

مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري

الدكتور إدريس عطية

كلية الحقوق والعلوم السياسية-جامعة العربي التبسي - تيسة/ الجزائر

Abstract:

This study addresses the issue of changing the concept of Security threats due to developments in the field of technology. This study will focus on Algerian perceptions in confronting cyber risks and challenges by adapting the security system to global geostrategic shifts. Cyber threats have become one of the most important and urgent issues for international security. Therefore, the Algerian security and defense strategy must be supported taking into account its degree from most to least serious, adapting it to the future requirements to face threats according to their gravity, and focusing on building this security system on The probability of what other actors will do, and dealing with these threats according to the logic of expectation and probability

The key words:

Cybersecurity, Algerian National Security, Cyber threats, Cyber Crime.

ملخص:

تعالج هذه الدراسة مسألة التغيير في مفهوم التهديدات الأمنية الحاصلة بسبب التطورات في مجال التكنولوجيا، حيث أصبحت قضية الأمن السيبراني من التحديات الكبرى التي توجهها الدول على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد حجم التهديدات السيبرانية التي تصيب أمن معلومات الدول، ما يؤدي إلى اختراق أمنها الوطني وانهياره، بحيث سيتم التركيز من خلال هذه الدراسة على التصورات الجزائرية في مجابهة المخاطر والتحديات السيبرانية من خلال تكييف المنظومة الأمنية مع التحولات الجيوستراتيجية العالمية، فالتهديدات السيبرانية أصبحت بشكل غير مسبوق من أكثر القضايا أهمية وإلحاحا بالنسبة للأمن الدولي، ولذا وجب دعم استراتيجية الامن والدفاع الجزائرية مع الأخذ بعين الاعتبار درجتها من الأكثر إلى الأقل جدية، وتكييفها حسب المتطلبات المستقبلية لمواجهة التهديدات حسب درجة خطورتها، والتركيز في بناء هذه المنظومة الأمنية على احتمال ما سيقوم به الفاعلون الاخرون، والتعاطي مع هذه التهديدات وفق منطق التوقع والاحتمال.

الكلمات المفتاحية:

الأمن السيبراني؛ الأمن الوطني الجزائري؛ التهديدات السيبرانية؛ الجريمة السيبرانية.

مقدمة:

أصبح الأمن في عالم العولمة من ضمن المعطيات النادرة، التي توجي بالحاجة العالمية والماسة لتطبيق مقاربة شاملة وفاعلة على كل المستويات بشكل يمكن أن يؤكد على النضج النظري في الدراسات الأمنية أو القول باستهلاك كل النظريات القائمة على تحليل ووصف، وكذا شرح وتفسير الظواهر اللأمنية، ومن ثم الإسهاب في التنبؤ بمستقبلها وإستشرافها (ماض ومستقبل)، ولذا جاز الحديث عن ما هو أبعد من النظرية (الميتا-نظرية) في الدراسات الأمنية كإطار عالمي قابل للتطبيق من أجل تحقيق الأمن لكل الإنسان دون إستثناء لكل الفواعل الأمنية (حكومية وغير حكومية/عقلانية وغير عقلانية).

ونحن الآن بصدد تجاوز عصر الأنترنت، إذ لم نعد نحتاج إلى «دخول الشبكة» من خلال الإتصال عبر حاسوب في المكتب أو البيت، بل أصبحنا نعيش «فيها»، إن عدد الأفراد المتصلين بالشبكة في تزايد أسي ويتوقع أن يتجاوز 3.2 مليارات نسمة في آخر هذا العام (2019) أي نصف عدد سكان الأرض.

نحن بالفعل نشهد ميلاد مجتمع «الإنسان المعزز» Augmented human، إنه الإنسان المعزز القدرات بفضل إتصاله الدائم بالشبكة وما توفر له من موارد، فقد أصبح يرى الأحداث لحظة وقوعها على بعد آلاف الأميال، ويستعين بخوارزمات الذكاء الإصطناعي للفصل السريع في المسائل المعقدة التي كانت تستوجب أياما من الدراسة، وطور أدوات جراحية تصلح ما فسد في جينات الإنسان بدقة نانوية، يحدث كل هذا بفضل تطوير تكنولوجيا الحاسوب.

ولذلك فإن الأمية في عصر «الإنسان المعزز» ليست العجز عن الكتابة والقراءة وإنما عن إستخدام الحاسوب وبرمجته، ولهذا السبب تدعو الحكومات الغربية الى إتاحة فرصة تعلم مهارات الحاسوب لجميع الأطفال منذ روضة الأطفال.

قد يبدو هذا حديثا عن هموم الأغنياء في الغرب ولا يعني من يعانون الفقر في بلاد العرب، والحقيقة أنه حديث عن تحديات تقرر مصيرنا، إذ ينبغي أن نكون أو لا نكون.

لكل عصر معركته ومجاهدوه، بالأمس كانت الجبال والغابات ساحة لمن أخذوا على أنفسهم تحرير البلاد، أما معركة تحرير العقول وبناء الوطن فساحتها المدارس والجامعات، لتكون «الإنسان المعزز» في النسخة الخامسة لمجتمع بشري.

تشير الإحصائيات المسجلة في الجزائر أن «الجريمة السيبرانية» أخذت منحاً تصاعدياً في الأونة الأخيرة، وهو ما ينبأ بخطورة الوضع، لا سيما في ظل توجه الجزائر نحو تبني مقاربة الحكومة الإلكترونية (e-Gouvernement)، ومن هذا المنطلق فإن السلطات الجزائرية ملزمة بإتخاذ الإحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم الإلكترونية المهددة لها، فهي عبر محاولة وضع حلول وإجراءات لمواجهة هذا التهديد الذي يترصد أمنها الوطني، كما تسعى جاهدة للتعاون مع باقي دول العالم خاصة المتطورة منها في مجال الحماية السيبرانية.

حيث توجهت منظومة الأمن الجزائري إلى وضع إستراتيجية أمنية شاملة من أجل ضمان «الأمن السيبراني»، لأن أمن المعلومات يعتبر ضمن الأمن الوطني الشامل، فالأجهزة الأمنية الجزائرية تدرك أن التغيرات المتسارعة في التكنولوجيا تؤدي إلى خلق تهديدات ليست بالسهلة، لذا لا بد من ضرورة العمل على ضمان أمن المعلومات وشبكات الأنترنت خلال خطوات مهمة تعتمد على مجموعة كبيرة من وسائل قانونية وتقنية لمقاومة الاستخدام غير الشرعي للشبكة العنكبوتية من أجل حماية نظم المعلومات ووسائل الإتصالات لحماية الوطن والمواطن والمؤسسات من مخاطر «التهديدات السيبرانية».

من خلال ما سبق نطرح مشكلة الدراسة التالية:

كيف يمكن تكييف منظومة الأمن الوطني مع التحديات التي يفرضها الفضاء السيبراني؟ وماهي خارطة الطريق والمنظومة النظرية والمذهبية التي ينبغي استثمارها من أجل تحقيق الأمن السيبراني؟

فرضية الدراسة؛

مساهمة منا في الإجابة على السؤالين المحوريين المطروحين، ينبغي أن نطرح الفرضية التالية:

كلما اعتمدت الدولة على الأساليب الجديدة في ممارسة عملها الأمني كلما أهلها ذلك لتحقيق أمنها الوطني بكل كفاءة وجنبها الإختراقات الإستراتيجية غير المحمودة.

أهداف الدراسة:

تهدف الدراسة إلى إبراز التوجه الجزائري لتجديد المنظومة الأمنية وتكييفها مع المتطلبات العصرية، بدل التمسك بالأساليب الكلاسيكية في العمل الأمني، من خلال الانفتاح على المجال الإفتراضي وإعمال كل الأساليب والأدوات الجديدة لخلق نظرة برغماتية فاعلة تستطيع تحقيق الأمن الوطني وتحصين المجتمع الجزائري.

المنهجية المتبعة:

تستدعي الدراسة المنهج التاريخي من خلال مساءلة المتغيرات المشكلة للفعل الأمني الجزائري ومدى القطيعة والتواصل الزمنية فيما بينها وبين الأحداث الدولية، وتوظف الدراسة أيضا المنهج المقارن التفسيري من خلال السعي للإجابة على العناصر المسؤولة على الإختلاف بين العقيدة الأمنية الجزائرية ومقارنتها دولياً، كما تستند الدراسة على الإقتراب النسقي لـ "دافيد استون" David Eston من خلال شرح العلاقة بين البيئة الداخلية والبيئة الخارجية وتقييم عملية التغذية العكسية في المنظومة الأمنية للجزائر.

المحور الأول: البناء الإيتومولوجي للأمن السيبراني:

لقد حازت مسألة «الأمن السيبراني» (Cybersecurity) على المزيد من الإهتمام على جميع المستويات العالمية والإقليمية والوطنية سواء من جهة إرتفاع عدد الهجمات

مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري

والتهديدات الناجمة عنها، حيث شهدت الكثير من الدول إختراقات أمنية مقلقة استهدفت المؤسسات والشركات وحتى الأفراد إلى سرقة البيانات والقرصنة والتجسس والتجنيذ والإرهاب الإلكتروني وغيرها.

1-1 تعريف الأمن السيبراني: ويمكن أن نقارب هذا المفهوم من عدة زوايا:
السيبرانية لغة: وهي مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني (فضاء الأنترنت)، وهي كلمة مشتقة من الكلمة اليونانية *Kybernetes* التي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة.¹

أما قاموس Oxford الإنجليزي فيعرفها على أنها «دراسة فاعلية العمل البشري بمقارنتها بفاعلية الآلات الحاسبة تتصل بسمات وخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي»²، فيما يعرفها قاموس مصطلحات الأمن المعلوماتي بأنها: «هجوم الفضاء الإلكتروني يهدف إلى السيطرة على المواقع الإلكترونية أو بني محمية إلكترونية لتعطيلها أو تدميرها أو الإضرار بها»³.

أما في اللغة العربية وبالرجوع إلى المختصين فيها، فنجد أن هؤلاء المختصين يواجهون تحديا في الوصول إلى مصطلح مقارب لمصطلح Cyber.

السيبرانية اصطلاحا: كلمة سيبرانية في مفهومها الحديث إستعملت لأول مرة من قبل عالم الرياضيات الأمريكي «نوربرت وينر» Norbert Winer وهو أستاذ الرياضيات في معهد ماساتشوستس التقني MIT الذي أعطاهم مفهومها الإصطلاحي الحديث وكان ذلك عام 1948، ومن أجل وصف نظام التغذية الرجعية Feedback الاستفادة من مخرجات الأنظمة out puts في ضبط مدخلاتها in puts وفي التحكم فيها وإستقرار أداؤها.

ورأى «وينر» أنه يمكن تطبيق هذا النظام على نطاق واسع في مختلف المجالات ليس العملية فقط بل الإنسانية أيضا، وبالتالي فالمصدر الإصطلاحي الحديث لكلمة سيبرانية وهو «علم القيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل».

لقد لخص «وينر» الحدود التي لا ينبغي أن يتعداها إيماننا بقدرات الآلة أو الخوف من طغيانها بقوله: «أعط ما للإنسان للإنسان، وما للعقل الإلكتروني للعقل الإلكتروني» وهو يعني بذلك أن الإنسان يظل له دوره العام والأساسي في عصر التقدم التكنولوجي، وأن أرقى أنواع الآلات يظل على الدوام أداة طبيعة في يد صانعها، وهي تتجه في نفس الطريق الذي يريدها الإنسان أن تسلكه سواء كان خيرا أم شرا⁴.

وكان ظهور علم السيبرنطيقا (Cybernetics) هذا العلم الجديد، هو بدوره واحد من المعالم البارزة لعصرنا الحاضر حيث كانت أبحاث «وينر» هي الأساس الأول لإختراع العقول الإلكترونية، فقد كانت فكرة هذا العالم هي تطبيق ما يحدث في الإنسان بوضعه جهازا

حيًا متكاملًا على الآلات من أجل بلوغ مرحلة جديدة في تطورها مختلفة عن كل ما استخدمت فيه الآلات من قبل، وعلى هذا الأساس فقد درس «وينر» الوظائف الذي يقوم بها الجهاز العصبي للإنسان والتي يتمكن الإنسان بواسطتها أن يصحح مسار أفعاله ويعيد توجيهها وفقًا لما يواجهه وأن يأمر نفسه ويطوعها ويختبر نتائج سلوكه ويعدلها.

وحين أمكن تطبيق نتائج هذه الدراسات في صنع جيل جديد من الآلات كانت تلك الآلات من نوع لم يألفه الإنسان من قبل، فهي ليست تلك الآلات التي تحتاج إلى إشراف دائم للإنسان ولا تعمل إلا وفقًا لأوامره ولا تسير إلا في خط واحد يرسمه لها مقدما، بل أنها كانت آلات تصحح مسارها بنفسها وتتبادل مع نفسها الأوامر وتنفيذ الأوامر وتقوم بأعمال إنتاجية أعقد وأكمل بكثير مما كانت تقوم به الأجيال السابقة من الآلات سواء منها البخارية والكهربائية. وهكذا كانت فكرة تلك الآلات تتضمن في داخلها عقلا حاسبا يراقب عملها ويعدله ويصححها ويعيد توجيه سيرها وفقًا لما يجريه من حسابات.

تعريف الأمن السيبراني: مفهوم مؤشك

ويعرف على أنه:

«عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني»⁵.

والأمن السيبراني هو: «سلاح إستراتيجي بيد الحكومة والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزء لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول»⁶.

ويعتبر مفهوم الأمن السيبراني من أكثر المفاهيم المثيرة للإهتمام والدراسة، حيث عرف تعددًا في التعريفات المقدمة له والتي يمكن إبرازها فيما يلي:

فقد عرفه «ريتشارد كمرر» Richard A Kemmerr على أنه: «عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القرصنة»، بينما يعرفه «إدوارد أمورسو Edward Amoroso» على أنه: «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».

والملاحظ هنا أن كل من «ريتشارد كمرر» و«إدوارد أمورسو» قد ركزوا في هذين التعريفين على أن الأمن السيبراني هو: «وسيلة دفاعية ضد الهجمات وعمليات القرصنة على مختلف الحواسيب والشبكات»

فالأمن السيبراني هو: «المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو

مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري

والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم ويشمل ذلك الأجهزة الإلكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية، الفضاء السيبراني ليس الإنترنت فقط وإنما شبكات أخرى كثيرة متصلة».

2-1 أبعاد الأمن السيبراني: وتشتمل على خمسة أبعاد وهي تكمل بعضها البعض:

الأبعاد العسكرية: تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدقيقها، وكذا السرعة وإعطاء الأوامر العسكرية والقدرة على إيصال الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن شبكة الإلكترونيات المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي قد ينسب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات، ومن ثم تجسس على أمن عسكري للدول، وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الإتصال في ما بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الإلكتروني فضلا عن إمكانية وفقدان السيطرة على وحدات القيادة⁸.

الأبعاد الاقتصادية: يرتبط الأمن السيبراني ارتباطا وثيقا بالإقتصاد فالتلازم واضح بين

إقتصاد المعرفة وتوسيع إستخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدم على كل المستويات، كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الإستخدام 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 إستثمارات 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 والعبارة للحدود كتنبيض الأموال والتهرب من الضريبة. فالأمن السيبراني يضمن تقديم الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الإقبال عليها بما يترجم عمليا بتطوير أسس إقتصاد سليم⁹.

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 إستقرار الفضاء الإلكتروني والمجتمع الذي يركز إليه، كما أن إنفتاح مجتمع ما على المجتمعات الأخرى يؤسس لتبادل خبرات وأفكار وتكوين آفاق للتعاون والتكامل¹⁰.

الأبعاد السياسية: يتمثل البعد السياسي للأمن السيبراني 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 تقدمه 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 لها¹¹.

الأبعاد القانونية: تعد العلاقة بين القانون والتكنولوجيات علاقة تبادلية فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية منها ولكن بصورة عامة تفتقد الجريمة السيبرانية 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 ومرور التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب ذلك فإن الجرائم السيبرانية غير مقيدة بحدود الدول، الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها¹².

3-1 الفواعل الأساسية في الفضاء السيبراني: يمكن تقسيم الفواعل في الفضاء السيبراني ومن لديهم القدرة على الفعل السيبراني أو شن الهجمات الإلكترونية إلى ما يلي:
الدولة:

تمثل الخطر الأكبر والفاعل الأكثر قوة في مجال الفضاء السيبراني، ففي نهاية العام 2018، استطاعت حوالي 180 دولة أن تمتلك ترسانة من الأسلحة الإلكترونية، مما قد يدفع الفواعل من الدول ومن غير الدول للتنافس في السنوات القادمة من أجل تحقيق التفوق الإلكتروني.

وتنقسم القدرات السيبرانية للدول بشكل عام إلى قدرات دفاعية وأخرى هجومية، وقد أضاف كل من «ريتشارد كلارك» (Ritchard Clarke) و«روبرت كناك» (Robert Knake)، في كتابيهما عن الحرب الإلكترونية باعتبارها الخطر القادم الذي يهدد الأمن الوطني للدول¹³.

الفواعل من غير الدول:

إن تصاعد خطر الفاعلين من غير الدول على الأمن السيبراني في العلاقات الدولية قد أثر بدوره على سيادة الدول، وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية وبروز أخطار القرصنة والجريمة الإلكترونية والجماعات الإرهابية، ومن جهة أخرى فقد فرض ذلك تحدي الحفاظ على الأمن دون إشراك هؤلاء الفاعلين الجدد في تحمل المسؤولية والعبء في تأمين البنية التحتية المعلوماتية وبدأ يظهر اتجاه التعددية في الحفاظ على الأمن بين كافة أصحاب المصلحة من الحكومات والمجتمع المدني والقطاع الأكاديمي والتفني والقطاع الخاص ووسائل الإعلام¹⁴.

الفرد

أضحى الفرد فاعلا مهما في الفضاء السيبراني، حتى أن له القدرة على إحداث ثورة الرقمية، لتصبح تلك الثورة مجال استخدام للدولة نفسها، ومثال ذلك ما قام به «مارك زوكربارغ» (Mark Zoukberg) عام 2004، حين أسس الـ (facebook)، لتستقطب أكثر من مليار مستخدم عبر العالم. وغيرها من وسائل التواصل الإجتماعي بمختلف أنواعها، حيث تبقى هذه الوسائل بحرا لحرية الأفراد الذين يمارسون نوعا من المعارضة الإفتراضية، إلا أن هذا الجانب من الحرية أعطى الوقت للأفراد على اختلاف توجهاتهم وانتماءاتهم سواء كانوا رسميون أو غير ذلك، فسحة واسعة لنشر الأفكار والمعلومات سواء كانت سليمة أو ضارة بالآخرين¹⁵

رابعا: المجموعات الإفتراضية (Virtual Community):

تتخذ هذه المجموعات سمات متميزة تجعلها فضاءات مثاليا للتواصل، خاصة بالنسبة إلى الأجيال الشبابية التي أضحت الثقافة الرقمية المرتكزة على الصورة تشغل حيزا مهما من حياتها بكل ما تحملهم من رموز ودلالات، وقواعد التواصل والتبادل، وعلاقات إجتماعية.

فالمجموعات الإفتراضية حسب «هاورد رينغولد» (Hawrd Rengold) هي مجموعات تنشأ من الشبكة حين يستمر أناس بعدد كاف من الزمن لتشكيل علاقات شخصية في الفضاء السيبراني، أما «نديم منصورى»، فيرى أنها مجموعة من الأفراد يتشاركون عبر الأنترنت لفترة زمنية، لتحقيق غاية أو هدف أو هواية، من خلال علاقة إجتماعية إفتراضية تحدها منظومة «تكنو-إجتماعية»، فتتحقق المجموعات الإفتراضية من خلال بروزها كفاعل أو متفاعل أثناء عمليات التواصل عبر الشبكة، وتختلف هذه هويات هذه المجموعات حسب «فاني جورج» (Vanny Gzorges)¹⁶ إلى:

الهوية التصريحية: (Identité déclarative) تبرز من خلال المعلومات التي يجرى إدخالها من قبل صاحب الحساب.

هوية ثنائية القطب: (Diasporiens Bipolaires) تضم أقلية تعبر عن ارتباطها العميق في الوقت ذاته بالوطن الأم والبلد والمستقبل.

هوية عالمية: (Les Cosmopolites) تعرض إفتاحا على مختلف الثقافات العالمية، وتشير الباحثة إلى أن هذه المجموعات لا تخفي حقيقة التغيرات والممارسات الهوياتية بفعل سهولة التواصل والتفاعل عبر الفضاء السيبراني.

المحور الثاني: التهديدات الأمنية السيبرانية في عصر التكنومعلوماتية

عندما نواجه التهديدات السيبرانية فنحن هنا نجد أن هناك أوجه للتشابه إلى حين يبين الجيوش فطوال التاريخ قد اختلفت المعارك في نطاق التعقيد والإستراتيجية والتكتيكات، ولكن الشيء المشترك لكل هذه المعارك هو العدو الذي يسعى إلى الإستفادة من البنية التحتية

وقدرات لشن هجوم آخر وهو نفس الشيء بالنسبة للتهديدات السيبرانية، هي قدرة العدو على الاستفادة من البنية التحتية لاستغلال نقاط الضعف كما هو الحال مع الجيوش في المعركة وكل عدو يوظف مختلف التكتيكات والتقنيات والإجراءات.¹⁷

1-4 تعريف التهديدات السيبرانية:

هي استغلال الحاسبات وتكنولوجيا المعلومات في تخريب وتدمير البنية المعلوماتية للخصوم، بل وتعطيل شبكات الدفاع الجوي وإختراق أنظمة المعلومات للبريد الإلكتروني مكاتب رؤساء الدول والتجسس عليهم وفق خطة ممنهجة.¹⁸

إذًا، التهديدات السيبرانية أو الهجمات السيبرانية هي التي تهدد أمن المجتمع وأمن الإقتصاد الوطني والجانب الأمني والعسكري للدول، كما أن للتهديدات السيبرانية أهداف مسطرة، حيث تمس كلا من الجانب المعنوي والجانب المادي وعلى جميع الأصعدة،¹⁹ لكن ما يتوجب على الدول المعرضة لتلك التهديدات وضع خطط إستراتيجية من أجل مكافحتها والتخلص منها ويمكن التوضيح أكثر من خلال الجدول الآتي:

جدول يوضح: طرق إستخدام التهديدات السيبرانية وكيفية التعامل معه

المصدر: أحمد السيد النجار، محمد عبد الهادي علام، حروب المعلومات: من يواجهها؟، مجلة الأهرام، العدد 139، (13 يوليو 2015)، ص 26.

الدفاع المجتمعي السيبراني	الدفاع الاقتصادي السيبراني	الدفاع العسكري السيبراني	
الدين - الشباب - التراث - الأخلاق	الجودة - السرعة - التنافسية - الاختراعات التنموية المعاملات المالية - التطوير الاقتصادي	العقيدة العسكرية - ميزان الربح - ثقة الشعب بالجيش والأمن	القيم المهددة
نشر الانحراف لتشكيل خلايا إلكترونية مشوشة للدولة - الحصول على معلومات من الأفراد - التحريض على العنف - تشكيك الشعب بقدراته	تدمير التنمية الاقتصادية الإلكترونية - سرقة الأموال - تدبير التجارة الإلكترونية - إيقاف التصدير والاستيراد - الحاق الخسائر المادية الاقتصادية	الحصول على معلومات تخص التسليح - التجسس على الاستخبارات - امكانية إعادة توجيه القتال والصواريخ الذكية - التجسس على البيانات الرقمية	أهداف التهديدات السيبرانية

مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري

<p>الهجوم الالكتروني المضاد - محاكاة عملية الاختراق الأمني العملياتي - ولاء المسؤولين الأجهزة الأمنية - تطوير ترسانة السلاح الرقمي</p>	<p>ضرورة توعية الخبراء والمختصين بمخاطر التهديدات السيبرانية - الحرص على استمرار عدم انقطاع الاتصال بشبكة الانترنت</p>	<p>توصية الهيئات الشخصية والأجهزة الأمنية المختصة الوطنية وتوجه وتركز الدفاع الشعبي الالكتروني وتخطط له</p>	<p>استراتيجيات الدفاع الوطني</p>
<p>توفير برامج الحماية- تجهيز منشآت الهجوم الالكتروني- توظيف الأنظمة الإلكترونية في الهجوم على مواقع العدو</p>	<p>مواقع الحماية من الفيروسات - إدخال نشاط أمن المعلومات إلى الشركات- تحفيز مواقع الانترنت الاحتياطية وتجهيز البريد الإلكتروني</p>	<p>الشبكات الاجتماعية الالكترونية - البريد الالكتروني - مواقع وسائل الاعلام - تقنيات الحماية الالكترونية</p>	<p>أدوات الدفاع السيبراني</p>
<p>وحدات خاصة بتقييم إحداثيات داخل الجيش والمخابرات، تكون مهمتها الدفاع والهجوم.</p>	<p>مديرية المعلوماتية في المؤسسات</p>	<p>كل من لديهم القدرة على عمل السلاح الرقمي</p>	<p>المسؤول عن الدفاع</p>

5-1 أنماط التهديدات السيبرانية:

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

خطر الكوارث الطبيعية أو (العرضية للكابلات البحرية):

تعد الكابلات (Submarine Cable) جزءاً هاماً لتوفير خدمة الاتصالات بين دول العالم في مجال الأنترنت، وشبكات الكمبيوتر وغيرها، فمنذ عام 2005 أصبحت الكابلات البحرية مأهولة على مجال الاتساع والانتشار، أما على نطاق التقدم والتطور تحولت إلى تقنيات أخف وزناً وأصغر حجماً، كما تعرضت تلك الكابلات إلى عدد من المشكلات التي تؤثر سلباً على أعمال البنى التحتية بالضرر، حيث لا تقع في مياه المحيط العميق.²⁰

التجسس الإلكتروني: (Cyber Espionage):

يعد أحد أنواع التجسس التقليدي، باستخدام وسائل التكنولوجيا الفائقة، ومعظم الهجمات السببرانية المتطورة التي تقع ضمن هذه الفئة، حيث يتم الحصول على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية إقتصادية، أو إستراتيجية أو عسكرية.¹⁸ فالتجسس السببراني هو ذلك التجسس الذي يعتمد على استخدام التقنيات الإلكترونية في الحصول على معلومات، ويختلف التجسس السببراني من حيث النوع، فهناك التجسس عن طريق الأفراد، ومن خلال الشبكات السلكية أو التجسس من خلال الأقمار الصناعية.²¹

الجريمة السببرانية: (Cyber Crime):

تتكون الجريمة السببرانية أو الإفتراضية من مقطعين هما: الجريمة (crime) والسببرانية (cyber) ويستخدم مصطلح السببرانية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجية على القانون. والجرائم السببرانية هي المخالفات التي ترتكب ضد الأفراد أو مجموعات من الأفراد بدافع الجريمة قصد إيذاء سمعة الضحية بأذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الإتصال مثل الأنترنت) كغرف الدردشة، البريد الإلكتروني والموبايل) فالأعمال ذات الصلة بالحاسب 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 السببرانية».²²

الإرهاب السببراني: (Cyber Terrorism):

المقصود بالإرهاب المعلومات أو الإرهاب السببراني هو ذلك الاستخدام للموارد المعلوماتية، المتمثلة في الإعلام وأجهزة الحاسوب وشبكة الأنترنت والفضائيات من أجل أغراض التخويف أو الإرغام لأغراض سياسية، أو الإقناع الفكري والتثقيف السلبي والعدواني،²³ ويرتبط الإرهاب المعلوماتي إلى حد كبير بالمستوى المتقدم للغاية والذي باتت تكنولوجيا المعلومات والإعلام تؤديه في جميع مجالات الحياة في العالم، ويمكن أن يتسبب الإرهاب المعلوماتي في إلحاق الشلل بأنظمة القيادة والسيطرة والإتصالات أو قطع شبكات الإتصاليين والوحدات والقيادة المركزية وتعطيل أنظمة الدفاع الجوي وغيرها.²⁴

الحروب السببرانية: (Cyber Warfare):

تشمل الحروب السببرانية الناجحة على أكثر من «مشغلي» حروب إلكترونية، وتعتمد على فريق من المختصين في المعارك الإلكترونية، حيث كل منهم يتميز بمسؤولياته ومهاراته الخاصة لترسيخ القدرة على القتال والتحكم بها وإيرازه ضمن الفضاء السببراني، ويقوم مشغلو «الحروب السببرانية» بالتخطيط للنشاطات الهجومية والدفاعية وإدارتها وتنفيذها عبر الفضاء السببراني.²⁵

6-1 تأثير التهديد السببراني على الأمن الوطني:

تتلورت المصالح الوطنية للدول في الفضاء السببراني، إثر تزايد الإعتماد على ربط البنى التحتية لها، بذلك الفضاء في بيئة عمل تشابكية واحدة، تعرف بالبنية التحتية الوطنية

مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري

المعلومات (NTI)، فأى هجوم أو تهديد محتمل على تلك المصالح قد يشكل حدوث عدم توازن إستراتيجي، وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي للدول، وأبرزها:²⁶
- تزايد إرتباط العالم الفضائي السيبراني، الأمر الذي اتسع معه خطر البنية التحتية الكونية للهجمات السيبرانية؛

- راجع دور الدولة في ظل العولمة وإنسحابها من بعض القطاعات الإستراتيجية لمصلحة القطاع الخاص؛

- نشوء نمط جديد من الضرر على خلفية الهجمات السيبرانية، يمكن تسببه الدولة (أ) للدولة (ب) دون الحاجة للدخول المادي إلى أراضيها؛

- تحول الحروب السيبرانية إلى إحدى أدوات التأثير في مستويات مراحل الصراع المختلفة؛

- توظيف الفضاء الإلكتروني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيانات المختلفة، وبالتالي ظهر ما يسمى بـ "الإستراتيجية السيبرانية" للدول؛

- إتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء الدول أو من غير الدول.

فنفرض طبيعة المجال الذي يتعرض له الأمن القومي للمخاطر السيبرانية، إجراءات وأساليب مناسبة يمكنها الحفاظ عليه، فالأسلحة التقليدية منها المتطورة، وحتى النووية، عاجزة عن حماية "الفضاء السيبراني" (Cyber Space)، بل أن القواعد العسكرية، وأجهزة الإتصال وغيره، يمكن أن تكون هي نفسها هدفا لمقتحمي الأنظمة المعلوماتية والمواقع، لكن ذلك لا يمنع أوجه التشابه بين سياسات الأمن، كما لا يمنع إعتداد بعض المبادئ في سياسة وإستراتيجية الدفاع والحماية.

وعلى خطّ مواز يشمل الأمن الوطني، أمن المعلومات ليس فقط بالمعنى المادي، أي ضمان عدم تخريبها، أو تشويهها، والقضاء عليها أو سرقتها، بل أيضا ضمان سرّيتها، وعدم إطلاع الآخرين عليها ومصادقتها وصحتها،²⁸ ومن أهم سمات المخاطر السيبرانية التي لها تأثير على الأمن القومي ما يلي:

السرعة الفائقة: هناك فجوة في السرعة بين الدول المتقدمة والنامية، ومن أمثلة هذا التسارع تنامي معدل المعاملات الإلكترونية العالمية عبر شبكات الأنترنت؛

اللامحدودية: (انهيار الفواصل الجغرافية): يحقق النظام الدولي للمعلومات الفرصة للجميع من أجل الخروج إلى العالمية، فوق كل الحدود، وفوق كل الفواصل، ويخلق ما يسمى "الفضاء اللامتناهي" يتسابق فيه الجميع نحو تلك العالمية؛

اللازمنية: (التنافس في الوقت): يتسم النظام الدولي للمعلوماتي بالعمل في الزمن الحقيقي، حيث تعمل كل المواقع والخدمات بلا توقف في جميع أنحاء العالم 24س/7 بالرغم من الفواصل الزمنية؛

اللامادية: (تساؤل قيمة المكونات المادية): تضاعلت قيمة المكونات المادية إلى 30% من قيمة المنتج، فإنها قد وصلت إلى حوالي 10% سنة 2011.²⁹

فيما أن المخاطر السيبرانية ترقى إلى مستوى الأمن الوطني ككل، فإن وسائل المواجهة والحماية لا بد وأن تظلها منظومة الأمن الوطني، لأنه من الخطأ أن تكون الأخطار والتهديدات شاملة وربما منسقة ومخططة أحيانا: ثم تأتي سبل وسائل مواجهتها جزئية وعفوية وخالية من التخطيط وتفقر للتنسيق والرشد، فإدارة التهديدات السيبرانية داخل البنية المعلوماتية الوطنية يتطلب بينتين للأمن الوطني (بنية داخلية وبنية خارجية):³⁰

البنية الداخلية للأمن الوطني: إدارة التهديدات المتداولة داخل البنية المعلوماتية الداخلية يتطلب فهما ورؤية جديدة لأساليب ومناهج وأدوات تداول المعلومات بين الدولة الواحدة أو بينها وبين أفرادها، ومجتمعاتها ومؤسساتها الحكومية وغير الحكومية؛

البنية الخارجية للأمن الوطني: إدارة التهديدات يتطلب مناهج وأدوات وأساليب بين الدولة وباقي الدول الأخرى والفواعل الرسمية وغير الرسمية.

المحور الثالث: مكانة الأمن السيبراني في السياسة الأمنية للجزائر:

لقد وضعت الجزائر الأمن السيبراني أحد أولوياتها على غرار باقي دول العالم التي سارعت إلى مراجعة سياساتها الأمنية، وإدراجها الآليات وميكانزمات جديدة تعني بهذه المسائل، بالموازرة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي، ويفرض مطالب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية. لقد أصبح الأمن السيبراني ركن أساسي ضمن العقيدة الأمنية الجزائرية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزتها المختلفة، ولا ننسى كذلك الجانب القانوني والمشرع الجزائري وكيف قام بمواجهة هذه الجرائم والاعتداءات الأمنية وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحاً تصاعدياً في الأونة الأخيرة، ولهذا فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم السيبرانية.

1-2 الأجهزة العملية المختصة في الأمن السيبراني:

إن المحيط الكمي لإجرام المعلوماتية في الجزائر غير واضح لعدم وجود دراسات وبحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في بلادنا جراء هذا النمط الإجرامي. وإن كانت الجزائر ليست بمنادى عن خطورة الجرائم المعلوماتية طالما أنها تحتل جزءاً من الفضاء الإلكتروني خاصة فيما يتعلق بالحاسوب المالية وبعض الهيئات الحكومية التي يعتبر إختراق مواقعها ضمن حجم الأضرار الناتجة عن الجريمة المعلوماتية.

مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني:

وقد أنشئ في سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، وهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رابيس، وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا

مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري

كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية وللبنوك.³¹

ويهدف هذا المركز إلى مساعدة الأجهزة الأمنية الأخرى بالتعاون من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال استغلال المعلومة من خلال تنسيق مع وزارة العدل وكذا من خلال معهد خاص بعلم الإجرام لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، فالجزائر تعمل جاهدا على الإستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها³²:

الوقائية: وتشمل حملة تحسيسية وتوعية بالتنسيق مع وزارة التضامن الوطني والأسرة، والعمل على ملتقيات ومحاضرات وأياما دراسية ومنتديات دولية، ومشاركة في منتديات صحفية وحصص تلفزيونية وإذاعية وغيرها من وسائل النشر والإشهار.

المكافحة: توعية الجزائريين من خلال استعمالهم لشبكات التواصل واستخدام الأنترنت وذلك من خلال تعليقاتهم المدافعة عن الجزائر ومعرفة الأخطار بسلوكيات مشبوهة أو اعتداءات عبر نشر فيديوهات توصل إلى الجناة، مما يسهل التحقيق لدى مصالح الدرك وإلقاء القبض على المشبوهين ومرتكبي الجرائم في الوقت المناسب.

المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة³³.

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني «ببوشاوي»، حيث تم إنشائه بموجب مرسوم رئاسي 133/04 المؤرخ في 26 جوان 2004، ودخل حيز الخدمة ابتداءً من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و2009 كرس لتكوين المورد البشري واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية، ضبط الشرطة القضائية والسلطات المؤهلة، قانونيا خاصة أثناء معالجة القضايا المعقدة³⁴.

والإسهام في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية، ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات؛ مصلحة البيئية؛ أما في ما يخص مجال الأمن السيبراني هناك **مصلحة الإعلام الآلي**؛ على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الإختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية³⁵.

المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

إستجابةً لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.³⁶

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 261-15 وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديريةية يرأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.³⁷

وكلفت الهيئة بإقتراح عناصر الإستراتيجية 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 جرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة

وقد نص سابقا على إنشاء هذه الهيئة المادة 13 من القانون 09/04 المؤرخ في أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال: «تنشأ هيئة وطنية وتنظيمها وكيفية سيرها عن طريق التنظيم» أما مهامها فقد أوردت المادة 14 من نفس القانون وتتمثل في:³⁸

أ- الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الإتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء، إختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية... الخ

ب- مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: بحسب نص المادة 14 من القانون 09/04 هناك نوعان من المكافحة تقوم بهما هذه الهيئة:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن

مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري

الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة (ب) من القانون 09/04؛

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،⁴⁶ يقترح المشروع في هذا الفصل إنشاء هيئة وطنية مختصة تتولى مهام أهمها: تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية ومصالح الشرطة القضائية من التحريات التي تجريها بشأن هذه الجرائم، وما تقوم به أيضا من تجميع المعلومات من نظيرتها في الخارج قصد محاربة هذا النوع الخطير من الإجرام.³⁹

2-2 معوقات تحقيق الأمن السيبراني الجزائري في ظل تحديات الراهنة:

إن الأطروحات الجديدة للأمن تستوجب علينا التوقف والتمعن في هذا المفهوم بما ينسجم والتغيرات الحاصلة في العالم، لاسيما في ظل التطور الرهيب في مجال الإعلام الآلي وتكنولوجيا الاتصالات والمعلومات، إلى حد التوجه إلى إنشاء ما اصطلح على تسميته بالمدن الذكية، والتي تحولت فيها الخدمات من الشكل التقليدي إلى الإلكتروني، لتخلق بذلك ميداناً جديداً يختلف عن سابقه، وعلى الرغم من إيجابياته إلا أنه يستلزم توفير الأمن لنجاح هذه الخدمات.

وعلى الرغم من حداثة التوجه الجزائري نحو «الحوكمة الإلكترونية»، إلا أن عدد الجرائم المرتكبة يوحى بحجم الأخطار التي تتربصها، وهو ما يجعل الجزائر أمام تحديات وعوائق جديدة وهو تحقيق الأمن السيبراني حاليا ومستقبلا.

إذ تواجه مصالح الدرك الوطني ومصالح الأمن الوطني العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن السيبراني في الجزائر، يمكن أن نذكر أهمها بما يلي:

-التطور التكنولوجي وظهور الأنترنت (WiFi/3G/4G/5G) عبر هذه التقنيات لم يعد المجرم يحتاج للجلوس وراء الحواسيب الموصولة سلكيا بشبكة الأنترنت للقيام بجريمته، مما يستدعي من الجهات الأمنية رفع التحدي والاستعداد بأحدث التقنيات لمواجهة والتصدي لهذه التطورات⁴⁰؛

-الإستعمال الواسع لشبكات التواصل الإجتماعي، إذ وصل عدد مستعملي هذه المواقع في الجزائر الإلكترونية لأكثر من 13 مليون مستعمل ما ساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم الإلكترونية مثل القذف، التحرش الجنسي، إستغلال القصر، وغيرها وهذا ما يستوجب وضع إستراتيجيات جد مكتملة لضمان الأمن السيبراني عند إستخدام مواقع التواصل الإجتماعي.⁴¹

عمليات التخفي أثناء إستعمال خدمات شبكة الأنترنت (Proxy)، يعد من أكبر الإشكاليات التي تواجهها الجهات المتخصصة بالتحقيق، ويتطلب تعاون جهات متعددة والتسلح بالوسائل

المتطورة التي يمكن لها رصد الجزئيات وفك الشفرات وتطوير البنى الخاصة بالمعلومات وتحديثها باستمرار، وتصميم برامج عالية التطور⁴²؛ غياب التنسيق بين الدول والحكومات إذ من المعلوم أن الجريمة الإلكترونية عابرة للحدود والقارات، وهو ما يعني أن مرتكبيها يمكنهم النفاذ إلى أنظمة الحاسوب في أحد الدول، يتم التلاعب وإختراق البيانات في بلد آخر، تسجل النتائج في بلد ثالث⁴³، ناهيك عن أنه من الممكن وكل هذا يساعد المجرم الإلكتروني في إخفاء هويته ونقل الموارد من خلال قنوات موجودة في بلدان مختلفة، وبالتالي ونتيجة القدرة على التنقل إلكترونياً من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، تصبح عدة دول ومحاكم وقوانين معينة بذلك، ما يشكل تحدياً حقيقياً، وذلك فإن المحاربة الفعالة للجريمة الإلكترونية تستدعي تعاوناً متزايداً سريعاً وفعالاً على أعلى درجات التنسيق⁴⁴.

التطور التكنولوجي في مجال الأنترنت والاتصالات وهو ما يفرض على الأجهزة الأمنية المختصة بأن تسير هذا التطور، سواء من حيث إكتساب التكنولوجيا أو من حيث التمكن من استخدامها وإستثمارها بالشكل اللازم⁴⁵ هذا ما يُرهق ميزانيتها المحدودة ولذلك يتوجب تركيز جميع الإمكانيات المادية، المالية والبشرية اللازمة لتحقيق الأمن السيبراني.

2-3 مستقبل الأمن السيبراني في الجزائر:

لا يمكن مناقشة مستقبل «الأمن السيبراني» دون النظر في الإتجاهات الناشئة في مجال التكنولوجيا والتهديدات المرتبطة بإستخدامها، إذ تقوم المنظمات المختصة بتطوير وإعتماد التكنولوجيات المتصلة بالبيانات الكبيرة والحوسبة الإدراكية، مما يجعل الأبعاد السيبرانية تنمو في الحجم والتعقيد بصورة مطردة، ولقد طور المختصون نماذج وطرق حديثة ومناسبة للإستفادة من هذه المعلومات في حملات الدعاية والتسويق الذكي⁴⁶، لكن نظرة المختصين في أمن المعلومات كانت حتى فترة قريبة تركز على تكنولوجيا الأجهزة والابتكارات التي تشكل ترابط عالمنا، حيث تصدر كميات هائلة من البيانات بسرعة مع تزايد عدد الأجهزة المرتبطة بالقضاء السيبراني.

بينما تمثل البيانات الكبيرة وإستخداماتها أهدافاً محتملةً للمحتالين⁴⁷، فإن هذه البيانات يمكن أن تساعد المختصين في أمن المعلومات على كشف النشاط الإجرامي الذي يترك دائماً وراءه أدلة رقمية، إذ يقوم المحللون المعنيون بإستخدام هذه البيانات للتنبؤ بالهجمات وتحديد الهجمات الفاعلة الخبيثة قبل وقوع الضرر بيد أن عملية تحليل الملايين من السجلات قد تستغرق أياماً من العمل الحاسوبي، وهنا تأتي الإستفادة من منهجية الأمن المعرفي التي تركز على مبدأ آلة التعلم، إذ يقوم محترفو تكنولوجيا المعلومات بصياغة نماذج ذكية يمكنها معالجة بيانات التهديد بصورة أكثر كفاءة وفاعلية ودقة للتنبؤ بالنشاط الإجرامي⁴⁸.

وثمة ضرورة للتصدي بشكل إستباقي للتهديدات الجيوسياسية التي أدت إلى ظهور هجمات أمنية معلوماتية من نوع جديد ومُعقد توجهه بعض الدول أو الأفراد، إذ تتصدى العديد من المؤسسات لذلك من خلال نشر أدوات متخصصة⁴⁹، مثل رصد المعلومات وتحليلها وتبادلها بشكل مباشر، إضافةً إلى بناء ثقافة أمنية مقبولة، وكل ذلك بهدف الإسهام في خلق بيئة آمنة في المجتمع والأعمال المختلفة⁵⁰.

كما أن التوجهات العالمية الجديدة تفرض تحقيق خطة التنمية لعام 2030 وأهداف القمة العالمية لمجتمع المعلومات للفترة ما بعد عام 2015 (wsis+10) على الدول العربية، والتي تعد الجزائر من بينها، عدة التزامات، منها تنفيذ الخطط العالمية التنموية⁵¹، ومجابهة التحديات التي تحول دون تنفيذها. وذلك من خلال إبداء الإلتزام، السياسي اللازم وتحديث الإستراتيجيات، لاسيما تكنولوجيا المعلومات والاتصالات، بما يتلاءم مع الأهداف التنموية الجديدة ووفقاً لأولويات الدول العربية بما فيهم الجزائر.⁵²

بالإضافة إلى الجريمة السيبرانية، يجب أن تهتم الجزائر دول الجوار بالإرهاب السيبراني والحرب السيبرانية، ويجب أن تضمن إستراتيجية حقيقية شاملة للأبعاد الثلاثة في إستراتيجية «الدفاع السيبراني»⁵³ كما أنه من التحديات المستقبلية ستشمل على نحو متزايد صراعات في الفضاء السيبراني في جميع الأبعاد، وبما أن «الفضاء الإلكتروني» هو مسرح جديد للعمليات في القرن الحادي والعشرين، فإن القوات المسلحة الحديثة لا يمكنها ببساطة أن تعمل بفعالية دون وجود شبكة اتصالات ومعلومات مؤثرة بها ومرنة، لذلك من المهم أن تتمتع الدولة الجزائرية بقدرة على التحكم في الفضاء السيبراني ويعد إطلاق الجزائر أول قمر صناعي للاتصالات بالتعاون مع الصين خطوة مهمة نحو تأمين مؤسساتها وتحقيق الأمن السيبراني.⁵⁴

الخاتمة

إن التهديدات السيبرانية هي خطر الحاضر والمستقبل، والأخطبوط الذي أنتجته الحضارة التقنية والثورة المعلوماتية التكنولوجية، الذي إمتدت أذرعه في جميع أنحاء العالم، ولم تغلت من قبضته الدول الضعيفة والمتطورة على حد سواء، وبات خطراً مدمراً لمختلف القطاعات الحياتية، الإقتصادية منها والإجتماعية والسياسية، وحتى الشخصية، فأصبح العالم يعيش زمن «الإستعمار السيبراني» بكل أشكاله ومظاهره الذي يستهدف التأثير بشكل مباشر وغير مباشر على شكل سلوكيات الفواعل الدولية وغير الدولانية.

فالأمن السيبراني مفهوم متعدد الأبعاد والمستويات، يبدأ بتحقيق أمن الدولة ثم أمن المجتمع وكذا أمن الأفراد، ليسع بعد ذلك كافة الدوائر التي يمكن أن تكون مصدراً للتهديد، سواء كانت في البيئة الداخلية أو الخارجية أو متداخلة بين الداخل والخارج، فالتطورات المعاصرة لثورة المعلومات أدت إلى إتساع نطاق مفهوم الأمن السيبراني، بحيث أصبحت المتغيرات الأمنية الإلكترونية، متغيرات حاكمة بالنسبة للعديد من البيانات والقرارات بدرجة لم تكن معهودة من قبل.

والتهديد السيبراني في الجزائر يعد من أهم التحديات الجديدة للسياسة الأمنية الجزائرية، التي فرضتها التطورات التكنولوجية المتسارعة، ومع تصاعد التحول الجزائري نحو بناء مجتمع معلوماتي، وإنشاء حكومة إلكترونية، وتكثيف الإعتماد على أدوات تكنولوجيا المعلومات والاتصالات، أدركت الأجهزة الأمنية الجزائرية أنه يتوجب عليها تأمين هذه المعلومات بشدة، لأن تداولها وإدارتها إلكترونياً عبر شبكات المعلومات والاتصالات، التي تربطت محلياً وإقليمياً وعلمياً، جعلها معرضة لخطر الإختراقات المعلوماتية.

ويُستنتج من خلال ما سبق:

1- أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانات تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار وتهديدات سيبرانية، تؤدي إلى تحول الفضاء السيبراني لوسيط ومصدر لأدوات للصراع المتعدد الأطراف؛

2- من بين العوامل التي تسهم في تطور المقاربة الأمنية الجزائرية، الدور البارز للعولمة والثورات التكنولوجية في مجالات الإتصالات، السابير والفضاء الخارجي، وما لا يُلاحظ أن العقيدة الأمنية الجزائرية تحاول التكيف مع ما هو مستجد من تهديدات أمنية خاصة تلك التي تتعلق بالتهديدات السيبرانية والتكنولوجية التي أصبحت هاجسا يُهدد أمن كل الدول.

1. سعد علي الحاج علي بكري، «الأمن السيبراني ومعضلة حمايته.. عجلة التعليم العالي.. الرقمي»، جريدة العرب الاقتصادية الدولية، العدد 25، (24 أوت 2017)، ص 24.
2. أحمد عبيس نعمة الفتلاوي، «الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر»، مجلة المحقق الخلي للعلوم القانونية والسياسية، العدد الرابع، (السنة الثامنة، 2016)، ص 214.
3. تولاي آسر، «ما هي السيبرانية؟ وما دورها في صناعة القرار؟ الحياة»، ع. 123، ص ص 41-32.
4. منى الأشقر جبور، «السيبرانية هاجس العصر»، (بيروت، المركز العربي للبحوث القانونية والقضائية، 2013)، ص 29.
5. منى الأشقر جبور، «الأمن السيبراني: التحديات ومستلزمات المواجهة»، المركز العربي للبحوث القانونية والقضائية، (مايو 2012)، ص 16.
6. أوس مجيد غالب العوادي، «الأمن المعلوماتي السيبراني»، (بيروت، مركز البيان للدراسات والتخطيط، 2016)، ص 06.
7. محمد مختار، «هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية؟»، اتجاهات الأحداث، العدد 06، (يناير 2015)، ص 06.
8. حمدون توريه، «الأمن السيبراني في لبلدان النامية»، الاتحاد الدولي للاتصالات، (2006)، ص 15.
9. طارق المجنوب، «ساحة «خفية» لحرب «ناعمة» قادمة!»، منشورات الدفاع الوطني اللبناني، العدد 89، (تموز 2014)، ص 58.
10. نوران شفيق، «أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني»، (القاهرة، المكتب العربي للمعارف، 2014)، ص 40.
11. عادل عبد الصادق، «خطر الحروب «السيبرانية» عبر الفضاء الإلكتروني»، مجلة الأهرام لكمبيوتر الانترنت والاتصالات، (مارس 2017)، ص 27.
12. اسماعيل قادي، «إدارة الحروب النفسية في الفضاء الإلكتروني: الاستراتيجية الأمريكية الجديدة في الشرق الأوسط»، الندوة الدولية: عولة الاعلام السياسي وتحديات الأمن القومي للدول النامية، جامعة الجزائر 3-، 2016 ص 05.
13. كلثوم بيميمون، «السياسات «التفافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية»، مجلة «إضافات» العدد 23، (ربيع 2016) ص 26.
14. محمد سعد أبو عامود، «المفهوم العام للأمن المعلوماتي»، (مصر، جامعة حلوان، 2013)، ص 07.
15. CERT-UK. Common Cyber Attacks Reducing The Impact of the Information Security of GCHQ. 2015. P 05.
16. أحمد السيد النجار، محمد عبد الهادي علام، «حروب المعلومات.. من يواجهها؟»، مجلة الأهرام، العدد 139، (13 يوليو 2015)، ص 26.
17. عادل عبد الصادق «الفضاء الإلكتروني وتحديات جديدة للأمن القومي»، المركز العربي للأبحاث الالكترونية، (2012)، ص 13.
18. نانسي البنا، «الأمن السيبراني.. بيئة تكنولوجية أكثر أمنا»، 20 جانفي 2018/21:14 http://boutiqueceena325/ ezez/rdoc329.eg
19. حسن بن أحمد الشهري، «الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس»، مركز النور للأبحاث الإلكترونية، (2010) ص 11.
20. ذياب موسى البديانة، «الجرائم الالكترونية: المفهوم والأسباب، ملتنقى علمي حول: الجرائم المستحدثة في ظل المتغيرات والتحولت الإقليمية والدولية»، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية، (2014)، ص 05.
21. أمجد المنيف «الإرهاب الإلكتروني- معركة حديثة»، المجلة العربية العربية، العدد 07، (يوليو 2015)، ص 02.
22. إدريس بن الطيب عطية «الظاهرة الإرهابية في زمن ما بعد الحداثة، دراسة تحليلية في الأشكال والأساليب والإجراءات المضادة»، المجلة العربية للدراسات الأمنية والتدريب، المجلد 31، العدد 63، الرياض، (2015)، ص ص 24 25.
23. Timothy Franz. The Cyber Warfare professional Realization for Developing the Next Generation. Summer 2011. p 04.
24. عادل عبد الصادق، «أنماط «الحرب السيبرانية» وتداعياتها على الأمن العالمي»، مجلة الاتجاهات النظرية، البنك العربي الافريقي، (14 ماي 2017)، ص 32.
25. عزيز ملحم بربر، «أمن الشبكات والانترنت»، (القاهرة، جامعة نايف العربية للعلوم الأمنية، 2008)، ص 04.
26. محمد علي قطب، «الجرائم المعلومات وطرق مواجهتها»، مركز الاعلام الأمني، الأكاديمية الملكية للشرطة، (2009)، ص 11.
27. جمال محمد غيطاس، «الأمن المعلوماتي والجرائم الالكترونية.. أدوات جديدة للصراع»، (القاهرة، مركز الجزيرة للدراسات، 2012)، ص 06.
28. زهوة خلوط، «التسويق الابتكاري وأثره على بناء ولاء الزبائن، دراسة حالة: مؤسسة اتصالات الجزائر»، رسالة ماجستير، (جامعة المحمد بوقرة، بومرداس، كلية العلوم الاقتصادية تجارة وعلوم التسيير، 2013- 2014)

29. نعيمة برنيس، «الوظيفة الإعلامية لشبكة الأنترنت في عصر ثورة المعلومات»، رسالة ماجستير، (جامعة منتوري قسنطينة، كلية العلوم الإنسانية والاجتماعية، فرع: صحافة مكتوبة وسمعية بصري، 2010-2009)، ص 101
30. باديس لويس، «جمهور الطلبة الجزائريين والأنترنت، دراسة في استخدامات إشباعات طلبة جامعة منتوري قسنطينة»، رسالة ماجستير، (جامعة منتوري- قسنطينة، كلية العلوم الإنسانية والعلوم الاجتماعية، قسم علوم الإعلام والاتصال 2008-2007)، ص 62.
31. خيرة رواحي، «ثقافة الأنترنت: دراسة ميدانية لاستعلامات الشبكة بمدينة تيهيرت»، رسالة ماجستير، (جامعة وهران، كلية العلوم الإنسانية والحضارة الإسلامية، قسم علم المكتبات والعلوم الوثائقية، 2010-2009)، ص 78
32. هند علوي، «المركز الوطني لجمع المعلومات بالجزائر، قياس النفاذ إلى تكنولوجيا المعلومات والاتصالات بقطاع التعليم بالشرق الجزائري»، أطروحة دكتوراه، (جامعة منتوري- قسنطينة، كلية العلوم الإنسانية، تخصص: علم المكتبات 2008-2007)، ص 41
33. مراد كريم، «مجمع المعلومات أثره في المكتبات الجامعية، مدينة قسنطينة-أمؤذجا-»، أطروحة دكتوراه، (جامعة منتوري - قسنطينة، كلية العلوم الإنسانية والاجتماعية، قسم علم المكتبات، 2008-2007)، ص 36.
34. أمينة بن عبد ربه، «النظام الإقتصادي الجديد المبني على المعرفة وتطور مجتمع المعلومات والتكنولوجيا الحديثة للإتصال، الحلول المقترحة لإرساء مجتمع معلومات ناجح ومتكامل في الجزائر»، رسالة ماجستير، (جامعة الجزائر كلية العلوم السياسية والإعلام، قسم علوم الإعلام والاتصال، 2006-2005)، ص 35-33
35. عادل غزال، «مشاريع الحكومة الإلكترونية من الاستراتيجية إلى التطبيق، مشروع الجزائر: الحكومة الإلكترونية 2013 - أمؤذجا»، مجلة المكتبات والمعلومات، العدد 34، (مارس 2014)، ص 64
36. إلياس شاهد، الحاج عرابية، عبد النعيم دفرو، تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث، (2016)، ص 130
37. عبد القادر عيان، «تحديات الإدارة الإلكترونية في الجزائر، دراسة سوسولوجية ببلدية الكاليتوس العاصمة»، أطروحة دكتوراه (ل م د)، (جامعة محمد خيضر - بسكرة، كلية العلوم الإنسانية والاجتماعية، 2015 تخصص: إدارة وعمل 2016)، ص 91
38. أسامة بن صادق طيب، محمد نور بن ياسين فطاني، عصام بن يحي الفيلالي، «الحكومة الالكترونية، نحو مجتمع المعرفة»، معهد البحوث والاستشارات، العدد التاسع، جامعة الملك عبد العزيز، جدة، السعودية، (2013)، ص 04.
39. سمير بارة، «الدفاع الوطني والسياسات للأمن السيبراني (Cyber Security) في الجزائر: الدور والتحديات»، جامعة قاصدي مرباح، ورقلة، ص 445
40. سهام بو عموشة، «الفضاء السبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية»، جريدة الشعب، العدد 17345، 24 ماي (2017)، ص 06
41. نسيمة سحواذ، «الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى»، في: 02 مارس 2018/13:63 http://Dikanews1322-pdf04L36/44.com
42. إدريس عطية، تطبيقات الهندسة الأمنية في سياسة الجزائر الإفريقية (الجزائر: دار الأمة، 2019)، ص 34.
43. أحمد غاي، «تكيف الشرطة القضائية مع متطلبات إصلاح العدالة، تقييم وآفاق»، في: 03 مارس 2019/14:13 w.w.w.mjjustice/3216PDF1470sany55 .dg
44. عبد القادر سعدي، «المصلحة المركزية الالكترونية في مواجهة مجرمي العالم الافتراضي»، في: 03 مارس 2019/17:42 www.essalamonline.s-doc896-24h/Lmnoq.com
45. راضية مناد، «تطوير قدرات الشرطة في مواجهة الجريمة الالكترونية، أمن واستراتيجية»، 03 مارس 2019/21:19www.dgayerinfo-pdf526/33s.com .
46. Dan Craiye and others, "Defining cybrescurity", Technology innovation management review, Montreal, Canada, (october 2014).p14.
47. الجريدة الرسمية، «القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وطرق مكافحتها»، الفترة التشريعية السادسة، السنة الثالثة، الدورة الرابعة، رقم 122، (27 يونيو 2009)، ص 04
48. إسماعيل حنة، «حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون»، مجلة الجيش، العدد 599، (جوان 2013)، ص 14
49. James Johnson, "Artificial intelligence & future warfare: Implications for International Security", Defense & Security Analysis, Vol. 35, no. 2, (2019), PP. 147-169.

50. مصطفى عباتي، «التدابير الأخرى في مجال نزع السلاح والأمن الدولي»، اللجنة الأولى للدورة الـ 71 الجمعية العامة للأمم المتحدة، بعثة الجزائر الدائمة لدى الأمم المتحدة، نيويورك، 24 أكتوبر 2016، ص 02
51. سليمة مقراني، «الجيش الوطني الشعبي: ملتقى حول الدفاع السيبراني، مكون أساسي للأمن والدفاع الوطني» في: 07 مارس 2019 [https :www.eljournhouria471PH///OR25scc3.dg](https://www.eljournhouria471PH///OR25scc3.dg)
52. فواز العنزي، «أمن المعلومات والقرصنة الإلكترونية، مجلة التقدم العلمي»، العدد 99، (أكتوبر 2017)، ص 96
53. James Johnson, “Artificial intelligence & future warfare: Implications for International Security”, Defense & Security Analysis, Vol. 35, no. 2, (2019), PP. 147-169.
54. صالح ميهوبي، «جرائم الانترنت تنخر المجتمع الجزائري»، جريدة البلاد، العدد 18، 5369 (جويلية 2017)، ص 07.