التهديدات السيبرانية وتأثيرها على الامن القومي الجزائري

Cyber threats and their impact on Algerian national security

تاريخ استلام المقال: 2022/03/31 تاريخ قبول المقال للنشر: 2022/07/04 تاريخ نشر المقال: 2022/12/31

د/ عبدالله جعفري

– جامعة احمد دراية، ادرار – (الجزائر) ، djaafriabdellah@univ_adrar.edu.dz

ملخص:

يعتبر موضوع الامن السيبراني والتهديدات المصاحبة له من اهم المواضيع الجديرة بالدراسة والتحليل في واقعنا اليوم نظرا للمخاطر التي اضحت تنشرها في مختلف المجالات والميادين وعلى رأسها الامن القومي الذي يعتبر الركيزة الاساسية لسلامة وامن المجتمعات لذلك سارعت العديد من الدول ومن بينها الجزائر الى تعزيز امنها القومي امام كافة المخاطر والتهديدات التي تخترق القواعد البيانية حفاظا على سلامة وامن معلوماتها، معتمدة في ذلك على العديد من الاليات والاستراتيجيات الدفاعية من خلال استحداث العديد من المصالح الامنية ذات الصلة والعلاقة بمحاربة التهديدات والجرائم السيبرانية في كافة المجالات اضافة الى الجانب القانوني التشريعي والجانب التحسيسي التوعوي بمخاطر الاستخدام غير الامثل لتكنولوجيا الاعلام والاتصال.

الكلمات المفتاحية باللغة العربية: الامن السيبراني، التهديدات السيبرانية ، الامن القومي.

Abstract:

Cybersecurity as well as its threats is considered as a crucial issue to study .This is due to the risks as well as threats that spread in various fields, especially national security, which is the main pillar of safety and security of societies. Therefore, many countries, including Algeria, tended to strengthen their national security facing risks and threats that penetrate the databases in order to preserve the safety and security of their information. Hence, various defense mechanisms and strategies are employed by security systems through the creation of various relevant security segments to evade cyber threats in all the fields, in addition to the legislative law as well as the awareness-raising aspect of the risks of improper use of Information and Communication Technology.

Keywords: word ; cyber security, cyber threats, national security.

مقدمة:

شهد العالم في السنوات والعقود الماضية تطورا هائلا عرفته تكنولوجيا الاعلام والاتصال بمختلف اشكالها ومجالاتها، فقد ساهمت في تقديم خدمات راقية وعالية الدقة في مختلف ميادين الحياة السياسية والاقتصادية والاجتماعية والثقافية والرياضية وغيرها، ناهيك عن اختزالها للوقت والزمن والجهد، ما جعل المواطن والفرد داخل المجتمع لا يستغني عنها وعن خدماتها نتيجة الاستخدام السهل لها، الا انها اصبحت في الوقت الراهن تشكل خطرا جسيما على امن الافراد والمجتمعات وكذا الامن القومي للدول نتيجة الاستخدام الغير الامثل لتكنولوجيا الاعلام والاتصال ، وهو ما يشهده العالم في الآونة الاخيرة جراء التصاعد المستمر لمختلف التهديدات السيبرانية وفي مختلف المجالات، ما جعل الدول والحكومات تعيد النظر في سياساتها الامنية والدفاعية بهدف تعزيز امنها القومي، والجزائر واحدة من الدول والانظمة

السياسية في العالم التي لم تسلم من هاته التهديدات وبشكل متزايد في مختلف مجالات الحياة، الامر الذي جعل النخب الحاكمة والامنية على حد سواء في التفكير في الاستراتيجيات المعتمدة في تعزيز الامن القومي من مختلف التهديدات السيبرانية، وهو ما سنحاول التطرق اليه من خلال هاته الدراسية.

الاشكالية: **ما مدى تأثير التهديدات السيبرانية على الامن القومي؟ وماهي الاليات الجزائرية المعتمدة في الحد من هاته التهديدات؟**

وتتفرع من هاته الاشكالية التساؤلات الفرعية التالية:

ما المقصود بالأمن القومي والامن السيبراني؟

ماهي اشكال التهديدات السيبرانية؟

كيف تؤثر التهديدات السيبرانية على الامن القومي؟

ما هي استراتيجية الجزائر في مواجهة التهديدات السيبرانية؟

الفرضية الرئيسية: للإجابة على الاشكالية الرئيسية اقترحنا الفرضية التالية: ارتبطت الاستراتيجية الجزائرية في تعزيز امنها القومي من التهديدات السيبرانية على المقاربة الدفاعية

اهمية الدراسة:

تنبع أهمية أي دراسة من المتغيرات التي تنطوي عليها وكذا مدى حاجة المجتمع لها ومدى تميزها عن غيرها الدراسات ، وتبرز أهمية الدراسة التي بين أيدينا كونها تقف على دراسة وتحليل تأثير التهديدات السيبرانية على الامن القومي وكذا استراتيجية الجزائر في مواجهة التهديدات السيبرانية علاوة على ذلك تقف الدراسة على واقع التهديدات السيبرانية وما تطرحه من مخاطر على امن الافراد والدول.

المنهج المعتمد

المنهج الوصفي التحليلي: يستخدم المنهج الوصفي في دراسة الاوضاع الراهنة للظواهر من حيث خصائصها واشكالها وعلاقاتها والعوامل المؤثرة في ذلك، وهو ما يعني ان المنهج الوصفي يقوم على رصد ومتابعة دقيقة لظاهرة معينة بطريقة كمية او نوعية خلال فترة زمنية معينة من اجل التعرف على الظاهرة او الحدث من حيث المحتوى والمضمون والوصول الى نتائج وتعميمات تساعد في فهم الواقع

المجلة الأفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، ادرار – الجزائر ISSN:2572-0082
المجلد: 06 ، العدد: 02، السنة: 2022 EISSN: 2710-804X

وتطويره[1]، وقد استخدمنا هذا المنهج من اجل تحليل طبيعة العلاقة بين التهديدات السيبرانية والامن القومي تحليلا يستند على الاستراتيجيات المعتمدة للحد منها ومن تأثيراتها المتزايدة على الامن القومي.

منهج دراسة الحالة: هو المنهج الذي يتجه إلى جمع البيانات العلمية المتعلقة بأية وحدة سواء كانت فردا أو مؤسسة أو نظاما اجتماعيا أو مجتمعا محليا وهو يقوم على أساس التعمق في دراسة مرحلة معينة من تاريخ الوحدة أو دراسة مرحلة معينة من تاريخ الوحدة أو دراسة جميع المراحل التي مرت بها وذلك بقصد الوصول إلى تعميمات علمية متعلقة بالوحدة المدروسة وبغيرها من الوحدات المشابهة لها. واخترنا هذا المنهج من أجل دراسة الحالات التي بين أيدينا، والمتمثلة أساسا في النظام السياسي الجزائري.

تقسيم الدراسة: للإحاطة بالموضوع الذي بين ايدينا قسمنا الدراسة الى المحاور التالية:

المحور الاول: مدخل مفاهيمي لمفهوم الامن القومي والتهديدات السيبرانية

المحور الثاني: تأثير التهديدات السيبرانية على الامن القومي

المحور الثالث: جهور الجزائر في مواجهة التهديدات والجرائم السيبراني

***

المحور الاول: مدخل مفاهيمي لمفهوم التهديدات السيبرانية والامن القومي

يعتبر موضوع الامن من المواضيع ذات الاهمية الكبيرة في حياة الافراد والجماعات نظرا لارتباطه بالعديد من الابعاد والمتغيرات التي من بينها القومي والسيبراني وهو ما سنحاول التعريف به من خلال هذا المحور.

اولا: مفهوم الامن:

لغويا الامن من آمن يأمن أمنا، فهو آمن، وآمن أمنا وأمانا، اطمأن ولم يخف، فهو آمن وأمن وامين، والامن يعني الاستقرار والاطمئنان، نقول أمن منه اي سلم منه، وامن على ماله عند فلان اي جعله في ضمانه، والأمان والأمانة بمعنى واحد، فالأمن نقيض الخوف والأمانة ضد الخيانة والمأمن موضع الامن.[2]

ومفهوم الامن يعد من المفاهيم اللغوية ذات الثراء في المعنى ومن ذلك قد يقصد بالأمن عدم الخوف، فالأمن والامان والامانة والمنة نقيض الخوف لذلك يقال امن فلان يأمن امنا وامنا اذا لم يخف

---

[1] – ربحي مصطفى عليان، عثمان محمد غنيم، مناهج واساليب البحث العلمي النظرية والتطبيق، ط.1، عمان، دار صفاء للنشر والتوزيع، 2000، ص.42.41.

[2]– ابن منظور، لسان العرب، ج1، ط1، بيروت، دار صادر، 2000، ص163.

وقد امنته ضد اخفته، وقد يقصد بالأمن ايضا التصديق فاصل الايمان التصديق وهو مصدر امن يؤمن ايمانا فهو مؤمن فالإيمان معناه التصديق، وقد يقصد بالأمن كذلك الحفظ فقد قيل ان الامنة وهي جمع امين وهم الحفظة واصل الحفظ الامن من خوف الضياع، ويقصد بالأمن الطمأنينة فالرجل الامنة هو من يطمئن الى كل واحد ويثق بكل واحد ويقصد بالأمن عدم الخيانة فالأمين هو المؤتمن وهو الذي لا يخون فيقال امنته على كذا، ويقصد بالأمن ايضا الثقة فمؤتمن القوم هو الذي يثقون فيه ويتخذونه امينا، ويشير مفهوم الامن كذلك الى الاجارة وطلب الحماية واستأمن اليه اي اتجاره وطب حمايته والسلم فيقال أمن فيه اي سلم.[1]

فمفهوم الامن في اللغة العربية يحمل العديد من الدلات والمقاصد ولا يقتصر المفهوم على اتجاه او بعد واحد وهو من محاسن لغة العرب ان اعطت للمفهوم الواحد العديد من الابعاد والاتجاهات فقد يقصد به الامن وعدم الخوف والثقة والاجارة وعدم الخيانة والسلم وكلها معاني تدخل بشكل او باخر تحت مفهوم الامن.

اما في اللغة الاجنبية فهو مرادف للكلمة الانجليزية Securityوالفرنسية Sécurité ويكاد يتطابق المفهوم في كافة المعاجم اللغوية حيث يعتمد على مبدأ تحقيق الطمأنينة وعدم الخوف[2].

اما اصطلاحا: فالأمن هو مجموعة التدابير الكفيلة بحفظ النظام وضبط العلاقات بين الافراد، وهو عكس التهديد في كل الجوانب السياسية والاقتصادية والاجتماعية سواء كانت داخلية او خارجية، وان تكون امنا بمعنى ان تكون سليما من الاذى اي الحاجة الى الاحساس بالأمن كقيمة انسانية وشرط مسبق للعيش بشكل محترم.[3]

والامن هو الادراك الذاتي للفرد او الجماعية الانسانية باختلاف صورها بالطمأنينة والاستقرار والسكينة والبعد عن الاخطار والمخاطر وعن كل ما يهدد الفرد في نفسه وجسده وعرضه وماله وما يهدد المجتمع في استقراره ونمائه وتقدمه.[4]

[1]– مصطفى محمود منجود، الابعاد السياسية لمفهوم الامن في الاسلام، القاهرة، المعهد العالمي للفكر الاسلامي، 1996، ص.30 31

[2]– تباني وهيبة، الامن المتوسطي في استراتيجية الحلف الاطلسي دراسة حالة: ظاهرة الارهاب مذكرة ماجستير في العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2014، ص.19

[3]– مارتن غريفيش، تيري اوكالاهان، المفاهيم الاساسية في العلاقات الدولية، دبي، مركز الخليج للأبحاث، 2008، ص.78

[4]– سعاد بيطاط، الامن دراسة في الحديث الموضوعي، عمان، مركز الكتاب الاكاديمي، 2015، ص54.

ثانيا مفهوم الامن القومي:

تطرقنا في ما سبق الى ان مفهوم الامن من المفاهيم التي يصعب تحديد مفهوم دقيق لها وذلك لارتباطها بالعديد من الاتجاهات والمجالات والابعاد سواء اقتصادية او اجتماعية او إنسانية او بيئية وغيرها، ومن بين مجالات الامن نجد الامن القومي الذي يرتبط ارتباطا وثيقا بكيان الدولة ومصالحها لذلك سنعرج على اهم التعريفات التي سيقت لمفهوم الامن القومي ومن ذلك نجد:

ان الدكتور علاء الدين هلال عرف الامن القومي باعتباره تأمين كيان الدول ضد الاخطار التي تهددها داخليا وخارجيا وتأمين مصالحها وتهيئة الظروف المناسبة لتحقيق اهدافها وغاياتها القومية.[1]

كما ذهب الاستاذ حامد ربيع الى تعريف الامن القومي في جوهره انه مفهوم عسكري ينبع من خصائص الاوضاع الدفاعية للإقليم القومي، فالأستاذ حامد ربيع ربط في تعريفه بين الامن القومي والدفاع العسكري عن الاقليم القومي باعتبار ان الدفاعات العسكرية تساهم بشكل او بأخر في تعزيز الامن القومي من اي مخاطر خارجية قد تضرب المصالح الحيوية للدولة والنظام السياسي[2].

في حين ذهب البرفسور "فيري" الى تعريفه للأمن القومي هو حالة من الهدوء وغياب عوامل الخوف والقلق عند قيام الدولة بتحقيق اهدافها القومية[3]، فقد عالج هذا التعريف الامن القومي من واوية الاستقرار السياسي والاقتصادي والاجتماعي للدولة والذي يعتبر احد عوامل الامن داخل الدولة وهو ما يساهم بشكل كبير في تحقيق الأهداف القومية للدولة سواء على الصعيد الداخلي او الخارجي

كما يرى "نيكولاس سبيكمان" الامن القومي بانه حماية استقلال الدولة وسيادتها والدفاع عن اقليمها ضد اي عدوان قد يهددها او يهدد وجودها مع الحفاظ على كرامتها الوطنية[4].

---

[1]– ثامر كامل الخزرجي، العلاقات السياسية الدولية واستراتيجية ادارة الازمات، ط.01، عمان، دار مجدلاوي للنشر والتوزيع، 2009، ص.67.

[2]– محمد طالب حميد، العلاقات الايرانية الامريكية توافق ام تقاطع، ط.01، القاهرة، العربي للنشر والتوزيع، 2016، ص.23.

[3]– عبدالرزاق الدليمي، الدعاية والشائعات رؤية معاصرة، الاردن، دار اليازوري العلمية للنشر والتوزيع، 2019، ص.144.

[4] –spykman; Nicholas J1944. The Geography of the peace . Hqrcourt Brqce and compqny. New york في فرج عصام بن جليل واخران، اثر التحديات الداخلية والخارجية على الامن القومي العربي: الواقع وافاق المستقبل، مجلة علوم الانسان والمجتمع، المجلد 10، العدد03، 2021، ص.128.

ثالثا: مفهوم الامن السيبراني

كلمة الامن في الفضاء الالكتروني تعني اجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيء لتكنولوجيا الاتصال والمعلومات[1].

ويعني مجموع الاجراءات الواجب اتخاذها من قبل الاجهزة الامنية للمحافظة على سرية المعلومات الالكترونية ومنع الاختراقات الفيروسية من اجل ضمان وصولها الى الجهات المختصة وفي الوقت المناسب وضمان عدم وقوعها في ايدي الاعداء او الاصدقاء على حد سواء خصوصا بعد الثورة الهائلة في عالم الاتصالات[2].

ويمكن تعريف الامن السيبراني بانه مجموع الاطر القانونية والتنظيمية التي تهدف الى حماية الفضاء السيبراني الوطني والدولي مع التركيز على ضمان توافر انظمة المعلومات وتمتين الخصوصية وحماية سر المعلومات الشخصية واتخاذ جميع الاجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني[3].

كما عرفته وكالة الامن القومي في الولايات المتحدة الامريكية بانه يعني المعايير والاجراءات المتخذة لمنع وصول المعلومات الى ايدي اشخاص غير مخولين بها عبر الاتصالات ولضمان اصالة وصحة هذه الاتصالات[4].

اضافة الى تعريف وكالة الامن القومي في الولايات المتحدة الأمريكية فقد عرفته المنظمة الدولية للاتحاد الدولي للاتصالات بمجموع الادوات والسياسات والمفاهيم الامنية والضمانات الامنية والمبادئ التوجيهية والتقنيات التي يمكن استخدامها لحماية البيئة الالكترونية وتنظيم اصول المستخدم حيث تشمل توصيل اجهزة الحوسبة والموظفين والبنية التحتية والخدمات ونظم الاتصالات السلكية واللاسلكية ومجمل المعلومات المرسلة او المخزنة في البيئة الالكترونية"[5]

---

1 عادل عبدالصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، ط.02، القاهرة، المركز العربي لابحاث الفضاء الالكتروني، 2016، ص.13.

2– علي زياد العلي، المرتكزات النظرية في السياسة الدولية، القاهرة، دار الفجر للنشر والتوزيع، 2017، ص.224.

3– علي زياد العلي، نفس المرجع، ص.226.

4– عادل عبدالصادق، المرجع السابق، ص.15.

5– كريم رقولي، اخضر نويوة ، الامن السيبراني المتوسطي بين الواقع والرهانات الامنية، مجلة طبنة للدراسات العلمية والاكاديمية، المركز الجامعي بريكة، المجلد 02، العدد.02، ديسمبر 2019، ص72

انطلاقا من التعاريف السابقة يمكن تعريف الامن السيبراني بانه احد مجالات الامن التي تعتمدها الدول والحكومات، بهدف حماية انظمتها المعلوماتية والبرامج والبيانات والشبكات والاجهزة وكل اشكال التعامل الالكتروني من الهجمات والتهديدات الالكترونية الفعلية او المحتملة، وذلك بهدف ضمان السير الحسن للنظام الالكتروني والخدمات التي يقدمها في تعاملاته داخل الدولة او خارجها.

اما التهديدات السيبرانية: فيقصد بها يقصد بالتهديدات السيبرانية تلك الهجمات والمخاطر التي تتم باستخدام اليات وشبكات الانترنت واجهزة الحاسوب الالي، وتهدف الى الحاق الضرر بالأجهزة والشبكات الالكترونية ذات الاتصال بالأنترنت، حيث تتباين التهديدات السيبرانية وتختلف من دولة الى اخرى بتطور وهيمنة التطور التكنولوجي.

ويمكن تعريفها بانها فعل يقوض من قدرات وظائف شبكة الكمبيوتر لغرض قومي او سياسي من خلال استغلال نقطة ما يمكن للمهاجم من التلاعب بالنظام، كما تعرف بانها هجوم عبر الفضاء الالكتروني يهدف الى السيطرة على مواقع الكترونية لتعطيلها او تدميرها او الاضرار بها"[1]

وقد عرفتها القيادة الاستراتيجية الأمريكية بانها تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعال لها، فضلا عن التسلل الى انظمة المعلومات وشبكات الاتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها.[2]

لذلك تعتبر التهديدات السيبرانية احد الاشكال الحديثة للتهديدات الامنية باعتبارها مرتبطة ارتباطا وثيقا بأنظمة المعلومات وشبكات الاتصال، وهي بذلك نتاج التطور التكنولوجي الذي وصلت اليه تكنولوجيا الاعلام والاتصال بمختلف اشكالها وانواعها، لذلك التهديدات السيبرانية اضحت تهدد امن وسلامة المعلومات سواء على الصعيد الشخصي او حتى على صعيد الانظمة السياسية والاجتماعية في العالم بأشكال مختلفة يمكن ايجازها في النقاط التالية:

- الحرمان من الخدمة
- التجسس السيبراني
- الارهاب السيبراني

[1]– احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ، كلية القانون، جامعة بابل، العدد 04، 2016، ص.614.

[2] – بن صابر بلقاسم، حيدرة محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الانسان والحريات العامة، جامعة مستغانم، المجلد.02، العدد04، جوان 2017، ص.189

المجلة الأفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، ادرار– الجزائر ISSN:2572-0082
المجلد: 06 ، العدد: 02، السنة: 2022 EISSN: 2710-804X

- سرقة المعلومات والبيانات العسكرية
- تزييف المعلومات واتلافها او تدميرها الكترونيا

وغيرها من الاشكال المصاحبة للتهديدات السيبرانية

المحور الثاني: التهديدات السيبرانية وتأثيرها على الامن القومي

بينا في المحور الاول من هاته الورقة البحثية اهم التعاريف لمتغيرات الدراسة التي بين ايدينا وسنحاول في هذا المحور التطرق الى العلاقة الارتباطية بين التهديدات السيبرانية والامن القومي، وكيف تؤثر التهديدات السيبرانية على الامن القومي.

فقد صاحب التطور التكنولوجيا لتكنولوجيا الاعلام والاتصال تصاعد وتزايد المخاطر والتهديدات السيبرانية على الامن القومي للدول والتي من بينها الجزائر، وذلك من خلال الاشكال المتعددة للتهديدات والتي من بينها:

1- الحرمان من الخدمة: وهو ذلك الهجوم الذي يهدف الى ايقاف قدرة الهدف على تقديم الخدمات المعتادة او المفترض تقديمها، وذلك عن طريق اغراق جهاز الحاسب الالي المقدم للخدمة بكم هائل من الاوامر تؤدي الى توقفه عن العمل، وذلك عن طريق اختراق الاجهزة الالكترونية للخصم وتحميل برامج عليها ليتم استخدامها لاحقا في شن هجوم على الخصم بشكل متزامن من خلال ارسال اشارة بدء الى هذه البرامج الموجودة على كافة الاجهزة التي تم اختراقها، حيث لا يستوجب ان يكون اصحاب الحواسيب المخترقة على علم بذلك، كما يلاحظ ان الاجهزة المخترقة قد تتواجد في منطقة بالعالم ولا يشترط ان ترتبط كلها بنطاق مكاني معين، ويشار الى هاته الاجهزة التي تمت مهاجمتها بالاكواد والبرامج الخبيثة بعدد من المصطلحات ابرزها zombies او Bots.[1]

2- التجسس السيبراني: وتعتبر هاته الجريمة من اخطر التهديدات السيبرانية فهي نتاج اسفر عنه التقدم العلمي والتكنولوجي الحديث في شأن اجهزة التنصت الحديثة ذات القدرة الفائقة، حيث تهدف الى جمع المعلومات العسكرية او السياسية او حتى جمع المعلومات غير العسكرية كجمع تلك المتعلقة بالمجال الاقتصادي والتجاري، فالتجسس قد يهدف الى تعطيل عمل الشبكات العنكبوتية وحواسيبها وانظمتها بهدف سرقة معلومات سرية سياسية او عسكرية او مالية من دولة ونقلها الى اخرى، فالتجسس السيبراني

[1]- نوران شفيق، "اشكال التهديدات الالكترونية ومصادرها"، المركز الاوربي لدراسات ومكافحة الارهاب والاستخبارات، المانيا وهولندا على الموقع الالكتروني: https://www.europarabct.com/%D8%A3%D8%B4% بتاريخ 29 يناير 2020، تم الاطلاع عليه بتاريخ 2022/02/28، على الساعة 14:56.

تعتبر من الاساليب التي تلجأ اليها التنظيمات الاجرامية والارهابية لجمع معلومات حول المؤسسات والقطاعات الحكومية ليتم استخدامها من اجل الاضرار بالمجتمع ومصالحه.[1] .

3-الارهاب السيبراني: وهو استخدام شبكات المعلومات والكمبيوتر من اجل التخويف والارغام لتحقيق اهداف سياسية، حيث تقوم الجماعات الارهابية بالتهديد عبر وسائل الاتصالات من خلال الشبكة العالمية للمعلومات وتتعد اساليب التهديد وتتنوع طرقه وذلك من اجل نشر الخوف والرعب بين الاشخاص والدول والشعوب، ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الارهابية من ناحية، ومن اجل الحصول على التمويل المالي او ابراز قوة التنظيم الارهابي من ناحية اخرى، فالإرهاب السيبراني يشمل اي نشاط يتم من خلال شبكة الانترنت بهدف بث الافكار المتطرفة سواء كانت سياسية او دينية او عنصرية للسيطرة على وجدان الافراد وافساد عقائدهم واذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع.[2]

4-سرقة المعلومات والبيانات العسكرية او التلاعب بها: من خلال اختراق قواعد البيانات العسكرية وسرقتها او تزييفها او تدميرها الكترونيا، حيث تسعى الهجمات الالكترونية في هذه الحالة الى اختراق الشبكات الخاصة بالمؤسسات العسكرية بهدف سرقة خرائط نشر انظمة التسليح او التصميمات الخاصة بالمعدات العسكرية، وقد انطلقت واحدة من اخطر الهجمات ضد انظمة حواسيب الجيش الامريكي في عام 2008، من خلال وصلة "USB" متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الاوسط، عدم اكتشاف انتشار برامج التجسس في كل الانظمة السرية وغير السرية في الوقت المناسب، شكل ما يشبه جسر رقمي تم من خلاله نقل الاف الملفات من البيانات الى خوادم خارجية[3].

كل هاته التهديدات وغيرها تؤثر بشكل او بأخر على الامن القومي، باعتبار ان الفضاء السيبراني فضاء واسع ومرن، فالتهديدات الامنية الحديثة اخذت بعدا اخر ذو طابع الكتروني، مرتبط ارتباطا ويثقا بالتطور التكنولوجي الذي وصل اليه العالم في السنوات الاخيرة، ومن جانب اخر ان التكنولوجية الحديثة لوسائل الاعلام والاتصال هي من نتاج الدول الغربية التي هي مصدر التهديدات السيبرانية، ومن جانب

1-اميرة عبدالعظيم، محمد عبدالجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد 35، 2020، ص. 415- 416

2- اميرة عبدالعظيم، محمد عبدالجواد، نفس المرجع، ص.421.

3- ايهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، مجلة اتجاهات الاحداث، العدد.22، المستقبل للأبحاث والدراسات المتقدمة، ابوظبي، يوليو- اغسطس 2017، ص.57

ثالث نجد ان البنية التحتية الالكترونية للجزائر هشة مقارنة بالدول الاوروبية والامريكية التي تمتلك مكانيزمات قوية لضمان امن معلوماتها من مختلف التهديدات الامنية، والتي لم تسلم هي الاخرى من هاته التهديدات، فاذا كانت دول العالم المتقدم والمسيطرة بشكل كامل على التطور التكنولوجي لوسائل الاعلام والاتصال فكيف بالجزائر التي تعتبر من دول العالم الثالث والمستورة بشكل كبير لهاته التكنولوجيا لذلك يتوجب على الجزائر استحداث منظومة دفاع قوية تجاه مختلف التهديدات السيبرانية التي اصبحت تهدد الامن القومي في كل دقيقة وثانية وهو ما سنحاول التطرق اليه في المحور الموالي

ومن جانب اخر يعتبر الامن القومي من اهم الوظائف التي تولي لها الدول والانظمة السياسية في العالم اهمية كبيرة، باعتباره يرتبط ارتباطا وثيقا بأمن المؤسسات والافراد والهيئات الحيوية داخل الدولة وخارجها، فالتهديدات السيبرانية اصبحت اليوم من اخطر التهديدات التي تمس بأمن المعلومات للدول وهو ما يعني المساس بشكل مباشر بالأمن القومي للدولة، فالتهديدات المتعلقة بالتجسس وقرصنة المعلومات خصوصا المعلومات المتعلقة باستراتيجيات الدولة في كافة المجالات السياسية والاقتصادية والاجتماعية، وكذا الارهاب السيبراني، كلها تهديدات تعصف بكيان الدولة واستمراريتها، فالتعاملات العصرية اليوم اصبحت مرتبطة ارتباطا وثيقا بالتطور التكنولوجي لوسائل الاعلام والاتصال، وبالتالي اي تهديد بإمكانه، تعطيل المصالح الاستراتيجية للدولة.

ومن ذلك يمكن القول ان تحدي الامن السيبراني يعد اعلى تحديات الامن القومي في القرن الواحد والعشرين، لان المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية بل يواكب كل التهديدات والتحديات التي يمكن ان تشكل عائق امام الاقتصاد الرقمي وتدفق المعرفة، فقد اسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية والسياسية والاقتصادية والاجتماعية بين الدول وهو ما يضع السيادة الوطنية والامن القومي على المحك خاصة مع الاختراق المتكرر والمتزايد للمواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.[1]

المحور الثالث: جهور الجزائر في مواجهة التهديدات والجرائم السيبرانية

في ظل تنامي التهديدات السيبرانية وتأثيراتها المتزايدة على الامن القومي الجزائري سارعت الجزائر الي تبني العديد من الجهود والاليات الكفيلة بمواجهة مختلف التهديدات والجرائم السيبرانية ومن ذلك نجد:

[1]– لامية طالمة، التهديدات والجرائم السيبرانية: تأثيرها على الامن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد04، العدد02، 2020، ص.56

اولا: في الجانب القانوني: استحدثت الجزائر العديد من التشريعات والقوانين الكفيلة بمحاربة التهديدات والجرائم السيبرانية، وذلك من اجل تعزيز امنها السيبراني، ومن ذلك نجد القانون رقم 09-04 المؤرخ في 09 ماي 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، اضافة الى القانون 05-10 الصادر في 20جوان 2005 المتضمن الدليل الالكتروني، اضافة الى قانون الاجراءات الجزائية، وقانون العقوبات لا سيما في المواد 303، 333، 394 ، 396، المتضمنة تجريم وتسليط العقوبات على كل من يثبت في حقه اختراق انظمة معلومات المؤسسات او الافراد بطريقة غير شرعية.[1]

فالاطار القانوني مهم في الحد من انتشار التهديدات السيبرانية وتأثيراتها المحتملة على الامن القومي، فالنظم القانونية تسعى الى تنظيم ممارسة واستخدام تكنولوجيا الاعلام والاتصال في الاطار الشرعي، لكن من الجانب الاخر تعمل على معاقبة كل من يسيء استخدامها في الاطر غير الشرعية، باعتبار ان امن المؤسسات والافراد هو من قبيل المحافظة على الامن القومي الجزائري، والمحافظة علية يستوجب اصدار القوانين والتشريعات الكفيلة بذلك. فقد افرد المشرع الجزائري فصلا كاملا متعلق بالتهديدات والجرائم المتعلقة بالمساس بأنظمة المعالجة الالية للمعطيات، حيث بين القسم السابع من قانون العقوبات كل اشكال المساس بأنظمة المعالجة الالية للمعطيات والعقوبات المترتبة عنها.

ثانيا في الجانب الامني

في هذا الجانب اعتمدت الجزائر من خلال اجهزتها الامنية الى استحداث مؤسسات امنية متخصصة في مواجهة التهديدات السيبرانية وذلك لتعزيز امنها القومي ومن ذلك نجد:

مركز الوقاية من جرائم الاعلام الالي وجرائم المعلوماتية للدرك الوطني: حيث أنشئ هذا المركز في 2008، بالجزائر العاصمة، تتمثل اهدافه في تأمين منظومة المعلومات لخدمة الامن العمومي، وهو بمثابة مركز توثيق يقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية المرتكبة ومحاولة تحديد اصحابها مما يؤمن الانظمة المعلوماتية للمؤسسات والبنوك والشركات ويعمل على التنسيق الامني بين الاجهزة الامنية الاخرى[2].

---

[1]– جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والافاق، مجلة العلوم القانونية والسياسية، المجلد 10، العدد.01، افريل 2019، ص.1278

[2]– يوسف بوغرارة، الامن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني، مجلة الدراسات الافريقية وحوض النيل، المركز الديمقراطي العربي، المانيا، المجلد 01، العدد 03 ، سبتمبر 2018، ص111

المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني: وهو ايضا مركز تابع للقيادة العامة للدرك الوطني، حيث يعتمد هذا المعهد في اداء مهامه على الخبرة العلمية والتجارب المخبرية الدقيقة لكل الادلة المتحصل عليها من مكان ارتكاب الجريمة عامة، ومن بين النتائج المتوصل اليها اتضح ان الجرائم الالكترونية بالجزائر تتضاعف بطريقة سريعة جدا، حيث سجلت سنة 2017 اكثر من 2500 جريمة ويتعلق ابرزها بانتهاك الحريات الشخصية والتهديد عبر الانترنت ونشر صور فاضحة عبر الانترنت والقرصنة الالكترونية، ما نسبته 70%.عمليات الاختراق طالت كذلك وزارة الدفاع الوطني، حيث تعمل المؤسسة على اجهاض ما يقارب 3500 محاولة اختراق يوميا لمواقع قياداتها اي بمعدل 130 الف محاولة اختراق في السنة من قبل عصابات ' الهاكرز" من مختلف دول العالم في اطار ما يعرف بالحرب الالكترونية[1].

المصلحة المركزية لمكافحة الجريمة المعلوماتية: وهي مؤسسة تابعة للأمن الوطني أنشئت سنة 2011 لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني حيث عملت على تكييف التشكيل الامني لمديرية الشرطة القضائية، ليتم بعدها انشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بقرار من المدير العام للأمن الوطني واضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.[2]

مصلحة الدفاع السيبراني ومراقبة امن الانظمة: وهي مصلحة تابعة لقيادة الجيش الوطني الشعبي على مستوى دائرة الاستعمال والتحضير، هدفها تأمين وحماية المنشأت الجوية للقوات المسلحة الجزائرية ضد اي تهديد امني سيبراني ، حيث تعمل هذه المصلحة على تطبيق السياسة العامة للدفاع السيبراني في الجيش الوطني الشعبي وكذا تعزيز وتقييم امن الانظمة المستغلة وتنظيم التسيير في مجال الدفاع السيبراني، وهي بذلك تعد طرفا فاعلا في العمليات العسكرية، حيث تتمحور استراتيجية الدفاع السيبراني للجيش الوطني الشعبي على سبعة محاور اساسية تتمثل في الجوانب التالية[3]:

- الجانب الوظيفي من اجل ضمان فعالية وتناسق اعمال الدفاع السيبراني
- الجانب القانوني من خلال تعزيز وتحيين الاطر القانونية التي تضمن التطور المتعلق باستعمال تكنولوجيا الاعلام والاتصال وتأمين منظومات الاعلام

الجانب البشري من خلال تكوين وكفاءة وجاهزية الموارد البشرية لاي هجوم سيبراني يهدد الامن القومي الجزائري.

---

[1]– جمال بوازدية، المرجع السابق، ص.1281.

[2]– بارة سمير، الامن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني، مخبر الامن الانساني، جامعة باتنة المجلد.02، العدد04، 2017، ص.437.

[3]– يوسف بوغرارةن المرجع السابق ، ص.114.

– الجانب التقني ويتعلق بمدى كفاء الاجهزة والوسائل المستعملة مع ضمان اليقظة للكشف والرد على الهجمات السيبرانية.

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها: هي سلطة ادارية مستقلة لدى وزارة العدل تعمل تحت اشراف ومراقبة لجنة مديرية يترأسها وزير العدل، وتضم قضاة وضباط واعوان من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني، تعمل على الكشف عن الجرائم الارهابية وجرائم المساس بأمن للدولة، كما تعمل على اقتراح الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها ومساعدة السلطات القضائية في مجال مكافحة هذه الجرائم من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية وضمان المراقبة الوقائية للاتصالات الالكترونية.[1]

انطلاقا مما سبق نجد ان الاستراتيجية الجزائرية في تعزيز امنها القومي من التهديدات السيبرانية تعتمد على المقاربة الدفاعية واعتماد الردع السيبراني كآلية لمواجهة مختلف التهديدات السيبرانية وهو ما اكدته العديد من التصريحات لقيادات الجيش الوطني الشعبي والاجهزة الامنية الجزائرية ان مهمة حماية فضاءنا السيبراني هي مسؤولية جماعية تضمن من خلال استراتيجية وطنية شاملة للأمن السيبراني يتعين ان ينخرط فيها الجميع، فالأجهزة الامنية في الجزائر تعي جيدا ان الامن السيبراني اضحى سلاحا استراتيجيا بيد الحكومات والافراد، خصوصا مع التطور المتسارع لتكنولوجيا الاعلام والاتصال.

اضافة الى الجهود القانونية والامنية اعتمدت الجزائر ايضا على الجانب التحسيسي والتوعي بمخاطر الاستخدام غير الامثل لتكنولوجيا الاعلام والاتصال والجرائم والتهديدات الناجمة عنها، في مختلف وسائل الاعلام والاتصال، وكذا الخرجات الميدانية لعناصر الامن الوطني والدرك الوطني، وذالك لما تلعبه الجوانب التحسيسية والتوعوية من دور مهم في الحد من انتشار التهديدات السيبرانية، فالتهديدات السيبرانية التي نشهدها في الوقت الراهن تعتبر تكنولوجيا الاعلام والاتصال المصدر الوحيد لانتشارها فوعي المواطن بخطورة الاستخدام غير الامثل لتكنولوجيا الاعلام والاتصال يساهم بشكل كبير في الحد من انتشار التهديدات الامنية، وهو ما عبرت عنه القيادات العسكرية الجزائرية في العديد من الخطابات حيث تطرق رئيس اركان الجيش الوطني الشعبي " سعيد شنقريحة" من خلال كلمته في افتتاح اشغال الملتقى الثاني "الأمن السيبراني والدفاع السيبراني: رهانات وتحديات على ضوء التحولات الجديدة المتعددة الأبعاد"، يومي 23 و24 ماي 2021، بالنادي الوطني للجيش،" كما لا يفوتني أن أؤكد على أن مهمة حماية، وتأمين، والدفاع عن فضائنا السيبراني، هي مسؤولية جماعية، تُضمن من خلال إستراتيجية وطنية شاملة للأمن السيبراني، يتعين أن ينخرط فيها الجميع، بداية من المواطن، من خلال وعيه بالمخاطر،

---

[1]– عائشة عبدالحميد، الاطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي، المجلة الدولية للتعليم بالانترنت، جمعية التنمية التكنولوجية والبشرية، المجلد 19، العدد 01، جويلية 2020 ص.101

التي ينضوي عليها هذا الفضاء، وتقيده الصارم بالإجراءات السليمة، عند استخدام الوسائل التكنولوجية، فضلا عن دور المختصين في هذا المجال، عبر المساهمة بخبراتهم وآرائهم في إنجاح الإستراتيجية الوطنية، وصولا إلى المسؤولين على كل المستويات، مع الحرص الدائم على التكيف مع التحولات السريعة للفضاء السيبراني، وتوفير الحلول اللازمة سواء الإستباقية، أو العلاجية، الكفيلة بحماية رصيدنا المعلوماتي، من جهة، والحفاظ على حقوق وحرية مواطنينا، من جهة أخرى"[1]

خاتمة:

بعد الدراسة والتحليل توصلنا الى ان الامن السيبراني اصبح اليوم من اهم اولويات الدول والانظمة السياسية في العالم باعتباره يرتبط ارتباطا وثيقا بأمن المعلومات والمعطيات ذات الطابع السياسي والاجتماعي والاقتصادي والثقافي، سواء تعلق الامر بأمن الدولة او بأمن الافراد، ويرجع ذلك لمختلف التهديدات التي بات يطرحها التطور التكنولوجي لوسائل الاعلام والاتصال، فالقرصنة والارهاب الالكتروني، وسرقة وتدمير المعلومات ،التجسس السيبراني، الارهاب السيبراني، سرقة المعلومات والبيانات العسكرية ، تزييف المعلومات واتلافها او تدميرها الكترونيا، كلها جرائم وتهديدات اضحت تؤثر بشكل كبير على الامن القومي للدول، ما جعل الجزائر تكثف جهودها بهدف الحد من هاته التهديدات من خلال استحداث العديد من الاليات سواء في شقها القانوني من خلال استحداث وتحيين العديد من القوانين بما يتماشى وظاهرة تنامي التهديدات السيبرانية، اضافة الى استحداث العديد من المؤسسات الامنية والادارية ذات العلاقة والصلة بالأمن السيبراني، بهدف حماية الفضاء السيبراني الجزائري من اي تهديدات قد تطاله فالجزائر اعتمدت المقاربة الدفاعية والردع السيبراني وهو ما يتماشى والاستراتيجية الجزائرية القاضية باحترام سيادة الدول وعدم التدخل في شؤونها الداخلية، مع مواجهة اي تهديد من شأنه التدخل في الشؤون الداخلية للجزائر، اضافة الى الدور التحسيسي والتوعوي بمخاطر الاستخدام غير الامثل لتكنولوجيا الاعلام والاتصال. وبالتالي يمكن القول ان مواجهة التهديدات السيبرانية وتعزيز الامن السيبراني والقومي يقتضي بالضرورة تكاتف كل الجهود وفي مختلف المجالات القانونية والسياسية والاقتصادية والاجتماعية والامنية، لان الظاهرة في تطور متسارع وتنشط في فضاء واسع ومرن.

[1] الشروق اونلاين، الفريق شنقريحة: أحبطنا كافة الهجمات السيبريانية ضد الجزائر، مقال منشور على الموقع الالكتروني: https://bit.ly/3IEUVGJ بتاريخ 23 ماي 2021 تم الاطلاع عليه بتاريخ 24 مارس 2022، على الساعة 17:19.

قائمة المراجع والمصادر

اولا: المؤلفات

1) spykman; Nicholas J1944. The Geography of the peace . Hqrcourt Brqce and compqny. New york

2) ابن منظور، لسان العرب، ج1، ط1، بيروت، دار صادر، 2000م.

3) ثامر كامل الخزرجي، العلاقات السياسية الدولية واستراتيجية ادارة الازمات، ط.01، عمان، دار مجدلاوي للنشر والتوزيع، 2009

4) ربحي مصطفى عليان، عثمان محمد غنيم، مناهج واساليب البحث العلمي النظرية والتطبيق، ط.1، عمان، دار صفاء للنشر والتوزيع، 2000.

5) سعاد بيطاط، الامن دراسة في الحديث الموضوعي، عمان، مركز الكتاب الاكاديمي، 2015.

6) عادل عبدالصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، ط.02، القاهرة، المركز العربي لابحاث الفضاء الالكتروني، 2016.

7) عبدالرزاق الدليمي، الدعاية والشائعات رؤية معاصرة، الاردن، دار اليازوري العلمية للنشر والتوزيع، 2019.

8) علي زياد العلي، المرتكزات النظرية في السياسة الدولية، القاهرة، دار الفجر للنشر والتوزيع، 2017.

9) مارتن غريفيثس، تيري اوكالاهان ، المفاهيم الاساسية في العلاقات الدولية، دبي، مركز الخليج للأبحاث ، 2008، ص.78.

10) محمد طالب حميد، العلاقات الايرانية الامريكية توافق ام تقاطع، ط.01، القاهرة، العربي للنشر والتوزيع، 2016.

11) مصطفى محمود منجود، الابعاد السياسية لمفهوم الامن في الاسلام ، القاهرة، المعهد العالمي للفكر الاسلامي ، 1996.

ثانيا: المقالات

12) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر" مجلة المحقق الحلي للعلوم القانونية والسياسية ، كلية القانون، جامعة بابل، العدد 04، 2016 .

13) اميرة عبدالعظيم محمد عبدالجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام " مجلة الشريعة والقانون، العدد 35، 2020.

14) ايهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مجلة اتجاهات الاحداث، المستقبل للأبحاث والدراسات المتقدمة، العدد.22، ابوظبي، يوليو – اغسطس 2017.

15) بارة سمير، الامن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني، مخبر الامن الانساني، جامعة باتنة، المجلد.02، العدد04، 2017، 2017.

16) بن صابر بلقاسم، حيدرة محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الانسان والحريات العامة، جامعة مستغانم، المجلد.02، العدد04، جوان 2017.

17) جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والافاق، مجلة العلوم القانونية والسياسية، المجلد 10، العدد.01، افريل 2019.

18) عائشة عبدالحميد، الاطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي، المجلة الدولية للتعليم بالانترنت، جمعية التنمية التكنولوجية والبشرية، المجلد 19، العدد 01، جويلية 2020.

19) فرج عصام بن جليل واخران، اثر التحديات الداخلية والخارجية على الامن القومي العربي: الواقع وافاق المستقبل، مجلة علوم الانسان والمجتمع، المجلد 10، العدد03، 2021.

20) كريم رقولي، اخضر نويوة ، الامن السيبراني المتوسطي بين الواقع والرهانات الامنية، مجلة طبنة للدراسات العلمية والاكاديمية، المركز الجامعي بريكة المجلد 02، العدد.02، ديسمبر 2019.

21) لامية طالمة، التهديدات والجرائم السيبرانية: تأثيرها على الامن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد04، العدد02، 2020.

22) يوسف بوغرارة، الامن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني، مجلة الدراسات الافريقية وحوض النيل، المركز الديمقراطي العربي، المانيا، المجلد 01، العدد 03 ، سبتمبر 2018.

ثالثا: المذكرات والرسائل الجامعية

23) تباني وهيبة، الامن المتوسطي في استراتيجية الحلف الاطلسي دراسة حالة: ظاهرة الارهاب مذكرة ماجستير في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو ، 2014.

رابعا: المواقع الالكترونية

24) الشروق اونلاين، الفريق شنقريحة: أحبطنا كافة الهجمات السيبريانية ضد الجزائر، مقال منشور على الموقع الالكتروني: https://bit.ly/3lEUVGJufu بتاريخ 23 ماي 2021 تم الاطلاع عليه بتاريخ 24 مارس 2022، على الساعة 17:19.

25) نوران شفيق، "اشكال التهديدات الالكترونية ومصادرها"، المركز الاوربي لدراسات ومكافحة الارهاب والاستخبارات، المانيا وهولندا على الموقع الالكتروني https://www.europarabct.com/%D8%A3%D8%B4% : بتاريخ 29 يناير 2020، تم الاطلاع عليه بتاريخ 2022/02/28، على الساعة 14:56.