منظم من طرف المركز المغاربي شرق أدنى _بريطانيا_، والمركز الاستشاري الإفريقي للتحكيم والوساطة _الجزائر_، وبالتعاون مع جامعة الزيتونة _ليبيا_

_17_18_19 نوفمبر 2022_

"دور الأمن السيبراني في التصدي لجريمة القرصنة الرقمية لمراكز التحكيم الإلكتروني"

The Role of Cybersecurity In Addressing the Digitale Hacking of E_ Arbitraion Centers

بلقيس قرازة

belkisbilla@gmail.com

طالبة دكتوراه ل.م.د

جامعة الأمير عبد القادر للعلوم الإسلامية _قسنطينة_

سعاد قصعة

habibkassaa@gmail.com

أستاذة محاضرة _أ_

جامعة الأمير عبد القادر للعلوم الإسلامية _قسنطينة_

الملخص:

يعتبر التحكيم الإلكتروني نظام قضائي حديث تم اعتماده لفض نزاعات المعاملات الإلكترونية، لما له من خصائص جعلته وِجهة للمتخاصمين بدل النظام القضائي العادي، ومن بين ميزاته السرية، غير أن البيئة الإلكترونية لا تخلو من اختراقات وهجومات سيبرانية مما يعني احتمال تعرض مراكز التحكيم عبر الأنترنيت للقرصنة، وهذا راجع لعدة أسباب متعلقة إما بالبنية المعلوماتية لهذه المراكز، أو بالمقرصن مفتعل الجريمة، أو بالضحية (أطراف النزاع)، لهذا تم وضع العديد من الحلول التقنية والتشريعية لحماية خصوصية البيانات أثناء المحاكمة، وفي الأخير خلصت الدراسة إلى ضرورة الاعتماد على أنظمة الذكاء الصناعي لتدعيم الأمن السيبراني وتطويره للحرص على سلامة وخصوصية التحكيم الالكتروني، وهذا

حتى لا تفقد المعاملات الإلكترونية مصداقيتها، وأيضا لابد من تظافر الجهود الدولية من أجل وضع سياسات تنظيمية وتقنية تتناول أمن وخصوصية البيانات المدرجة من قبل أطراف النزاع.

الكلمات المفتاحية: الأمن السيبراني _ التحكيم الإلكتروني _ القرصنة الرقمية.

Summary:

Electronic arbitration is a modern judical system adopted to resolve electronic transaction disputes because it has the advantage of making it a destination for litigants rather than the ordinary judicial systeme. Among thess confidential features; however the electronic environment is not without cyberattacks and arbitration centres may be exposed to piracy due to several reasons related to either the centres' information structure or the pirate this is why many technical and legislative solution have been developed to protect data privscy during the trial. Finally the stydy concluded that it is necessary to rely on artificial intelligence systems to strengthen and devlop cybersecurity to ensure the integrity and privacy of e_arbitration so that electronic transactions do not lose credibility. And also that there is a need for concerted international efforts to devlope regulatory and technical policies addressing the security and privacy of the data listed by the parties to the cinflict.

Keywords: cyber security – electronic arbitration – digital piracy.

مقدمة:

في ظل التطور التكنومعلوماتي السريع الذي نتج عنه ظهور العقود الإلكترونية عموما والعقود التجارية خصوصا على الساحة الدولية، وما ترتب عنها من ارتفاع في وتيرة النزاعات الناجمة عنها، أصبح من الضروري استحداث طرق حديثة لفضّ هذه النزاعات كون أن القضاء العادي لم يعد فعّالا بدرجة كافية خاصة مع طول إجراءات التقاضي التي تتنافى وسرعة المعاملات الإلكترونية، لهذا برزت الحاجة إلى ضرورة الاحتكام لنظام خاص يساير طبيعتها، على إثر هذا تم استحداث مراكز تحكيم رقمية تُعنى بفض النزاع القائم بين أطراف العقد باستخدام تقنيات إلكترونية يتم اللجوء إليها بناءً على إرادة المتعاقدين.

إلا أن البيئة السيبرانية التي يتم فيها هذا النوع من التحكيم تعتبر بيئة خصبة للهجمات الماسة بأمن المعلومات، وعلى رأسها القرصنة الرقمية، التي تستهدف أنظمة مراكز التحكيم بهدف كشف ملفات القضايا، مما يستوجب تحقيق الحماية الفعالة والمستجدة من طرف مسؤولي الأمن السيبراني، على ضوء ما سبق تبرز **إشكالية** الورقة البحثية في ما يلي: **كيف تؤثر البيئة السيبرانية على سرية التحكيم الإلكتروني؟**

يندرج تحت هذا التساؤل الرئيس جملة من **الأسئلة الفرعية:**

1) ما العلاقة التي تربط مراكز التحكيم الإلكتروني بكل من الأمن السيبراني والقرصنة الرقمية؟

2) فيم تتمثل الأسباب الرئيسية المساعدة على نجاح عملية قرصنة مراكز التحكيم الإلكتروني؟

3) هل تقنيات الأمن السيبراني التقليدية كافية لتحقيق حماية تامة لعملية التحكيم من الاختراق الرقمي؟

أهمية الدراسة:

في ظل الاستغلال المرتفع لتكنولوجيات المعلومات والاتصال في المعاملات بين الأفراد وبين المؤسسات والدول، وضرورة اعتماد مراكز التحكيم الإلكتروني لفض ما ترتب عنها من نزاعات، تظهر إشكالية اختراق السرية _الواجب تحققها في عمليات التحكيم_ كنتاج لهذه

الرقمنة الحديثة في القطاع القضائي، كونها تمس بحق الأطراف في خصوصية وسرية بياناتهم حفاظا على مراكزهم في أوساط المعاملات الإلكترونية.

أسباب الدراسة:

بغض النظر عن الأسباب الشخصية لاختيار الموضوع محل الدراسة (الرغبة في البحث في الأمن السيبراني وما يتعلق به من ملحقات)، فإن من أهم الأسباب الموضوعية هي الانتهاكات التي تُطال قطاع العدالة بعد رقمنته، فالأصل أن أتمتة أي قطاع إنما تكون بغية توفير ميزات أكبر كضمان سرية التحكيم الإلكتروني، إلا أن ما يحدث هو العكس نظرا للاختراقات السيبرانية التي تتم على مستوى مراكز التحكيم ، هذا كان دافعا لتسليط الضوء لبحث كل من أسباب هذه القرصنة والحلول الممنهجة للحد منها.

أهداف الدراسة:

تهدف الدراسة إلى بحث كيفية تأثر مراكز التحكيم الإلكتروني بالبيئة السيبرانية التي يتم على مستواها، ومعرفة العوامل التي تسهل من الاختراقات الرقمية لها.

منهج الدراسة:

يعتبر المنهج الوصفي هو الغالب في الدراسة، كونها تعرض وصفا شاملا لعملية القرصنة التي تمس مراكز التحكيم الإلكتروني، من خلال إيراد الأسباب والحلول المعتمدة.

خطة الدراسة:

المبحث الأول: تحديد المفاهيم الأساسية

المبحث الثاني: أسباب واستراتيجيات قرصنة مراكز التحكيم الإلكتروني

المبحث الثالث: وسائل تأمين مراكز التحكيم الإلكتروني

المبحث الأول: تحديد المفاهيم الأساسية

بما أن عملية التحكيم تتم في بيئة سيبرانية، فإن هذا يجعلها عرضة للقرصنة الرقمية في أي وقت وفي أي مرحلة من مراحلها، مما يستوجب تعزيز الأمن السيبراني لحماية البيئة المعلوماتية الخاصة بها، ونظرا لخطورة هذه الجريمة على هذا النوع من المراكز كان من المناسب منهجيا أن يتم التعرض لأهم متغيرات العنوان (الأمن السيبراني، جريمة القرصنة الرقمية، مراكز التحكيم الإلكتروني) بشيء من الشرح والتوضيح، وبيان هذا في ما يلي:

المطلب الأول: تعريف الأمن السيبراني

عَرّف الاتحاد الدولي للاتصالات[1] الأمن السيبراني بأنه "من المهمات والوسائل والسياسات والإجراءات الأمنية والمبادئ التوجيهية والمقاربات لإدارة المخاطر، والتدريبات والممارسات الفضلى والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"[2] وبعبارة أخرى يمكن اعتباره "المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات ومنع التعديات أو للحد من آثارها في أقسى وأسوأ الأحوال".[3]

إذا فالأمن السيبراني هو مجموع الوسائل الأمنية المتخذة من طرف الجهات المختصة بهدف توفير حماية أكبر للبيئة الإلكترونية وهذا لصد الهجمات السيبرانية التي تطال عليها بهدف التخريب والتجسس وقرصنة البيانات الخاصة إما بالأفراد أو المؤسسات والشركات، أو الحكومات.

---

[1] هو وكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات (ICT)، www.itu.int

[2] أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي الإنساني"، مجلة الشريعة والقانون، العدد 35، ج 3،ص 388.

[3] منى الأشقر جبور، السيبرانية هاجس العصر، المركز الوطني للبحوث القانونية والقضائية. جامعة الدول العربية، د ط، د ت، ص 26.

المطلب الثاني: تعريف القرصنة الرقمية

تعد القرصنة أحد أنواع الهجمات السيبرانية[1] التي تهدد الأمن المعلوماتي، وتهدد حق الفرد في الحفاظ على بياناته الخاصة وعدم كشفها للغير، لذا عُرِّفت على أنها "استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التحايل على أنظمة المعالجة الآلية للبيانات، واكتشاف البيانات الحساسة أو تغييرها والتأثير على سلامتها أو حتى إتلافها"[2]، ويباشرها القراصنة وهم "أشخاص لهم القدرة على التعامل مع أنظمة الحاسبات أو الشبكات" وهؤلاء المخترقين إما أن يكونوا هاكرز أو كراكز، فأما الهاكرز يمكن اعتبارهم متطفلين على أمن المعلومات والشبكات وهذا بكسرهم لحواجز الأمن بهدف الفضول أو اثبات الذات، أما الكراكز هدفهم من القرصنة هو التخريب والحاق الضرر والعبث بالمعلومات المخزنة.[3]

وبالربط بين مصطلحي الأمن السيبراني والقرصنة الرقمية يمكن القول أن الأمن السيبراني هو الخط الدفاعي ضد هجمات القرصنة الرقمية التي طغت في الفضاء السيبراني مهددة بذلك أمن المعلومات والبيانات، الذي تسعى الدول والمؤسسات والشركات والأفراد للحفاظ عليه، ونظرا لخبرة القراصنة ومعرفتهم التقنية والتكنولوجية وكشفهم لثغرات الأنظمة بات من الضروري تدخل بالأمن السيبراني لتعزيز الحماية في الأوساط الرقمية.

---

[1] "الهجمات السيبرانية هي فعل يقوض من قدارت وظائف شبكة الكومبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تمكّن المهاجم من التلاعب بالنظام ومن بين الهجمات السيبرانية ما يلي: سرقة كلمات المرور للمستخدمين للتسلل في النظام، والنفاذ إلى ملف تخزين كلمة المرور والسطو على كلمات المرور السرية والتجسس على المستخدمين القرصنة الالكترونية في الفضاء السيبراني "، نورة شلوش، "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الانسانية، العدد 2، المجلد 8، 2018م، ص 191.

[2] ليتيم فتيحة، ليتيم نادية، "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة"، مجلة المفكر، العدد 12، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، ص 242.

[3] روان بنت عطية الله الصحفي، "الجرائم السيبرانية"، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، ماي 2020م، ص 14.

المطلب الثالث: تعريف مراكز التحكيم الإلكتروني

يُعَرَّف التحكيم الإلكتروني على أنه "نظام قضائي خاص يختار الأطراف فيه قضاتهم، ويعهدون إليهم بمقتضى اتفاق مكتوب بمهمة تسوية المنازعات التي قد تنشأ أو نشأت بالفعل بينهم بخصوص علاقاتهم التعاقدية أو غير التعاقدية"[1] وهذا بطريقة الكترونية منذ عرض النزاع إلى غاية إصدار القرار وتبليغه،[2] وهذه العملية تتم على مستوى مراكز خاصة تسمى بمراكز التحكيم، لهذا يمكن تعريفها كالآتي: مراكز تقوم بحل النزاعات الناشئة عن المعاملات الالكترونية (على سبيل المثال: المنازعات الناجمة عن الاخلال ببنود العقد الإلكترونية، ونزاعات أسماء النطاق[3])، معتمدة في ذلك على قواعد معينة يرسمها المركز لتحديد مجرى العملية التحكيمية منذ اتفاق التحكيم حتى صدور قرار المحكمين وتسمى أيضا بمراكز التحكيم عبر الانترنيت.[4]

ومن أمثلة هذه المراكز جمعية المحكمين الأمريكية (AAA) التي طورت نظام القضاء الافتراضي، ومحكمة التحكيم الإلكترونية التابعة للمنظمة العالمية لحماية حقوق الملكية الفكرية ويبو (WIPO)، وكذلك قامت بعض المؤسسات غير الحكومية مثل كلية الحقوق بجامعة مونتريال بكندا بإنشاء نظام محكمة تحكيم الكترونية،[5] أما على الصعيد العربي فقد تم تأسيس

---

[1] هواري صباح، "التحكيم الإلكتروني ومدى فعاليته في حل منازعات عقود التجارة الالكترونية"، المجلة العربية في العلوم الانسانية والاجتماعية، مجلد 14، عدد 3، جويلية 2022م، ص 75، ينظر أيضا: سعد خليفة سعد الهيفي، "القانون الواجب التطبيق على التحكيم الإلكتروني"، رسالة ماجيستر، قسم القانون الخاص، كلية الحقوق، جامعة الشرق الأوسط، أيلول 2013م، ص 6، سهام صديق، "نظام التحكيم الإلكتروني لتسوية المنازعات الالكترونية"، مجلة البصائر للدراسات القانونية والاقتصادية، العدد 4، المجلد 2، 2022م، ص 4.

[2] سهام صديق، مرجع سابق، ص 4.

[3] خالد ممدوح ابراهيم، ابرام العقد الإلكتروني، الدار الجامعية، الاسكندرية، ط1، 2007م، ص 405.

[4] طيب كامش، "الإجراء التحكيمي ذو المواصفات الالكترونية في منازعات التجارة الإلكترونية"، مجلة الدراسات القانونية المقارنة، المجلد 7، العدد2، 2021م، ص 1511.

[5] خالد ممدوح ابراهيم، مرجع سابق، ص 406.

الاتحاد العربي للتحكيم الإلكتروني في 2007/9/1 وهو يعمل تحت اشراف جامعة الدول العربية[1]

ومن أهم المميزات التي يمنحها التحكيم الإلكتروني هي الحفاظ على سرية التحكيم فإجراءاته تتم عبر انشاء موقع الكتروني خاص بملف القضية تودع فيه الإعلانات والبيانات والأدلة وقرارات التحكيم ولا يسمح بولوجه إلا من طرف المعنيين بالأمر (هيئة التحكيم وأطراف النزاع أو وكلائهم) وهذا باستخدام أرقام سرية،[2] هذه الميزة تضمن لهم استمرار المعاملات التجارية واستقرارها بينهم وبين من يتعاملون معهم دون أن تكون هناك شائبة تشوب معاملاتهم وعلاقاتهم،[3] بمقابل ذلك لا يوفر التحكيم الإلكتروني السرية المطلوبة بصفة قاطعة، [4] فجلسات التحكيم تتم عبر الوسائط الالكترونية المتاحة في هذا المجال والتي تسمح بتبادل النصوص والصور والملفات عبر البريد الالكتروني، هذه البيئة الرقمية [5] تشكل تهديدا لسرية التحكيم[6] فتكون هناك امكانية اختراقها من قبل قراصنة شبكة الانترنت، مما يهدد سرية العملية التحكيمية برمتها، فالحفاظ على سرية النزاع و الفصل فيه يعد من الدوافع الأساسية للجوء إلى التحكيم دون القضاء[7] ما يسبب الذعر في الوسط التجاري خاصة ممن يحرصون على المحافظة على أسرارهم التجارية وعدم إفشاءها خوفا على عملهم ومكونات منتجهم، وهذا من طرف القراصنة والمخربين.[8]

---

[1] مصطفى ناطق صالح مطلوب، "التحكيم التجاري الإلكتروني"، مجلة الرافدين للحقوق، العدد 39، المجلد 11، 2009م، ص 152.

[2] زعزوعة فاطمة، زعزوعة نجاة، "التحكيم الالكتروني كآلية لتسوية منازعات التجارة الالكترونية في ظل التشريع الجزائري"، مجلة القانون العام الجزائري والمقارن، المجلد 8، العدد 1، ماي 2022م، ص 145.

[3] محمد مأمون سليمان، التحكيم الإلكتروني: التجارة الالكترونية (اتفاق التحكيم، عملية التحكيم، حكم التحكيم)، دار الجامعة الجديدة، الاسكندرية د ط، 2011م، ص 593.

[4] سهام صديق، مرجع سابق، ص 6.

[5] زعزوعة فاطمة، زعزوعة نجاة، مرجع سابق، ص 146.

[6] سهام صديق، مرجع سابق، ص 6.

[7] صديقي سامية، بولواطة السعيد، "التحكيم الالكتروني كوسيلة لتسوية منازعات التجارة الالكترونية"، مجلة البيبان للدراسات القانونية والسياسية، العدد 1، المجلد 3، جوان 2018م، ص 150.

[8] ياسر احمد العلجوني، التحكيم الإلكتروني وسيلة لفض المنازعات، مجلة المنارة، http://revuealmanara.com 21:39، 2022/11/0/7.

المبحث الثاني: أسباب واستراتيجيات قرصنة مراكز التحكيم الإلكتروني

إن الأصل في مراكز التحكيم أن تتم في بيئة سرية مؤَمّنة عن أي هجوم سيبراني من شأنه المساس بحق أطراف النزاع في الحفاظ على خصوصياتهم وبياناتهم ونتاج محاكمتهم تلك بعيدا عن الأعين، إلا أن هذا الأصل ليس ثابت فما دامت هذه العملية تتم في بيئة رقمية لا بد وأن تتعرض لبعض الهجمات السيبرانية، وعلى رأسها القرصنة الرقمية، لهذا سيتم التطرق في هذا المحور للأسباب التي من شأنها أن تجعل هذه المراكز معرضة للاختراق من طرف القراصنة، وإلى استراتيجياتهم في تنفيذ هذا الاختراق.

المطلب الأول: أسباب تعرض مراكز التحكيم الإلكتروني للقرصنة

إن تعرض مراكز التحكيم الإلكتروني للقرصنة راجع لعدة أسباب متعلقة إما بالبيئة الافتراضية لهذه المراكز، أو بالمخترق، أو بالضحية، وسيتم التطرق لهذه الأقسام الثلاثة وما يندرج تحتها من أسباب فرعية تباعا.

أولا: أسباب متعلقة بطبيعة البيئة السيبرانية

إن البيئة الرقمية التي يتم على مستواها التحكيم والطرق المعتمدة لتأمينها من شأنها تسهيل عملية القرصنة وبيان هذا كالآتي:

1) البيئة الرقمية لعملية التحكيم الإلكتروني

يتم التحكيم بكل مراحله على مستوى افتراضي حيث يتم انشاء موقع الكتروني خاص بملف القضية، ويتم رفع المستندات والأدلة عليه من خلال مذكرات ترسل عبر وسائط إلكترونية (البريد الإلكتروني)، وفي حال رَغِبَ الأطراف في مناقشة بعض المسائل المتعلقة بموضوع التحكيم فإنّ اللقاء يكون عن بعد وهذا باعتماد غرف المخاطبة والحوار على الانترنيت CHAT ROOM فيعقد بينهم ما يسمى بالمؤتمر الافتراضي.[1]

[1] خالد ممدوح ابراهيم، مرجع سابق، ص 404.

إذا فالحقيقة الرقمية _كما سبق بيانه_ لهذه المراكز تجعلها قبلة أكيدة للاختراقات السيبرانية في أي مرحلة من مراحل التحكيم، خاصة أن أطراف النزاع يحمِّلون بياناتهم الشخصية وملفاتهم على الموقع الخاص بقضيتهم، وفي خضم اشكالية عدم أمن المعلومات والبيانات الرقمية أصبح من الممكن استغلالها بطرق غير شرعية من قبل القراصنة.

2) ضعف الحماية الإلكترونية لمراكز التحكيم الإلكتروني

إن محاولة تأمين عملية التحكيم عبر إدراج كلمة السر التي تخول للمعنيين بالأمر فقط الولوج إلى موقع القضية هي أسلوب أمني غير كفء وغير فعال كما يجب، فالاختراقات الأمنية أغلبها تتم عبر اكتشاف كلمة السر، كونها غالبا ما تكون ضعيفة، وشائعة، وسهلة، فقد تتصل بمحيط المعني بالأمر، أو بحياته الخاصة، هذه كلها تُضعف من قوتها أمام فعالية البرمجيات الملتقطة لكلمات السر خلال تجوالها في الشبكة أو أحد عناصرها، فيقوم المخترق بمراقبتها وتتبعها وجمعها، ثم اخفاء أنشطة الالتقاط بعد انتهاء المهمة. [1]

إذا فالحرص على أمن المعلومات المدرجة في مراكز التحكيم الإلكتروني لا يصح أن نعتمد فيه على أسلوب كلمة السر فالتطور الرقمي والمعلوماتي الذي خلق لنا بيئة سيبرانية متطورة من جهة، وتقنيات حديثة للهجوم عليها في نفس الوقت من جهة أخرى، لا يسمح لنا أن نتعامل مع هذه الاختراقات بنفس تقنيات الحماية التي اعتمدت في وقت سابق، وإن ثبتت فعاليتها آنذاك فإنها الآن تعتبر خطا دفاعيا ضعيفا وإن تم الاعتماد على كلمات سر صعبة طويلة وغير متوقعة.

3) سهولة شراء برامج القرصنة

إن الأمر الخطير المساعد على القرصنة هو سهولة اقتناء البرمجيات والأدوات الخبيثة الغير متاحة للعامة بأسعار زهيدة، ويمكن اقتنائها في أي وقت، فعلى سبيل المثال نجد أن سعر برنامج خبيث أقل من 1000 دولار، وبرامج الفدية قيمتها 200 دولار، وخدمات الرسائل الإلكترونية غير المرغوبة (SPAM) ب400 دولار تقريبا،[2] هذا الأمر يضع مراكز التحكيم

---

[1] منى تركي الموسوي، جان سيريل فضل الله، "الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها"، مركز بحوث السوق وحماية المستهلك، جامعة بغداد، مجلة كلية بغداد للعلوم الاقتصادية، 2013م، ص 27.

[2] أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص 384.

الإلكتروني في خطر خاصة وأنّ هناك العديد من المنافسين الذين يرغبون بالاطلاع على ملف القضية، فيلجؤون إلى اقتناء برامج تعينهم على القرصنة بأنفسهم إن كان لهم خبرة تقنية، أو إحالة الأمر إلى المخترقين الذين تعتبر مسألة الحصول السهولة بالنسبة لهم خاصة مع توافر الأنترنيت المظلم (DEEP WEP).

4) صعوبة اكتشاف وإثبات جريمة القرصنة

إن هدف المقرصن هو القيام بجريمته دون لفت الأنظار إليه لهذا من مصلحته الإبقاء على النظام دون أي خلل حتى يحقق أكبر المكاسب التي تضاف إليه حال عدم كشفه،[1] ومن طبيعة هذه الجريمة أنها غير مادية أي تتصف بالخفاء مما يعني أن المجرم بمجرد انتهائه (لحظات فقط لارتكاب الجريمة) يحذف كل الأدلة الأمر الذي يصعب من الكشف عن الجريمة من جهة، ومعرفة الجاني من جهة أخرى،[2] وعليه فمخترق مراكز التحكيم الإلكتروني غالبا ما يكون مرنا خبيرا، حتى لا يتفطن أطراف القضية من دخوله للموقع أصلا فضلا عن سرقته الملفات أو الاطلاع عليها، مما يسبب فيما بعد اشكالية كيف تم تسريب تلك البيانات وكيف يتم الوصول للمجرم بالاعتماد على تقنيات الأمن السيبراني.

ثانيا: أسباب مرتبطة بالمخترق (المجرم)

لا يكفي توفر بيئة سيبرانية حتى تتم عملية القرصنة بل لابد من توافر جملة من الأسباب المتعلقة بمفتعل الجريمة (الهاكر /الكراكر) تزيد من حظوظ نجاحه.

1) الخبرة والمعرفة التقنية

إن ولوج عالم القرصنة يتطلب من الشخص أن يكون ملمّا بمعلومات تقنية وخبرة إلكترونية قيمة، تساعده فيما بعد على الاختراق بسهولة لهذا لا نجد مرتكبي هذا الجرم مستخدمين عاديين بل أشخاص لديهم القدرة الفائقة في مجال الحاسب الآلي، [3] ونظرا للحقيقة التي مفادها

---

[1] المرجع نفسه، ص 395.

[2] أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص 402.

[3] المرجع نفسه، ص 409.

أن الفضاء السيبراني في تغير مستمر وأن الهجومات في جدة دائمة، عكس أساليب الدفاع الأمني التي تستغرق فترة لحل الهجوم بل لا يحله إلا بعد وقوعه، نجد كنتيجة لذلك أن المخترق يحتاج إلى مرة ناجحة واحدة لتنفيذ هجومه بينما يحتاج المدافع إلى أكثر من مرة نجاح لاكتشاف الهجوم والتصدي له في كل مرة خاصة مع وجود الثغرات واحتمال اكتشافها من طرف المهاجم في كل مرة. [1]

إن هذه القدرات التقنية المتوفرة لدى شخص المخترق من شأنها أن تسهل عليه عملية الهجوم على مراكز التحكيم فكل ما عليه هو توظيف خبراته في اكتشاف الثغرات التقنية الموجودة على مستواها، واستخدام الأساليب الناجعة لاختراقها للوصول إلى البيانات التي يبحث عنها.

2) دوافع شخصية وتجارية

من أهم أسباب القرصنة الدوافع الشخصية إذ غالبا ما تدفع مشاكل العمل إلى رغبة في الانتقام،[2] وكذلك الدوافع التجارية التي يكون التجسس فيها بهدف الحصول على معلومات اقتصادية وتجارية وتقوم به بعض الشركات والمؤسسات التجارية للحصول على معلومات قيمة من الشركات المنافسة.[3]

وعليه في حال ما كان لأحد أطراف النزاع مكانة تجارية في سوق العمل وله اعتبار على الساحة الاقتصادية كلمت زاد عدد منافسيه غير النزهاء الذين يلجئون للقرصنة من أجل الاطلاع على ملف القضية والاطلاع على بياناتهم وما يمكن أن يخدمهم تجاريا، وكذلك الاطلاع على نتائج القضية وقد تكون دوافعهم أيضا مالية وهذا بابتزاز أحد طرفي النزاع على دفع فدية أو كشف قضيته للعلن مما يؤثر على سمعته التجارية.

---

[1] فاتح حارك، رياض حمدوش، "الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني"، المجلة الجزائرية للأمن الإنساني، المجلد 7، العدد 1، جانفي 2022م، ص 139/138.

[2] بشرى حسين الحمداني، القرصنة الإلكترونية أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، الأردن، ط1، 2014م، ص 70.

[3] أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص419.

ثالثا: أسباب مرتبطة بالضحية.

لا يتوقف نجاح عملية القرصنة الرقمية على توفر البيئة الإلكترونية المناسبة، وعلى الخبرة والدوافع التي تدفع المجرم لارتكابها فقط، بل الأمر راجع أيضا للضحية، ففي عصر تكنولوجيا المعلومات وهيمنتها على أغلب القطاعات من جهة، وغياب الوعي بالأمن السيبراني لتفادي الهجمات السيبرانية لأطراف النزاع من جهة أخرى هو عامل مساعد لارتكاب الجريمة، وكأبسط مثال عمليات القرصنة معلوم أنها تتم بطرق بسيطة وأخرى جد معقدة فمن الطرق البسيطة وصول رسائل بها فيروسات أو دخول مواقع غير مأمنه وغير معروفة، فهنا قد لا يولي المستخدم أدنى اهتمام بما وصله وصادق عليه، والحقيقة التي يجهلها أن المخترق قد يكون اعتمد هذه الطريقة كوسيلة للولوج فيما بعد لموقع النزاع.

المطلب الثاني: استراتيجيات قرصنة مراكز التحكيم الإلكتروني

إن الجريمة الإلكترونية لا يمكن أن تكلل بالنجاح دون اعتماد استراتيجية ناجحة مبنية على أساليب دقيقة معينة على تحقيق الهدف، لهذا يمكن القول أن نجاح قرصنة مراكز التحكيم (بعد توافر الأسباب السابقة) مرتبط بنجاعة الأساليب المعتمدة.

أولا: تحديد مداخل النظام الضعيفة

يحدد المخترق مداخل النظام على أساس مواطن الضعف التي يفترض حمايتها من طرف مسؤول نظام الأمن الذي يتفوق عليه المجرم في غالب الأحيان في كَمِّ المعلومات المتقدمة مما يجعل اختراق الأنظمة اكثر سهولة من الدفاع عنها.[1]

ثانيا: خداع بروتوكول الأنترنيت

ويتم ذلك بالتخفي واستغلال بروتوكول الانترنيت بأن ينتحل المخترق هوية مستخدم مخول له بالدخول ويقوم بتزوير العنوان المرسل مع حزمة البيانات ليظهر للنظام أنه عنوان صحيح وبذلك يسمح النظام لحزمة المعلومات بالمرور باعتبارها حزمة مشروعة.[2]

---

[1] منى الأشقر جبور، مرجع سابق، ص 52.

[2] ليتيم فتيحة، ليتيم نادية، مرجع سابق، ص 246.

ثالثا: الاعتماد على برامج القرصنة

1) الفيروسات VIRUSES

هي إحدى أنواع البرامج الآلية التي تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، مما يؤدي إلى إيقاف عمل الجهاز، ويتكون الفيروس من أربعة أجزاء أساسية:

- آلية التكرار: وهو الجزء الذي يسمح للفيروس بالانتشار.
- آلية التخفي: يجعل الفيروس مخفيا.
- آلية التنشيط: وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يتم اكتشافه.
- آلية التنفيذ: وهو الجزء الذي ينفذ الفيروس بمجرد تنشيطه.[1]

2) أحصنة طروادة TROJAN HORSES

تهدف إلى إضعاف قوة الدفاع لدى الضحية لتسهيل الاختراق، مثلا يقوم بإرسال بيانات عن الثغرات الموجودة في نظام ما، أو ارسال كلمة السر الخاصة بمخزون معلومات الطرف المستهدف.[2]

3) الديدان WORMS

الديدان هي برامج صغيرة لا تعتمد على غيرها تتميز بسرعة الانتشار والتناسخ مما يجعل التخلص منها امرا صعبا.[3]

إذا باجتماع الأسباب المعينة على قرصنة مراكز التحكيم تبقى آخر خطوة وهي اعتماد تقنيات واستراتيجيات فعّالة لاختراقها، وهذا بمحاولة النفاذ عبر المداخل الضعيفة في النظام، إذ ثبت من قبل أنه لا يوجد أمن سيبراني كامل إنما تقاس قوة المواقع بقوة أضعف نقطة في النظام، وعليه يحدد المخترق أضعف المواطن والدخول عبرها، وأيضا خداع بروتوكل النظام

---

[1] المرجع نفسه، ص 245.

[2] بشرى حسين الحمداني، مرجع سابق، ص 108.

[3] المرجع نفسه، ص107.

بانتحال صفة أحد الأطراف المخول لهم بدخول ملف القضية، أو الاعتماد على فيروسات مقرصنة تعين على الاختراق.

المبحث الثالث: وسائل تأمين مراكز التحكيم الإلكتروني

من أساسيات التحكيم أن يكون سريا حفاظا على أسرار الأطراف التجارية والتقنية والصناعية، وهذا ما نصت عليه المادة 20/7 من قواعد غرفة التجارة الدولية في باريس، والمادة 4/19 من قواعد محكمة لندن للتحكيم الدولي، وغيرها من المواد،[1] لهذا ولضمان حماية مراكز التحكيم من القرصنة الرقمية، تم اعتماد حلول تقنية وأخرى تشريعية.

المطلب الأول: الوسائل التقنية والفنية

لضمان حماية أوفر لسرية مراكز التحكيم لا بد من تعزيز وسائل الدفاع التي اعتاد الأمن السيبراني عليها، وفيما يلي ذكر لبعضها على سبيل التمثيل لا الحصر.

أولا: جدران النار

يمكن القول أنها تعمل كحراس للأنترنيت فتقوم بفحص رزم البيانات الداخلة والخارجة، اعتمادا على مجموعة القواعد التي يضعها المشرف على الشبكة للسماح للرزم بالمرور أو عدم السماح. [2]

ثانيا: محاكاة أساليب الهجوم الإلكتروني

أو ما يسمى بالمناورات الأمنية الالكترونية، وهذا للتأكد من قوة الأنظمة وهذا بالقيام بهجمات مضادة لاختبارها. [3]

---

[1] مصطفى ناطق صالح مطلوب، مرجع سابق، ص 166.

[2] ليتيم فتيحة، ليتيم نادية، مرجع سابق، ص 249.

[3] المرجع نفسه، ص 249.

ثالثا: تشفير المعلومات المنقولة والمحفوظة

وهذا مهم جدا في حالة التحكيم الإلكتروني، إذ من الواجب اعتماد تقنيات تشفير عالية تظهر المعلومات الخاصة والبيانات بصورة ضبابية غير مفهومة لكل من يحاول التنصت عليها، وتعتمد طريقة التشفير الحديثة على نظرية: تمتلك كل جهة مفتاحين لتشفير وفك تشفير البيانات، المفتاح الأول وهو المفتاح الخاص، والمفتاح الثاني هو العام الأول يكون بحوزة المخول له بالدخول فقط، أما العام فيتم نشره على سطح الأنترنيت ليتم استخدامه من طرف الجهة المرسلة للبيانات حتى تشفرها. [1]

وكذلك تعزيز أساليب الدخول للنظام كاستخدام البطاقات الذكية المستعملة للتعريف ووسائل التعريف البيولوجية التي تعتمد على تحديد الهوية عن طريق التحقق الحيوي وهذا بتسجيل معلومات عن بصمة اليد، العين وغيرها من الخصائص الفيزيولوجية، هذا اضافة الى اعتماد كلمة سر موثوقة تكون طويلة ومعقدة.[2]

رابعا: استخدام برامج خاصة لمكافحة الفيروسات

وهذا من خلال فحصها للبريد الإلكتروني والمحافظة على قواعد البيانات كما تراقب البرامج القادمة والخارجة من الشبكة،[3] خاصة وأن مبدأ المحاكمة يعتمد على ما يتم تبادله من مستندات وملفات للحكم في القضية.

خامسا: رفع الوعي الأمني

والتعريف بالمخاطر والقضايا المتعلقة بالأمن السيبراني من خلال القنوات الفضائية المتعددة ووسائل التواصل الاجتماعي .[4]

---

[1] المرجع نفسه، ص 250.

[2] خوسيه فارغيز، "الذكاء الاصطناعي في مجال الأمن السيبراني: من الضجيج المُثار حوله إلى الواقع"، www.eyeofriyadh.com/ 5/11/2022 10:22.

[3] المرجع نفسه، ص 250.

[4] آمنة على البشير محمد، "الأمن السيبراني في ضوء مقاصد الشريعة"، مجلة كليات الدراسات الإسلامية والعربية للبنات بالإسكندرية، العدد37، مجلد 1، ص 491.

سابعا: الاعتماد على تقنيات الذكاء الصناعي

إن أساليب الحماية ومناهجها التقليدية التي اعتاد الأمن السيبراني تبنيها لم تعد صالحة للتطبيق على التنظيم الرقمي الجديد، ولم يعد في وسع خبراء الأمن المعلوماتي معالجة كل الهجمات السيبرانية مما يجعل اللجوء لتقنيات الذكاء الصناعي الحل الأمثل، نظرا لسرعتها، ودقتها في التعامل المستمر مع التهديدات التي تواجهها الأنظمة،[1] ومن بين أهم الوظائف التي يساهم بها الذكاء الاصطناعي في تعزيز الأمن السيبراني، والتي يمكن الاعتماد عليها أيضا لمجابهة جريمة قرصنة مراكز التحكيم الإلكتروني ما يلي:

1) توقع الخطر وكشف التهديدات الجديدة وتنبيه التعقب

إن القدرات الفائقة للذكاء الاصطناعي تمكنه من الكشف عن التهديديات التي تشكل خطرا على الأنظمة، وهذا بسبب قدرته على التعلم الآلي، ولا يقتصر الأمر على كشف التهديدات فقط بل حتى التنبأ بها قبل وقوعها، لهذا نجد العديد من المنظمات تعتمد عليه، لقدرته على التنبأ وتحديد مكان الاختراق وكيفيته، عبر تحديده لنقاط ضعف النظام، وتحسين الدفاع ضد أي هجوم محتمل[2] وهذا ما لا تسطيع تقنيات الحماية التقليدية فعله، كونها غير قادرة على مواكبة كل البرامج الضارة المستجدة كل مرة فتكون خاصية التنبأ مساعدة في تعزيز الأمن عبر التخطيط وتخصيص الموارد لتقوية نقاط ضعف النظام[3].

لهذا يفضل للمسؤولين في مراكز التحكيم الإلكتروني تعزيز أمن المعلومات بالاعتماد على الذكاء الصناعي وعدم الاقتصار على التقنيين المسؤولين عن تحقيق الحماية، للتمكن من كشف الاختراق من جهة والتنبأ به قبل حدوثه من جهة أخرى، درءًا لمفسدة تسرب البيانات الخاصة بالقضية وكشفها أو تخريب الأدلة المدرجة في الموقع.

---

[1] المرجع نفسه.

[2] ألبانا إيسيني، الذكاء الاصطناعي والأمن السيبراني دراسة فيما يخبئه المستقبل، مركز البيان للدراسة والتخطيط، ترجمة باسم علي خريزان، 2022م، ص 5.

[3] فوائد استخدام الذكاء الاصطناعي للأمن السيبراني، 10:30، 11/05 2022، www.careerera.com

2) الاستجابة

تتميز آليات الذكاء الاصطناعي بالقدرة على الاستجابة السريعة للتهديدات والانتهاكات مهما كان النمط والأسلوب المعتمد من طرف المخترق، كما أن الذكاء الاصطناعي يساعد في خفض التكلفة التي تطلبها الحماية.[1]

إذا يمكن القول أن الوسائل التقنية المعتمدة لتعزيز الأمن السيبراني لحماية مراكز التحكيم الإلكتروني من الاختراق الرقمي قسمان: تقليدية، وحديثة، فأما التقليدية فقد ثبت عدم نجاعة بعضها، وأما الحديثة فالمقصود بها التقنيات المبنية على أنظمة الذكاء الصناعي وهي أكثر فعالية نظرا للخصائص التي تتميز بها دون الوسائل التقليدية.

المطلب الثاني: وسائل التأمين التشريعية

استدعت الهجومات السيبرانية المساس بالأمن المعلوماتي ضرورة وضع تشريعات دولية تعنى بتعزيز الأمن السيبراني، ومن بينها ما يلي: قرارات كل من الأمم المتحدة، الاتحاد الدولي للاتصالات، اتفاقية بوداباست لمقاومة جرائم السيبرانية والاتصالات.

أولا: الأمم المتحدة

حيث صدر عن الجمعية العامة للأمم المتحدة جملة من القرارات على غرار القرار 239/57، حيث نددت فيه بضرورة تظافر الجهود الدولية والإقليمية لتعزيز الأمن السيبراني للتصدي للهجمات المعادية له، والقرار رقم 199/58 الصدار في 30 يناير 2004 لإرساء الثقافة السيبرانية وحماية البنى التحتية، وكل من القرار 63/55 و121/56 المنظمان للإطار القانوني لمكافحة الاستعمال السيء لتكنولوجيا المعلومات، أما بالنسبة للقرارات الصادرة عن المجلس الاقتصادي والاجتماعي الذي افتتح دورته لعام 2010 بجلسة اعلامية عن تحديات الأمن السيبراني، حيث دعى فيه إلى ضرورة تكثيف التعاون بين الدول لتبادل المعلومات في هذا الخصوص، وطلب من الأعصاء أيضا تقديم موجزات سياستها المعتمدة في إطار الأمن

[1] ألبانا إيسيني، مرجع سابق، ص 5.

السيبراني والهجمات السيبرانية، وندد بضرورة استقدام موظفين خبرة لمكافحتها، وأيضا ضرورة ارساء ثقافة عالمية سيبرانية عن طريق تجديد المناهج التعليمية تفضي إلى ايجاد مواهب تهتم بتحديات وأمن السيبرانية

مؤتمر هافانا وهو مؤتمر الأمم المتحدة الثامن لمحاربة الجريمة ومعاملة المذنبين 1990حيث حث على محاربة سوء استعمال التكنولوجيا على المستوى الوطني والدولي، فأما الوطني حث على تجريم الأفعال الماسة بسلامة وأمن المعلومات، وفي نفس الوقت ضرورة تعزيز الأمن السيبراني، وعلى الصعيد الدولي حث على ضرورة رفع الجهود لضمان الأمن السيبراني، وهذا بانضمام الدول الى معاهدات تسمح بتسليم مجرمي أمن المعلومات.[1]

ثانيا: الاتحاد الدولي للاتصالات ITU:

حيث كانت له جهود فعالة في الحفاظ على الأمن السيبراني، ومن بين قراراته تلك المتخذة في القمة العالمية لمجتمع المعلومات 2006 بشأن بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، وخلص ببناء برنامج الأمن السيبراني 2007 ليكون إطارا للتعاون الدولي وهذا بتنسيق الجهود الدولية لتحقيق الأمن في المجال السيبراني.[2]

ثالثا: اتفاقية بوداباست لمقاومة جرائم السيبرانية والاتصالات 2001:

تتضمن الاتفاقية التعاون بين أعضاء الاتحاد ذوي المصلحة والصلة لبناء ثقافة للأمن السيبراني عن طريق رفع الوعي وتطوير مواد التدريب فيها، وهذا بالسماح لأي دولة بالانضمام للاتحاد للتعاون بين الدول لوضع إطار عالمي للتصدي للجرائم السيبرانية.[3]

وكذلك جامعة الدول العربية التي أصدرت القرار رقم 495 عام 2003، وهي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وهذا لتعزيز التعاون بين الدول لمكافحة الجرائم السيبرانية. [4]

هذا بالإضافة إلى التشريعات التي سنت لمعاقبة مخترقي الأنظمة الإلكترونية، مثلا قانون البيانات السويدي (1973) الذي عالج قضايا الاحتيال الإلكتروني، وجرائم الدخول غير المشروع للبيانات، وأمريكا شرعت قانونا خاصا بحماية أنظمة الحاسب الآلي (1985)،

---

[1] أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص 490/483.
[2] المرجع نفسه، ص 492_495.
[3] أميرة عبد العظيم محمد عبد الجواد، ص 496.
[4] المرجع نفسه، ص 499.

بريطانيا حيث استحدثت عام 1990 قانون يعالج اساءة استخدام البيانات والدخول الغير المصرح به للبرامج، وغيرها من الدول الغربية، ويوجد قانون وق فالقرصنة (SOPA) وهو قانون تم تشريعه من طرف الكونغرس الأمريكي وهذا عن طريق وقف أي موقع الكرتوني من شأنه انتهاك أو المساعدة على القرصنة.[1]

وعليه يسعى المجتمع الدولي إلى ضمان استغلال آمن لتقنيات التكنولوجيا عبر تشريعه لقوانين تجرم الاختراقات والدخول غير المصرح به للأنظمة، وعقد اتفاقيات تهدف إلى تبادل المعلومات والخبرات بين الدول وخاصة بنود امكانية تسليم مرتكبي الجرائم الإلكترونية.

خاتمة

بعد التطرق للمباحث السابقة من كشف لمفاهيم الدراسة، وتبيان لأسباب وأساليب قرصنة التحكيم الإلكتروني، وعرض لأهم الحلول التقنية والتشريعية للتقليل منها، تم التوصل إلى جملة من النتائج والتوصيات هي في مجملها كالآتي:

- ⇐ يعتبر الأمن السيبراني منهجا متكاملا من تشريعات وتقنيات وآليات تهدف لحماية البنية الرقمية للفضاء السيبراني لضمان حماية أوفر للمستخدمين من أفراد ودول.
- ⇐ تعتبر القرصنة الرقمية أحد مفرزات التطور التكنولوجي التي تهدف إلى تخريب وتدمير الأنظمة والتجسس عليها بطرق احترافية.
- ⇐ تعتبر مراكز التحكيم الإلكتروني نظاما قضائيا حديثا يتوجه إليه بناءً على رغبة الأطراف، حيث يتم على مستواها رفع الأدلة وتداول المستندات واجراء اللقاءات الافتراضية، كل هذا تحت طائلة ضمان السرية، غير أن هذه الميزة غير محققة دوما.

[1] بشرى حسين الحمداني، المرجع السابق، ص 240_246.

⇐ العلاقة بين مفاهيم البحث الأساسية علاقة طردية أي كلما لجأ الأطراف إلى وسائط الكترونية لفض نزاعاتهم كلما زادت احتمالية القرصنة التي تستوجب زيادة الجهد المبذول من قبل الأمن السيبراني لصد الهجوم.

⇐ تختلف الأسباب التي تسهل من تعرض مراكز التحكيم الإلكتروني للقرصنة ولكن يمكن القول أنها عموما إما أن تتعلق بالبيئة السيبرانية التي تنشأ فيها هذه المراكز، أو بالمقرصن ذاته، أو بالضحية خاصة من ناحية نقص الوعي السيبراني لديه، وتعتبر الأسباب التجارية والشخصية من أهم الدوافع لقرصنة مراكز التحكيم الإلكترورني، بسبب المنافسة المتصاعدة بين الشركات.

⇐ تعتبر الفيروسات أحد أساليب القرصنة ومن أمثلتها: أحصنة طروادة، الديدان.

⇐ التشريعات الدولية الهادفة لتحقيق الأمن السيبراني تتضمن قرارات لضمان حماية البنية الإلكترونية للأنظمة، والدعوة إلى تظافر الجهود الدولية، والانضمام إلى معاهدات الكشف والاعلان عن الجرائم الإلكترونية حتى يسهل تسليم المجرمين، وإلى رفع الوعي والثقافة السيبرانية وتغيير المناهج التعليمية بما يتناسب ومتطلبات العصر الرقمي.

التوصيات:

- ✓ عقد دورات تدريبية لأطراف النزاع (تجميع عدد من القضايا ودعوة الأطراف) حول كيفية سير التحكيم الإلكتروني وبيان عيب عدم السرية المطلقة حتى يأخذ المعنيون بالأمر احتياطاتهم وهذا برفع مستوى ثقافتهم في الأمن السيبراني.
- ✓ إثراء المنظومة التعليمية وتجديدها بحيث تستوعب مقاييس، وتخصصات في الأمن السيبراني مما يترتب عليه وجود خبراء تقنيين في هذا المجال لتعزيز الدفاع ضد الهجومات السيبرانية، ورفع لنسبة الوعي فيه من جهة أخرى لمن لم يتخصص فيه مستقبلا.
- ✓ تدريب المحكمين على استعمال التقنيات الحديثة الخاصة بالذكاء الاصطناعي والمعتمدة في مراكز التحكيم الإلكتروني لضمان السير الناجح للمحاكمة.

قائمة المراجع:

1) ألبانا إيسيني، "الذكاء الاصطناعي والأمن السيبراني دراسة فيما يخبئه المستقبل"، مركز البيان للدراسة والتخطيط، ترجمة باسم علي خريزان، 2022م.

2) آمنة على البشير محمد، "الأمن السيبراني في ضوء مقاصد الشريعة"، مجلة كليات الدراسات الإسلامية والعربية للبنات بالإسكندرية، العدد37، مجلد 1.
3) أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي الإنساني"، مجلة الشريعة والقانون، العدد 35،ج 3.
4) بشرى حسين الحمداني، القرصنة الإلكترونية أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، الأردن، ط1، 2014م.
5) خالد ممدوح ابراهيم، ابرام العقد الإلكتروني، الدار الجامعية، الاسكندرية، ط1، 2007م.
6) خوسيه فارغيز، "الذكاء الاصطناعي في مجال الأمن السيبراني: من الضجيج المُثار حوله إلى الواقع"، www.eyeofriyadh.com.
7) روان بنت عطية الله الصحفي، "الجرائم السيبرانية"، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، ماي 2020م.
8) . زعزوعة فاطمة، زعزوعة نجاة، "التحكيم الالكتروني كآلية لتسوية منازعات التجارة الالكترونية في ظل التشريع الجزائري"، مجلة القانون العام الجزائري والمقارن، العدد 1، المجلد 8، ماي 2022م.
9) سعد خليفة سعد الهيفي، "القانون الواجب التطبيق على التحكيم الإلكتروني"، رسالة ماجيستر، قسم القانون الخاص، كلية الحقوق، جامعة الشرق الأوسط، أيلول 2013م.
10) سهام صديق، "نظام التحكيم الإلكتروني لتسوية المنازعات الالكترونية"، مجلة البصائر للدراسات القانونية والاقتصادية، العدد 4، المجلد 2، 2022م.
11) صديقي سامية، بولواطة السعيد، "التحكيم الالكتروني كوسيلة لتسوية منازعات التجارة الالكترونية"، مجلة البيبان للدراسات القانونية والسياسية، العدد 1، المجلد 3، جوان 2018م.
12) طيب كامش، "الإجراء التحكيمي ذو المواصفات الالكترونية في منازعات التجارة الإلكترونية"، مجلة الدراسات القانونية المقارنة، العدد2، المجلد 7،2021م.
13) عبد العزيز بن فهد بن محمد بن داوود، "الجرائم السيبرانية دراسة تأصيلية مقارنة"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العدد3، المجلد 9، 2020م.

14) فاتح حارك، رياض حمدوش، "الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني"، المجلة الجزائرية للأمن الإنساني، العدد 1، المجلد 7، جانفي 2022م.

15) ليتيم فتيحة، ليتيم نادية، "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة"، مجلة المفكر، العدد 12، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة.

16) محمد مأمون سليمان، التحكيم الإلكتروني: التجارة الالكترونية (اتفاق التحكيم، عملية التحكيم، حكم التحكيم)، دار الجامعة الجديدة، الاسكندرية، د ط، 2011م.

17) مصطفى ناطق صالح مطلوب، "التحكيم التجاري الإلكتروني"، مجلة الرافدين للحقوق، المجلد 11، العدد 39، 2009م

18) منى الأشقر جبور، السيبرانية هاجس العصر، المركز الوطني للبحوث القانونية والقضائية. جامعة الدول العربية، د ط، د ت.

19) منى تركي الموسوي، جان سيريل فضل الله، "الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها"، مركز بحوث السوق وحماية المستهلك، جامعة بغداد، مجلة كلية بغداد للعلوم الاقتصادية، 2013م.

20) نورة شلوش، "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الانسانية، العدد 2، المجلد 8،2018م.

21) هواري صباح، "التحكيم الإلكتروني ومدى فعاليته في حل منازعات عقود التجارة الالكترونية"، المجلة العربية في العلوم الانسانية والاجتماعية، عدد 3، مجلد 14، جويلية 2022م.

22) ياسر أحمد العلجوني، التحكيم الإلكتروني وسيلة لفض المنازعات، مجلة المنارة، http://revuealmanara.com