مجلة البحوث في العقود وقانون الأعمال
The Journal of Research in Contracts and Business Law
المجلد 10 / العـدد: 02 (2025)، ص 456–467

الهجمات السيبرانية و تحديات رقمنة القضاء الجزائري

Cyber Attacks and the Challenges of Digitalizing the Algerian Judiciary

مبروك تيزيري* [1] ، بن طيبة شفيق [2]

[1] جامعة عبد الرحمان ميرة، بجاية (الجزائر)، Mebrouk.tiziri@droit.univ-bejaia.dz

مخبر البحث حول فاعلية القاعدة القانونية

[2] جامعة يحي فارس، المدية(الجزائر) ، bentiba.chafik@univ-medea.dz

مخبر السيادة والعولمة ،

تاريخ الاستلام: 2025/02/09 تاريخ القبول: 2026/04/23 تاريخ النشر: 2026/06/06

ملخص

تعد فكرة الهجمات السيبرانية وليدة ما توصل إليه الفكر البشري من تطور معرفي وتكنولوجي، فأصبحت من أكثر التهديدات التقنية الخطيرة التي تشكل هاجسا أمام القضاء الجزائي الإلكتروني في الجزائر، وذلك راجع لسهولة امتلاك القوة السيبرانية وتعدد الفواعل فيها في الفضاء الإلكتروني، الأمر الذي يترتب عليه تهديدات سيبرانية خطيرة من شأنها انتهاك أمن وسلامة المعلومات القضائية وتدمير خدمات القضاء الجزائي المعلوماتي في الجزائر، و عليه فإنه سينصب التركيز في هذا البحث معرفة خطر الهجمات السيبرانية وأنماطها المتعددة من ناحية، وتحديات رقمنة القضاء الجزائري.

الكلمات المفتاحية: الهجمات السيبرانية، التقاضي الإلكتروني، المادة الجزائية، الأمن السيبراني، الخدمة الإلكترونية.

Abstract:

The idea of cyber attacks is the product of the cognitive and technological development achieved by human thought. They have become one of the most serious technical threats, constituting a major concern for electronic criminal justice in Algeria. This is due to the ease of acquiring cyber power and the multiplicity of actors operating within cyberspace, which results in serious cyber threats capable of violating the security and integrity of judicial information and undermining the functioning of digital criminal justice services in Algeria. Accordingly, this research focuses on identifying the risks posed by cyber attacks and their various patterns on the one hand, and the challenges facing the digitalization of the Algerian judiciary on the other**.**

Keywords: Itigation, criminal matters, cybersecurity, electronic service.

* المؤلف المرسل.

مقدمة:

أدت التحولات الرقمية في العالم المعاصر إلى خلق بيئة جديدة في الفضاء الافتراضي، لاسيما في ظل ثورة تكنولوجيا الاعلام والاتصال التي يشهدها العالم، فأصبحت تبعا لذلك معظم حكومات العالم تسعى لمواكبة هذا التطور التكنولوجي بغرض الاستفادة من محاسنه.

والجزائر على غرار مختلف دول العالم، واكبت هذا التطور الملحوظ في السنوات الأخيرة من خلال إصدار المشرع الجزائري لقانونه رقم15-03 المتعلق بعصرنة العدالة الجزائرية، وذلك بهدف رقمنة اجراءات التقاضي بوجه عام وإلكترونية اجراءات التقاضي الجزائي بوجه خاص عن طريق استحداث منظومة معلوماتية مركزية لدى وزارة العدل تكون بمثابة المحرك الرئيسي لهذه العملية[1].

إلا أن إنجاح ذلك يبقى مرهونا بمدى قدرة الجزائر على توفير الحماية اللازمة لنظامها المعلوماتي المركزي التابع لأجهزة القضاء الجزائرية عامة والجزائية خاصة، لاسيما في ظل التطورات التي يشهدها سوء استخدام الوسائل الالكترونية الحديثة في الفضاء السبيراني، خاصة في ظل الأزمات السياسية التي تعرفها الجزائر مع دول الجوار واستفحال ظاهرة الارهاب الالكتروني.

من هنا تتجلى أهمية موضوع هذه الورقة البحثية، والتي تستهدف معرفة خطر الهجمات السبيرانية وأنماطها المتعددة من ناحية، وأثار الهجوم السبيراني على النظام القضائي الجزائي المعلوماتي في الجزائر من ناحية ثانية.

انطلاقا مما سبق ذكره، تطرح هذه الورقة البحثية إشكالية البحث التالية: **ما مدى إستعداد القضاء المعلوماتي الجزائي في الجزائر لمواجهة الهجمات السبيرانية المتعددة؟**

للإجابة عن هذه الإشكالية اعتمدت دراسة هذا الموضوع على كل من المنهج الوصفي والتحليلي، من خلال وصف مختلف المفاهيم المرتبطة بالهجمات السبيرانية وانماطها المختلفة، وتحليل مختلف أثارها على أجهزة القضاء الجزائي المعلوماتي في الجزائر، فضلا عن تحليل مختلف النصوص القانونية المتعلقة بهذا الشأن.

وتطلب البحث في هذا الموضوع تقسيمه إلى محورين، أما المحور الأول يتطرق إلى مفهوم الهجمات السبيرانية، ويقسم بدوره إلى عنصرين، الأول يتناول مفهوم الهجمات السبيرانية، بينما الثاني يتضمن انماط الهجمات السبيرانية، في حين خصص المحور الثاني لمعرفة أخطار الهجمات السبيرانية على القضاء الجزائي المعلوماتي، ويقسم هذا المحور بدوره إلى عنصرين، أما العنصر الأول يعالج تجريد النظام المعلوماتي القضائي الجزائي، بينما العنصر الثاني يتعرض لتدمير خدمات النظام المعلوماتي القضائي الجزائي في الجزائر.

المحور الأول : مفهوم الهجمات السيبرانية

إن الظهور الحتمي للفضاء الإلكتروني جراء التطور الهائل الذي يشهده العالم المعاصر في مجال تكنولوجيا الإعلام والاتصال، ساهم في بروز مفهوم جديد للقوى على المستوى الوطني والدولي، وهو ما يصطلح له بالقوة السيبرانية، هذه لأخيرة التي من شأنها أن تستخدم بغرض تهديد الأمن السيبراني للدول ومؤسساتها الحكومية، وذلك من خلال شن هجمات إلكترونية متعددة الأهداف والفواعل[2].

وللتفصيل أكثر في مفهوم الهجمات السيبرانية يقسم إلى شقين، الشق الأول يتطرق إلى فكرة الهجمات السيبرانية، بينما الشق الثاني يتناول أنماط الهجمات السيبرانية.

أولا: فكرة الهجمات السيبرانية

لقد ساهمت تكنولوجيا الإعلام والاتصال في ظهور نوع جديد من القوى في العالم المعاصر، حيث تجعل هذه الأخيرة الفضاء السيبراني محلا لها، وتسعى إلى تحقيق العديد من الأهداف في البيئة الواقعية باستخدام الوسائل الإلكترونية، من خلال السيطرة والتحكم في البنى الإلكترونية عن طريق هجمات إلكترونية متعددة الأشكال[3]، لتمثل بذلك الهجمات السيبرانية ترجمة فعلية للقوى السيبرانية في العالم المعاصر، ومفهوما جديدا للهجمات التي يعرفها العالم الواقعي.

بناء عليه وللإحاطة أكثر بمفهوم الهجمات في الفضاء السيبراني سنتعرف أولا على تعريف الهجمات السيبرانية، بعدها نتطرق إلى أسلحة الهجوم السيبراني.

1: تعريف الهجمات السيبرانية

يعد مصطلح الهجمات السيبرانية من أكثر المصطلحات التي اختلف في تعريفها الباحثون الأكاديميون والمختصون في مجال القانون الدولي العام، إلا أن معظم تلك التعريفات تلتقي في معنى واحد للهجمات السيبرانية، والذي يقصد به استخدام الحاسب الآلي وشبكة الإنترنيت كأداة للتسلل للأنظمة المعالجة للمعطيات التابعة للخصوم، وذلك بغرض تجميع وحيازة البيانات التي تحتويها، أو من خلال التشويش على الاستخدام الفعال للفضاء السيبراني من قبل الخصوم وتعطيل المواقع الإلكترونية التابعة له وتدميرها، بينما يقصد بالخصم في هذا المقام كل الأطراف المستهدفة في عملية الهجوم السيبراني[4].

2: أسلحة الهجوم السيبراني

تختلف طبيعة الأسلحة المستخدمة في هجمات الفضاء الإلكتروني عن نظيراتها في العالم الواقعي، حيث تتمايز هذه الأخيرة بتغييرها التام لمعنى العنف، بالإضافة إلى هيكلتها المتقدمة والمنسقة التي تسمح بشن هجمات إلكترونية ضد عدة خصوم في آن واحد، من خلال وسائل إلكترونية قادرة على تعطيل الحواسيب الرئيسية التي تبنى عليها البنية التحتية الوطنية الإلكترونية للدول[5].

وفضلا عن مختلف الوسائل الإلكترونية التي تكون على شاكلة الحواسيب الآلية كسلاح رئيسي للهجمات السيبرانية، يندرج ضمن مفهوم الأسلحة الإلكترونية كل من الفيروسات باختلاف أنواعها مثل فيروسات التشغيل والعتاد، والبرامج الضارة التي تسوق عبر العديد من التقنيات بغرض إتلاف بيانات الأنظمة الآلية لمعالجة المعطيات، مثل برنامج القنبلة الموقوتة (Bomb) وبرنامج الدودة (Worm)[6].

ثانيا: أنماط الهجمات السيبرانية

تتخذ الهجمات السيبرانية العديد من الأنماط والأشكال في مباشرة عمليات الهجوم الإلكتروني في الفضاء السيبراني على البنية التحتية للنظام الآلي لمعالجة المعطيات التابع لإحدى المؤسسات الحكومية في الدولة، وتكون هذه الهجمات السيبرانية في إطار ما يعرف بالحرب السيبرانية، أو من خلال هجمات خارج هذه الحرب، يغلب عليها الطابع الإرهابي والتخريبي للمنظومة المعلوماتية للدولة[7].

ولأجل البحث أكثر في أنماط الهجمات السيبرانية سنحاول التعرق على الحرب السيبرانية، بعدها التطرق إلى الإرهاب السيبراني .

1: الحرب السيبرانية

يقصد بمصطلح الحرب السيبرانية بأنه كل نزاع مسلح في الفضاء السيبراني بين دولتين أو أكثر، تستخدم الوسائل التقنية الحديثة كأسلحة حربية، وذلك بغرض مباشرة مجموعة من العمليات الحربية الهجومية أو الدفاعية في ساحة الحرب الافتراضية، ويتجسد ذلك من خلال شن هجمات سيبرانية من قبل الدولة المهاجمة تجاه المنظومة المعلوماتية للعدو، يتبعها هجمات مضادة تندرج ضمن الدفاع الشرعي ضد الهجمات السيبرانية الهجومية[8].

هذا وتتنوع الحرب السيبرانية بحسب طبيعة الصراع الحاصل في الفضاء السيبراني بين دولتين أو أكثر، وتعتبر الحرب السيبرانية الباردة والمنخفضة الشدة أولى أنواعه، تتميز هذه الأخيرة بديمومتها وتداخل أهدافها وأسبابها، وذلك خلافا للحرب السيبرانية المتوسطة الشدة والساخنة، والتي يحتدم فيها الصراع بين الدول في ساحة المعركة السيبرانية من خلال استخدام وسائل حربية أكثر تطورا، وأشكال أخرى من الهجوم السيبراني مثل التجسس الإلكتروني[9].

ويعتبر التجسس السيبراني في هذا الإطار أخطر الأساليب التي تفرزها الحرب السيبرانية، من خلال اختراق المنظومة الآلية لمعالجة المعطيات والمواقع الإلكترونية للدولة بغرض التنصت والتطفل لمعرفة ما تحتويه من بيانات ومعلومات نصية كانت أو مرئية مسموعة[10].

2: الإرهاب السبيراني

يعتبر الإرهاب من أكثر القضايا التي شغلت اهتمام الباحثين في العالم المعاصر، ويندرج ضمنه كل عداء يحمله مجموعة من الأفراد للدولة، ويترجمونه من خلال عمليات إجرامية وتخريبية عشوائية كانت أو منظمة، نظامية كانت أو غير نظامية سواء من داخل الدولة أو خارجها، وهو ما يعرف بالإرهاب المحلي والدولي[11].

وفي ظل التطورات الراهنة في مجال تكنولوجيا الإعلام والاتصال أصبحت الجماعات والأفراد النظامية وغير نظامية من خارج وداخل الوطن، يتخذون وسائل حديثة تواكب تطور هذا العصر، من خلال استخدام الوسائل والتقنيات التكنولوجية الحديثة لابتزاز وتهديد السلطات العامة والحكومات ومؤسساتها المتعددة، والسعي نحو الإخلال بالنظام العام عن طريق استهداف المنظومة الحكومية الإلكترونية وإلحاق الضرر بها، أو تدميرها بالكامل مما يترتب عليه زعزعة الأمن السيبيراني داخل الدولة[12].

المحور الثاني : أخطار الهجمات السبيرانية على التقاضي الجزائي الإلكتروني

يقوم التقاضي الإلكتروني بوجه عام والتقاضي الجزائي الإلكتروني بوجه خاص، على مبدأ سيادة الوسائل الإلكترونية المستخدمة في عملية التقاضي الإلكتروني في المادة الجزائية، وما يترتب عنه من سيادة رقمية في الفضاء الإلكتروني لأجهزة القضاء الجزائي الإلكتروني في الدولة[13].

وذلك راجع للضوابط التي تفرضها الحوكمة الإلكترونية على مختلف المؤسسات في الدولة، لاسيما تلك الضوابط التقنية التي يتم من خلال احترامها ضمان أمن وسلامة ودقة مختلف الخدمات الإلكترونية واتاحتها للجمهور، سواء تعلق الأمر بالخدمات الصماء عن بعد أو الخدمة المتطورة الإلكترونية[14].

بناء عليه سنحاول في هذا المحور معرفة أخطار الهجمات السبيرانية على أجهزة القضاء الجزائي الإلكتروني، وذلك من خلال التطرق إلى تجريد النظام القضائي الجزائي المعلوماتي في الشق الأول، بعدها تدمير خدمات التقاضي الجزائي الإلكتروني.

أولا: تجريد النظام القضائي الجزائي المعلوماتي

يفترض في وجود نظام قضائي جزائي معلوماتي تعزيز دفاعته الالكترونية، بما يسمح بأمن بيئته الافتراضية للحيلولة دون أي هجمات على الفضاء المعلوماتي وتهديد السيادة الرقمية[15]، إضافة إلى تحقيق الأمن المعلوماتي من خلال سلامة محتوى البيانات الإلكترونية، وسرية هذه المعلومات الإلكترونية[16]، انطلاقا من ذلك ولأجل البحث في أخطار الهجمات السبيرانية على أمن المعلومات الالكترونية، سنبين أولا إتلاف البيانات القضائية الجزائية الالكترونية، بعدها نخصص الجزء الثاني لمناقشة مسألة السماح بالاطلاع على المعلومات القضائية الإلكترونية.

1: إتلاف بيانات نظام القضاء الجزائي المعلوماتي

أنشأ المشرع الجزائري على غرار مختلف دول العالم المعاصر دعامة إلكترونية تابعة لوزارة العدل، وذلك بموجب قانون عصرنة العدالة رقم 15-03، وهذا بغرض إعطاء السند القانوني للبدء في عملية التقاضي الالكتروني بوجه عام والتقاضي الجزائي الإلكتروني بوجه خاص، من خلال استحداث منظومة معلوماتية مركزية للمعالجة الآلية للمعطيات لدى وزارة العدل، على اعتبار أنها المحرك الرئيس لهذه العملية والحاضنة المركزية للبيانات القضائية الجزائية في الفضاء المعلوماتي[17].

هذا ما يجعل المنظومة المعلوماتية المستحدثة على مستوى وزارة العدل الجزائرية عرضة للهجمات السيبرانية بمختلف انماطها، ولعل أبرز تلك الأنماط المهددة لسلامة وأمن المعلومات القضائية الإلكترونية في المنظومة المعلوماتية المركزية الجزائرية، ما يعرف بالحرب السيبرانية والتي تستهدف مهاجمة النظام المعلوماتي المركزي عن طريق شن هجوم سيبراني على الحواسيب والشبكات التابعة له، مما يخلف أعطال بالغة بالنظام وبياناته القضائية، وهو الأمر الذي ينطبق على الهجمات الإرهابية المستخدمة للوسائل الإلكترونية والهادفة لتعطيل واسع النطاق لشبكات الكمبيوتر وأجهزته وإتلاف البيانات القضائية الإلكترونية[18].

وفي هذا الإطار تحتل الجزائر المرتبة 14 عربيا و108عالميا في مجال الأمن السيبراني، وهي مراتب متأخرة مقارنة بالإمكانيات المادية والبشرية التي تزخر بها البلاد، ذلك ما جعل الجزائر في السنوات الأخيرة تتعرض لحرب سيبرانية مسعورة، الأمر الذي أكده رئيس الجمهورية السيد عبد المجيد تبون في رسالته بمناسبة اليوم الوطني للصحافة الموافق 22 أكتوبر من سنة 2022، وأشار الرئيس الجمهورية وفي نفس السياق أن أكثر من 97 بالمائة من الهجمات السيبرانية التي تتعرض لها الجزائر مصدرها المغرب[19].

ذلك الأمر الذي يثير العديد من المخاوف على مصير البيانات القضائية الجزائية في المنظومة الإلكترونية المركزية التابعة لوزارة العدل الجزائرية، وهذا راجع لم قد ينجم عن تلك الهجمات السيبرانية من أخطار من شأنها الإضرار بسلامة وأمن البيانات القضائية في نظام القضاء الجزائي المعلوماتي ومختلف الشبكات التابعة له على المستوى القطر الوطني الجزائري.

2: الاطلاع على معلومات نظام القضاء الجزائي المعلوماتي

فضلا عن أمن وسلامة المعلومات القضائية في النظام المعلوماتي التابع للقضاء الجزائي في الجزائر، يقتضي الأمر ضرورة المحافظة على سرية النظام والبيانات القضائية الجزائية المخزنة فيه إلكترونيا، وذلك من خلال السماح بالاطلاع على تلك البيانات من قبل اصحابها وحسب، وتفعيل طرق الحماية المناسبة لها للحيلولة دون أي اختراق أو هجوم سيبراني من شأنه القضاء على مبدأ السرية القضائية[20].

ويمثل التجسس السيبراني في هذا المقام أكثر التهديدات التي من شأنها ضرب سرية التبادل القضائي للمعلومات الإلكترونية في المسائل الجزائية، وهذا من خلال محاولة التنصت والولوج للأنظمة الآلية لمعالجة المعطيات بغرض التسلل وحيازة البيانات الإلكترونية وسرقتها، مما يحول دون سرية البيانات القضائية في الدعامة الإلكترونية المخصصة لعملية التقاضي الإلكتروني[21].

وفي سياق متصل تعرض موقع وزارة العدل الجزائري على التويتر في شهر مارس الفارط من سنة 2022 إلى عملية قرصنة من قبل قراصنة مغاربة، وبحسب الوزارة أن العملية استهدفت نشر تغريدات تسيئ للجزائر ومواقفها الدولية[22].

وبالرغم من أن الهجمات السيبرانية الشرسة من قبل الجارة الغربية في إطار الحرب السيبرانية الجزائرية المغربية الباردة والمتوسطة الشدة، لم يلحق إلى حد الساعة أضرار بالغة بالأنظمة الآلية المعالجة للمعطيات التابعة لوزارة العدل الجزائرية والمنظومة المعلوماتية للقضاء الجزائي الجزائري، إلا يثير العديد من المخاوف التي تستلزم مجابهة هذه الهجمات العدائية حفاظا على حسن سير العدالة الجزائية وإلكترونية التقاضي الجزائي في الجزائر، وتحقيق مبدأ سرية البيانات القضائية المعلوماتية في النظام القضائي الالكتروني.

ثانيا: تدمير خدمات القضاء الجزائي الالكتروني

يتيح نظام التقاضي الجزائي الإلكتروني العديد من الخدمات القضائية، من أهمها التبادل الإلكتروني للوثائق والمعلومات القضائية، إضافة إلى التسجيل الإلكتروني للعرائض والدعاوي فضلا عن استخدام الوسائل الإلكترونية في مختلف اجراءات الدعوى الجزائية والخدمات المقدمة[23].

وفي ذلك كفل المشرع الجزائي الجزائري بموجب قانون الإجراءات الجزائية، العديد من الخدمات القضائية الإلكترونية للمتقاضين في المسائل الجزائية، وهذا بداية من تسجيل وتقييد الدعوى الجزائية إلكترونيا في النظام المعلوماتي التابع لوزارة العدل باستخدام الحاسب الآلي، وصولا إلى المحاكمة الجزائية عن بعد باستخدام تقنية الاتصال عن بعد المرئي والمسموع[24].

بناء عليه وللبحث أكثر في مجال الأضرار الناتجة عن الهجمات السيبرانية والماسة بخدمات النظام المعلوماتي للقضاء الجزائي الجزائري، قسمنا الدراسة هنا إلى عنصرين، أما االعنصر الأول يتطرق إلى عرقلة خدمة التقاضي الجزائي الالكتروني، بينما العنصر الثاني يتناول تعطيل خدمة العمل بالنظام الآلي للقضاء الجزائي.

1: تعطيل خدمة التقاضي الجزائي الالكتروني جزئيا

في ظل تذيل الجزائر لقائمة الدول المهتمة بالأمن السيبراني بالرغم من الامكانيات البشرية والمادية التي تزخر بها البلاد، ومع تزايد الهجمات السيبرانية المستمرة ضمن حرب سيبرانية شرسة تقودها المغرب ضد الجزائر، أصبح من الضروري دق ناقوس الخطر.

لاسيما في ظل اتساع البنية الشبكية لخدمة الإنترنيت، والتي من شأنها توسيع خطر الهجمات السيبرانية نظرا للسمات التي تتمايز بها هذه الأخيرة من سرعة فائقة ولامحدودية، بالإضافة إلى التطور التكنولوجي الذي تشهده وسائل الاتصال والإعلام والاستعمال الواسع لها على المستوى المحلي[25].

هذا الأمر الذي من شأنه أن يلحق بالنظام المعلوماتي المركزي التابع لوزارة العدل الجزائرية، العديد من الأعطال مما يترتب عليه حتما عطلا جزئيا لخدمة التقاضي الإلكتروني في المادة الجزائية، ويفرض العديد من التحديات على الجزائر في سبيل المضي بهذه العملية، من أبرزها تطوير دفاعاتها السيبرانية.

2: تعطيل خدمة التقاضي الجزائي الالكتروني كليا

إن الغاية الأسمى من شن هجمات سيبرانية على الأنظمة الآلية لمعالجة المعطيات تتمثل في التدمير الكلي للمنظومة المعلوماتية والشبكية التابعة للحكومات أو المؤسسات التابعة لها، من خلال شن هجومات متعددة على البنية المعلوماتية للدولة ومؤسساتها الحكومية[26]، وهو الأمر الذي يسلب النظام القضائي الإلكتروني بوجه عام والنظام المعلوماتي التابع للقضاء الجزائي أساسهما، ومحور وجودهما ووجود عملية التقاضي الالكتروني، كون أن النظام المعلوماتي التابع لوزارة العدل الجزائرية والمستحدث من قبل المشرع الجزائري بموجب القانون رقم15-03 المتعلق بعصرنة العدالة، يعتبر حجرة الأساس التي لا يمكن الاستغناء عنها في مجال التقاضي الجزائي الإلكتروني وإدارة الدعوى الجزائية إلكترونيا[27].

وفي ذلك يمكن القول إن الهجمات السيبرانية المتعددة قد نجحت في مبتغاها الأساسي من شن الهجوم، وهو ما يتوافق والمميزات التي تسعى إليها فواعلها، من خلال السعي نحو الأسبقية التكنولوجية بتدمير أنظمة الخصوم المعلوماتية، تحقيقا لعدة أهداف سياسية وعسكرية مغرضة يحركها العداء والحقد على الجارة الشرقية الصامدة، الجزائر.

الخاتمة:

بوسعنا أن نستخلص في ختام هذه الورقة البحثية، أن الهجمات السيبرانية من أكثر المسائل التقنية التي تحول دون تطبيق فكرة التقاضي الإلكتروني في المادة الجزائية، وذلك راجع لضرورة توافر مجموعة من الضوابط التقنية للمضي في إلكترونية اجراءات التقاضي الجزائي بالجزائر، من أهمها سلامة وسرية البيئة الافتراضية المتمثلة في المنظومة المعلوماتية المركزية التابعة لوزارة العدل الجزائرية.

ومن بين أهم النتائج التي توصلت إليها هذه الورقة البحثية، ما يلي:

-الهجمات في القضاء السيبراني مفهوم مستحدث أفرزته تكنولوجيا الإعلام والاتصال في العالم المعاصر، من خلال نقل الأعمال العدائية والهجمات الارهابية والحربية من العالم الواقعي إلى العالم الرقمي.

-الهجوم السيبراني أداة تقنية تجرد فكرة التقاضي الالكتروني من معناها، من خلال تجاوز مبادئه في الأمن والسرية، بينما تدمر المنظومة الآلية لمعالجة المعطيات التابعة للقضاء الجزائي الجزائري، عن طريق المساس بالمنظومة المعلوماتية والشبكات التابعة لها.

-تعتبر الحماية التقنية من المتطلبات الضرورية لإنجاح إلكترونية التقاضي الجزائي الجزائري، من خلال ضمان سلامة النظام المعلوماتي وديمومته، والمحافظة على أمن وسرية المعلومات القضائية الالكترونية.

بناء عليه يمكن تعزيز هذه الورقة البحثية بمجموعة من المقترحات، كالتالي:

-ضرورة عمل الجزائر على تطوير البنية التحتية المعلوماتية، من خلال تطوير آليات دفاعية وهجومية في الفضاء الإلكتروني للمحافظة على الأمن السيبراني وتحقيق سيادتها الرقمية.

-السهر على التكوين القاعدي للعاملين بالهيئات المختصة بالأمن السيبراني وطنيا، في مجال تكنولوجيا الإعلام والاتصال.

- ضرورة تجريم بعض السلوكيات المرتبطة بالهجمات السيبرانية كتجريم إختراق الحسابات الإلكترونية الشخصية و المهنية بشكل عام و في نطاق القضاء بشكل خاص

-السعي لإبرام اتفاقيات مشتركة مع الدول الحليفة المتطورة تكنولوجيا، وذلك بغرض الدفاع السيبراني المشترك ضد الهجمات السيبرانية، والتكوين مشترك للتقنيين العاملين في هذا الشأن.

-تحسيس وتوعية المواطنين الجزائريين بأخطار الفضاء السيبراني، وانعكاساتها على الأمن السيبراني وجودة الحياة الاجتماعية والقضائية في الواقع.

قائمة المراجع:

1 الكتب:

1-أحمد سلام عبد العاطي، الحوكمة الالكترونية، مؤسسة طيبة للنشر والتوزيع، الطبعة الأولى، القاهرة، السنة2021.

2-إيهاب خليفة، الحرب السيبرانية-الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، الطبعة الأولى، القاهرة، السنة2020.

3-خالد حسن أحمد لطفي، التقاضي الالكتروني كنظام قضائي معلوماتي-بين النظرية والتطبيق، دار الفكر الجامعي، الطبعة الأولى، الاسكندرية، السنة2020.

4-عبد المجيد مبلغي وآخرون، الإرهاب-تعريفه وآليات مكافحته، ترجمة أحمد الموسوي، الديوان للطباعة والنشر والتوزيع، مركز الحضارة لتنمية الفكر الإسلامي، الطبعة الأولى، بيروت، السنة2016.

2 الرسائل العلمية:

1-نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، السنة2021.

3 المقالات:

1-أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، جامعة الأزهر، القاهرة، المجلد35، الجزء الثالث، العدد03، السنة2020.

2-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة المصداقية، المدرسة العليا العسكرية للإعلام والاتصال، الجزائر، المجلد01، العدد02، السنة2019.

3-بلقاسم بن صابر، محمد حيدرة، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، مخبر حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، المجلد02، العدد02، الجزائر، السنة2017.

4-سعاد قصعة، خديجة قصعة، تحديات الأمن المعلوماتي في مواجهة الجريمة الالكترونية في ظل الاعلام الجديد، مجلة المعيار، كلية أصول الدين جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، الجزائر، المجلد24، العدد50، الجزائر، السنة2020.

5-سهيلة بضياف، آمنة حمراني، أمن المعلومات في الجزائر-الإجراءات والتحديات، المجلة الجزائرية للأمن والتنمية، جامعة الحاج لخضر باتنة، الجزائر، المجلد09، العدد16، السنة2020.

6-صباح كزيز، أمال كزيز، الارهاب الالكتروني وانعكاساته على لأمن لاجتماعي-دراسة تحليلية، مجلة التراث، جامعة زيان عاشور الجلفة، الجزائر المجلد08، العدد02، السنة2018.

7-علاء الدين فرحات، الفضاء السيبراني-تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، المجلد10، العدد03، الجزائر، السنة2019.

8-مراد قريبيز، أمن المعلومات الالكترونية بين متطلبات السيادة الرقمية وجهود المنظمات الدولية والاقليمية، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، الجزائر، المجلد06، العدد01، الجزائر، السنة2021.

9-موسى بن تغري، الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد12، العدد22، الجزائر، السنة2022.

10 -يحي مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي، الجزائر، المجلد14، العدد01، السنة2017.

4 النصوص القانونية:

1- قانون رقم15-03، مؤرخ في11 ربيع الأول عام1436، الموافق لـ 01فبراير سنة2015، يتعلق بعصرنة العدالة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد06، مؤرخة في 10 فيفري 2015.

2-الأمر رقم20-04، مؤرخ في 11محرم عام1442، الموافق لـ 30 غشت سنة2020، يتضمن تعديل قانون الاجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد51، مؤرخة في 21 غشت 2020.

5 مواقع الانترنت:

1-عثمان لحياني، الجزائر تفتح تحقيقا في اختراق وزارة العدل على تويتر، تاريخ النشر 12مارس سنة2022، تاريخ الإطلاع24جانفي سنة2023، على الساعة 11:00.

/https://www.alaraby.co.uk/entertainment_media

2-عمار قردود، حرب سيبرانية مستعرة لاختراق المواقع بين القراصنة الجزائريين والمغاربة، مقالة منشور بتاريخ 14مارس سنة2022، تاريخ الاطلاع يوم23جانفي2023، على الساعة 18:00.

/https://africanews.dz

[1]- قانون رقم15-03، مؤرخ في11 ربيع الأول عام1436، الموافق لـ 01فبراير سنة2015، يتعلق بعصرنة العدالة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد06، مؤرخة في 10 فيفري 2015.

[2]- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، السنة2021، ص07.

[3]- إيهاب خليفة، الحرب السيبرانية-الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، الطبعة الأولى، القاهرة، السنة2020، ص.ص66، 69، 70.

[4]- بلقاسم بن صابر، محمد حيدرة، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، مخبر حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، المجلد 02، العدد02، السنة2017، ص188، 189.

[5]- علاء الدين فرحات، الفضاء السيبراني-تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، المجلد10، العدد03، السنة2019، ص.ص97، 98.

[6]- سهيلة بضياف، آمنة حمراني، أمن المعلومات في الجزائر-الإجراءات والتحديات، المجلة الجزائرية للأمن والتنمية، جامعة الحاج لخضر باتنة، الجزائر، المجلد09، العدد16، السنة2020، ص181.

[7]- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة المصداقية، المدرسة العليا العسكرية للإعلام والاتصال، المجلد01، العدد02، الجزائر، السنة2019، ص.ص 109، 110.

[8]- يحي مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي، الجزائر، المجلد14، العدد02، السنة2017، ص237.

[9]- موسى بن تغري، الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد12، العدد22، السنة2022، ص.ص204، 205.

[10]- أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، جامعة الأزهر، القاهرة، المجلد35، الجزء الثالث، العدد03، السنة2020، ص418.

[11]- عبد المجيد مبلغي وآخرون، الإرهاب-تعريفه وآليات مكافحته، ترجمة أحمد موسوي، الديوان للطباعة والنشر والتوزيع، مركز الحضارة لتنمية الفكرة الإسلامي، الطبعة الأولى، بيروت، السنة2015، ص.ص53- 55.

[12]- صباح كزيز، أمال كزيز، الارهاب الالكتروني وانعكاساته على لأمن لاجتماعي-دراسة تحليلية، مجلة التراث، جامعة زيان عاشور الجلفة، الجزائر، المجلد08، العدد02 السنة2018، ص.ص313، 314.

[13]– خالد حسن أحمد لطفي، التقاضي الالكتروني كنظام قضائي معلوماتي–بين النظرية والتطبيق، دار الفكر الجامعي، الطبعة الأولى، الاسكندرية، السنة2020، ص44.

[14]– أحمد سلام عبد العاطي، الحوكمة الالكترونية، مؤسسة طيبة للنشر والتوزيع، الطبعة الأولى، القاهرة، السنة2021، ص.ص29، 30.

[15]– مراد قريبيز، أمن المعلومات الالكترونية بين متطلبات السيادة الرقمية وجهود المنظمات الدولية والاقليمية، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، الجزائر، المجلد06، العدد01، السنة2021، ص1598.

[16]– سعاد قصعة، خديجة قصعة، تحديات الأمن المعلوماتي في مواجهة الجريمة الالكترونية في ظل الاعلام الجديد، مجلة المعيار، كلية أصول الدين جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، الجزائر، المجلد24، العدد50، السنة2020، ص380.

[17]– قانون رقم15–03، يتعلق بعصرنة العدالة، المرجع السابق.

[18]– أميرة عبد العظيم محمد عبد الجواد، المرجع السابق، ص.ص421، 462.

[19]– عمار قردود، حرب سيبرانية مستعرة لاختراق المواقع بين القراصنة الجزائريين والمغاربة، مقال منشور بتاريخ 14مارس سنة2022، تاريخ الاطلاع يوم23جانفي2023، على الساعة 18:00: https://africanews.dz/ .

[20]– خالد حسن أحمد لطفي، المرجع السابق، ص62.

[21]– أميرة عبد العظيم محمد عبد الجواد، المرجع السابق، ص415.

[22]– عثمان لحياني، الجزائر تفتح تحقيقا في اختراق وزارة العدل على تويتر، تاريخ النشر 12مارس سنة2022، تاريخ الإطلاع24جانفي سنة2023، على الساعة 11:00:
https://www.alaraby.co.uk/entertainment_media/ .

[23]– خالد حسن أحمد لطفي، المرجع السابق، ص15، 16.

[24]– الأمر رقم20–04، مؤرخ في 11محرم عام1442، الموافق لـ 30 غشت سنة2020، يتضمن تعديل قانون الاجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد51، مؤرخة في 21 غشت 2020.

[25]– إدريس عطية، المرجع السابق، ص111و ص115.

[26]– بلقاسم بن صابر، محمد حيدرة، المرجع السابق، ص.ص188، 190.

[27] –قانون رقم15–03، المرجع السابق.