراني اصطلاحاً :هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يعرف بأنه" مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة ".وهذا ما ذهب إليه الكاتبان Martti Lehto ,Pekka Neittaanmäki في كتابهما Security: Analytics, Cyber Automation and Technology، حيث عرفا الأمن السيبراني أنه:عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصـ نة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة . بينما عرفه إدوارد أمورسو Edward Amoroso بأنه" وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة ....وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010-2011 عرف الأمن السيبراني بأنه :مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة ا لمخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين .وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني فاعتبرته جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكا لها المادية والإلكترونية، من مختلف الجرائم : الهجمات، التخريب، التجسس والحوادث . في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات ".وتجدر الإشارة إلى أن الأمن

السيبراني مفهوم أوسع مـ ن أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية " الورقية"، بينما لا يهتم الأمن السيبراني بذلك. (الموسوعة السياسية political://https-encyclopedia.org/dictionary/)

3- **أهداف الأمن السيبراني:** (net.as7ab://https) :

3-$_1$- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.

3-$_2$- التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

3-$_4$- توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.

3-$_5$- صمود البني التحتية الحساسة للهجمات الإلكترونية.

3-$_6$- توفير المتطلبات الأزمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.

3-$_7$- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.

3-$_8$- سد الثغرات في أنظمة امن المعلومات.

3-$_9$- مقاومة البرمجيات الخبيثة، ما تستهدفه من أحداث أضرار بالغة للمستخدمين

3-$_{10}$- حد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

3-$_{11}$- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

3-12- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة .

4- أهمية الأمن السيبراني : وتتمثل أهمية الأمن السيبراني فيما يلى :

4-1- الحفاظ على المع لومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها.

4-2- تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها .

4-3 -حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات .

4-5- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

4-6- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيِق مبادئ الأمن السيبراني.

4-7- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية

5- أهمية دراسة الأمن السيبراني : من أبرزها :

1- يشهد سوق العمل حاجة مستمرة لخبراء مجال الأمن السيبراني .

2- بالعمل في مجال الأمن السيبراني يمكن جني الكثير من الأرباح المالية .

3- الخبرة في مجال الأمن السيبراني ستكون غاية لكل مؤسسة مميزة.

4- يشمل الأمن السيبراني كافة المجالات العملية بالرغم من اختلافها وتنوعها .

5- تمكين الدارس من الحصول علي امتيازات فريدة في العمل.

6- أنواع الجرائم السيبرانية : تتعدد جرائم الأمن السيبراني ، من أهم هذه الجرائم : جرائم التعدي على البيانات المعلوماتية ، التعدي على الأنظمة المعلوماتية، إساءة استعمال الأجهزة أو البرامج ا لمعلوماتية، الجرائم الواقعة على الأموال ،الاستغلال الجنسي للقاصرات، التعدي على الملكية الفكرية للأعمال الرقمية، البطاقات

المصرفية والنقود الإلكترونية، جرائم تمس المعلومات الشخصية، جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، جرائم المقامرة وترو يج المواد المخدرة بوسائل معلوماتية عبر الإنترنت، الجرائم المعلوماتية ضد الدولة والسلامة العامة، وجرائم تشفير المعلومات(net.as7ab://https) .

7- أسباب الجرائم السيبرانية:

1 - الرغبة في جمع المعلومات وتعلمها .

2- الاستيلاء على المعلومات والاتجار فيها .

3- قهر النظام وإثبات التفوق على تطور وسائل التقنية.

4- إلحاق الأذى بأشخاص أو جهات.

5- تحقيق أرباح ومكاسب مادية.

6- تهديد الأمن القومي والعسكري.

8- أبعاد الأمن السيبراني (https://ab7as.net) :

-أولا: الأبعاد العسكرية :تنشا أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشاة النووية، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي إلى كوارث .

-ثانيا: الأبعاد السياسية :تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار امن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها .

– ثالثا: الأبعاد الاقتصادية :يرتبط الأمن السيبراني ارتباطا وثيقا بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة فاغلب الدول تعتمد في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة والمعلومات على المستويات، مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية .

– رابعا: الأبعاد القانونية :ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومن ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية المجتمعات وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد ويقوم الأمن السيبراني في هذا البعد على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات آليات (متطلبات).

9 – آليات تحقيق الأمن السيبراني:https://www.arageek.com/)

قد تساعدك الخطوات البسيطة أدناه في الحفاظ على مستوى جيد من الأمان والسلامة السيبرانية:

– الموثوقية : وتعني استخدام المواقع الموثوق بها عند تقديم معلو مات شخصية، والقاعدة الأساسية هي التحقق من عنوان URL.، وإذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أما إذا كان عنوان URL يحتوي على http بدونs، فيجنّب الحذر من إدخال أي معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي.....الخ.

–البريد الاحتيالي : ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة، إذ إن إحدى الطرق الأكثر شيوعا التي

يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها مرسلة من شخص موثوق به .

- التحديثات(Always up-to-date)وتعني الحرص دائما على تحديث الأجهزة ، فغالبا ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإن هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.

- النسخ الاحتياطي : ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام لمنع هجمات الأمان على الإنترنت.

10- عوائق تحقيق الأمن السيبراني في ظل التحديات الآنية والمستقبلية:

❖ انتشار تكنولوجيا الانترنت فائق السرعة: تسهم التكنولوجيا المتطورة في سرعة انجاز الجريمة، وهذا يضع الجهات الامنية المختصة أمام تحدي سرعة مباشرة التحقيقات ومتابعة الجناة، والتسلح بالأجهزة المتطورة والبرامج الحديثة السريعة الخدمة.

❖ التطور التكنولوجي وظهور الانترنت اللاسلكي: عبر هذه التقنيات لم يعد المجرم يحتاج للجلوس وراء الحواسيب الموصولة سلكيا بشبكة الانترنت، للقيام بجريمته، مما يستدعي من الجهات الأمنية رفع التحدي، والاستعداد بأحدث التقنيات لمواجهة والتصدي لهذه التطورات.

❖ عمليات التخفي أثناء استعمال خدمات شبكة الانترنت: وهي من أكبر الاشكاليات التي تواجهها الجهات المختصة بالتحقيق، ويتطلب تعاون جهات متعددة، والتسلح بالوسائل المتطورة التي يمكن لها رصد الجزئيات وفك الشفرات، وتطوير البنى التحتية الخاصة بالمعلومات وتحديثها باستمرار، وتصميم برامج عالية التطور.

❖ غياب التنسيق بين الدول والحكومات: اذ ان المعلوم ان الجريمة الالكترونية عابرة للحدود والقارات، وهو ما يعني ان مرتكبيها يمكنهم النفاذ الى أنظمة الحاسوب في أحد الدول، ليتم التلاعب واختراق البيانات في بلد آخر، تسجل النتائج في بلد ثالث، ناهيك عن أنه من الممكن تخزين أدلة الجريمة الالكترونية في حاسوب موجود في بلد آخر غير الذي ارتكبت فيه الجريمة، وكل هذا يساعد المجرم الالكتروني في اخفاء هويته ونقل المواد من خلال قنوات موجودة في بلدان مختلفة.

11- تحليل المخاطر التي تعترض الدول العربية:

تتمحور أهم المخاطر المحدقة بالأمن السيبراني في المنطقة العربية خاصة على المستوى القانوني والمؤسساتي حول النقاط التالية:

- ❖ عدم اعتماد العديد من الدول العربية استراتيجية وطنية للامن السيبراني.
- ❖ عدم اعتماد الدول العربية لتشريع خاص بالأمن السيبراني.
- ❖ تبعثر التشريعات المتعلقة بالأمن السيبراني والجرائم السيبرانية بين عدة قوانين وغياب قانون موحد في الغرض يسهل الرجوع الى أحكامه.
- ❖ تعدد الهياكل المعنية بالأمن السيبراني مما خلق صعوبات على مستوى تحديد مجالات تدخل كل واحد منها وعلى مستوى التنسيق بينها.
- ❖ عدم ملائمة بعض التشريعات المتعلقة بالأمن السيبراني لخصوصيات وتحديات الفضاء الرقمي.
- ❖ بقاء العديد من القوانين المتعلقة بالأمن السيبراني دون نفاذ لغياب النصوص الترتيبية اللازمة لتحقيقها.(والمعلومات، 2021، صفحة 18).

12-أسباب الارهاب السيبراني:

1. انخفاض تكلفة الآليات الالكترونية مقارنة بالادوات التي تستخدم بالارهاب التقليدي في الارهاب السيبراني يحتاج الارهابي جهاز الالكتروني وخط انترنت، اما الارهاب التقليدي يحتاج شقة أماكن تداريب وسيارات...الخ.

2. غياب السيطرة والرقابة على الشبكة المعلوماتية من أهم اسباب انتشار الارهاب السيبراني.
3. ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق، وهذا بطبيعة الحال يوفر للإرهابيين طريقا لتحقيق أهدافهم بسهولة.
4. غياب الحدود الجغرافية في الفضاء الالكتروني يعد فرصة مناسبة للإرهابيين.(صفوت، الصفحات 35-36).

13- توصيات:

- إدراج مجال الفضاء السيبراني ضمن مناهج التعليم .
- تشجيع بحوث ودراسات الأمن السيبراني في الدراسات الجامعة.
- تشجيع مجالات البحث العلمي والابتكار في مجال الأمن السيبراني.
- توعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية الاحترافية لديهم وإرساء بنية تحتية للدخول إلي مجال صناعة البرمجيات العالمية والقدرة علي منافسة المنتج المستورد .
- تشجيع مؤسسات المجتمع المدني والتأكيد علي دورها الفعال في التعامل مع الاستخدام غير الآمن لتكنولوجيا المعلومات، وذلك من خلال الأنشطة العلمية ونشر ثقافة الاستخدام الآمن لشبكة الانترنت والتطبيقات الرقمية الحديثة.
- تشجيع الاستثمار في مجال الأمن السيبراني وينقسم الاستثمار لجانبين، الأول توطين التكنولوجيا والبني التحتية السيبرانية، الثاني تطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة علي بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها.
- إجراء مزيد من الدراسات العلمية حول قضية أمن المعلومات بمختلف مؤسسات المملكة عامة ، ومجال التعليم بشكل خاص -عقد دورات تدريبية مستمرة للعاملين في مجال المعلومات.

- خاتمة :

يجب القول على أن الأمن السيبراني له أهمية بالغة في عالم تكنولوجيا المعلومات الحالي، فقد تطورت أساليب الهجمات السيبرانية بشكل كبير، مما يشكل تهديدًا جديًا على الأفراد والشركات والمؤسسات.

ومن خلال تحقيق الأمن السيبراني، يتم حماية البيانات والشبكات والأنظمة من الاختراق والاستغلال غير القانوني، وتعتبر اتخاذ سياسات أمنية قوية وتوظيف التكنولوجيا المتقدمة مثل تحليل الضوابط وانترنت الأشياء والتعرف على السياق واسعة النطاق، ضرورةً ملحّة لمكافحة التهديدات السيبرانية.

كما تُعزز الوعي والتدريب في مجال الأمان السيبراني قدرة الأفراد والمؤسسات على التعامل مع التحديات الأمنية الرقمية بفعالية.

- المراجع :

– أبو زيد ، عبد الرحمن عاطف (2019) الأمن السيبراني في الوطن العربي ،دراسة حالة المملكة العربية السعودية المركز العربي للبحوث والدراسات علي الموقع بتاريخ 6/4/2020http://www.acrseg.org/list.aspx?r=24734 :

– البكري ، يوسف الشيخ (2018) أمن المعلومات بالمكتبات الجامعية السودانية بالإشارة إلي مكتبتي جامعة النيلين وجامعة وادي النيل، في المؤتمر الثالث والعشرون لجمعية المكتبات الخاصة، قطر 30 أحمد عيسى : بوابة أخبار اليوم العدد الأسبوعي الأربعاء، 18 سبتمبر 2019.

–الشيتي، إيناس ابراهيم (2019) تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربي السعودية دراسة تطبيقية علي جامعة القصيم ، ماجستير غير منشورة، جامعة القصيم .

–العتيبي،عبد الرحمن بن بجاد (2018) دور الأمن السيبراني في تعزيز الأمن الإنساني أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية .

. https://akhbarelyom.com/news/newdetails-

-محمود عزت، (٢٠١٨) الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية العدد 498 .

-الهيئة الوطنية للأمن السيبراني : المملكة علي الموقع https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

- الموسوعة السياسية بتاريخ 6/4/2020 علي الموقع https://political-encyclopedia.org/dictionary/٢٩ .

المعهد العربي للتخطيط (2019) مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي علي الموقع https://www.researchgate.net/institution/Arab_Planning_Institute2 9.

- El Hissi, Y.& Arezki, S.(2018).Conceptualization of an Information System Governance Model Dedicated to the Governance of Scientific Research in Moroccan University,2018 4 th International Conference on Computer and Technology Applications.

- https://ab7as.net - https://www.arageek.com/ What is Cyber-Security?، موقع من: usa.kaspersky.com 2019 ، بتـاريخ عليه اطّلع.

- Ivanov Anton, Orkhan Mamedov. The Return of Mamba Ransomware Secure list - Information about Viruses, Hackers and Spam. N.p., 09 Aug. 2017. Web. 13 Sept. 2017 - ------https://securelist.com/thereturn-ofmamba-ransomware/79403 (https://www.easyunime.com/advice/) 2019

- Rehman, H.,Masood ,A.& Cheema ,A.(2013). Information Security Management in Academic Institutes of Pakistan,2 nd .National Conference of Information Assurance(NCIA)

-What is cyber security? What you need to know، موقع من: us.norton.com . اطّلع عليه بتاريخ2019.