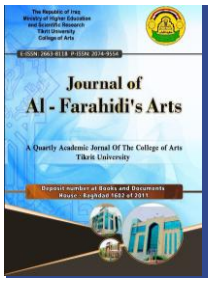

Tikrit University | جامعة تكريت
مجلة آداب الفراهيدي
Journal of Al-Farahidi's Arts

Social Dimensions of Hacking and Cyber Security

[*] Lecturer. Dr. Omar Jassim Mohammed
[1] Asst. Lecturer. Mohammed Burhan Mahdi
[2] Asst. Lecturer. Jamal Ibrahim Ghazai
[*], [1], [2] Department of Sociology, College of Arts, University of Anbar
[*], [1], [2] Al-Anbar, Iraq

الأبْعاد الاجْتماعيَّة لِلْقرْصنة الإلكْترونيَّة والأَمْن السِّيبْراني

(*) م. د. عمر جاسم محمد
(١) م. م. محمد برهان مهدي
(٢) م. م. جمال إبراهيم غزاي
(*)، (١)، (٢) قسم الاجتماع، كلية الآداب، جامعة الأنبار
(*)، (١)، (٢) الأنبار، العراق

SUBMISSION التقديم	ACCEPTED القبول	E-PUBLISHED النشر الإلكتروني
10/08/2024	17/10/2024	30/12/2024

P-ISSN: 2074-9554 | E-ISSN: 2663-8118 https://doi.org/10.25130/jaa.9th.1.23 Conference (9th) No (1) September (2024) P (286-296)

ABSTRACT

The topic of electronic piracy is one of the topics that has dangerous social dimensions for society because it has become one of the emerging global crimes in society that accompanied the digital technological progress and its destructive social effects on infrastructure and social effects on individuals in their digital communication and the psychological, social, economic and political effects it creates. It has become one of the phenomena that affect most societies alike, whether those societies are advanced or simple. As long as they are connected through the digital space, and on this basis, the research aims to identify the social dimensions of electronic piracy, and to know the role of cyber security in confronting these social risks, and to know the negative effects of electronic piracy, and to know the mechanisms followed by the state to try to stop these attacks to protect members of society, and to know the strategies aimed at reducing the risks of electronic piracy in our Iraqi society. On this basis, the study concluded that there are important negative social dimensions of piracy that affect the lives of People who communicate through the digital space, and there are important and necessary positive social dimensions of cybersecurity for users and the state alike, as preventive cybersecurity is one of the important, necessary and important strategies for every state in order to preserve society and the state. Cyberspace has imposed an urgent reality full of challenges and has negative social effects if it is addressed by technological and scientific methods in order to preserve society and the state and transform it into positive benefits.

الملخص

يُعَد مَوضُوع القرْصنة الإلكْترونيَّة مِن المواضيع اَلتِي لَهَا أبْعادًا اِجْتماعيَّة خَطِيرَة على المجْتمع لِأَنَّهَا أَصبَحت مِن الجرائم العالميَّة المسْتحْدثة فِي المجْتمع اَلتِي رافقتْ التَّقَدُّم التِّكْنولوجيَّ اَلرقْمِي ومَا لَه مِن آثار اِجْتماعيَّة مُدَمرَة لِلْبنى التَّحْتيَّة وآثار اِجْتماعيَّة على الأفْراد فِي تواصلهم اَلرقْمِي ومَا يَخلُقه مِن آثار نَفسِيَة واجْتماعيَّة واقْتصاديَّة وسياسيَّة وَأَصبحَت مِن الظَّواهر اَلتِي تَطَال أَغلَب المجْتمعات على حدٍّ سَوَاء أكانتْ تِلْك المجْتمعات مُتَقدمَة أم بَسِيطَة مَا دَامُوا مُتواصلِيْن عَبْر الفضَاء اَلرقْمِي، وَعلَى هذَا الأَسَاس بَهدِف البحْث فِي التَّعَرُّف على الأبْعاد الاجْتماعيَّة لِلْقرْصنة الإلكْترونيَّة، وَمعرِفة دَوْر الامن السِّيبْراني فِي مُوَاجهَة تِلْك المخاطر الاجْتماعيَّة، والتَّعرُّف على الآثَار السَّلْبيَّة لِلْقرْصنة الإلكْترونيَّة، وَمعرِفة الآليَّات المتْبعة مِن قِبل الدَّوْلة لِمحاولة إيقَاف تِلْك الهجمات لِحماية أَفرَاد المجْتمع، والتَّعرُّف على الاسْتراتيجيَّات الهادفة لِلْحدِّ مِن مَخاطِر القرْصنة الإلكْترونيَّة فِي مُجْتمعنَا العراقِيّ وعلى هذا الأساس توصلت الدراسة الى أن هناك أبعاد اجتماعية سلبية مهمة للقرصنة تؤثر على حياة الأشخاص الذين يتواصلون عبر الفضاء الرقمي، وهنالك أبعاد اجتماعية إيجابية مهمة وضرورية للأمن السيبراني للمستخدمين والدولة على حد سواء، فالأمن السيبراني الوقائي هو أحد الاستراتيجيات المهمة والضرورية والهامة لكل دولة من أجل الحفاظ على المجتمع والدولة. لقد فرض الفضاء السيبراني واقعا ملحا مليئا بالتحديات وله آثار اجتماعية سلبية إذا تم معالجته بالطرق التكنولوجية والعلمية من أجل الحفاظ على المجتمع والدولة وتحويله إلى فوائد إيجابية.

KEYWORDS

Cybersecurity, Social Dimensions, Hacking, Social Impacts

الكلمات المفتاحية

الأمْن السيبراني، الأبْعاد الاجْتماعيَّة، القرصنة الالكترونية، الاثار الاجتماعية

المقدمة:

ان القرصنة الالكترونية لها مضار كبيرة وجسيمة على المجتمع وتمس حياة الناس من المستخدمين لتلك الوسائل التكنولوجية التي هي من سمات عصرنا الحالي وفي جميع مناحي حياتهم فتعددت اشكال ووسائل الاختراقات في عصرنا هذا وفي ضوء ثورة المعلومات الحديثة مما ينجم عنه أثاراً سلبية عديدة ويخلق تحديا قويا على المجتمع بكافة مؤسساته وتحديا قويا أيضا على الأمن السيبراني. مما يدعو الى تحديد تلك المشكلة التي تخلق نوعا جديدا من الجرائم التي تواجه المجتمع وبشكل متكرر ومتجدد من اجل الاستعداد لمواجهة تلك الهجمات الالكترونية وما لها من تداعيات تؤثر سلبا على المجتمع.

أهمية البحث:

في عالمنا المعاصر اليوم الذي يتصف بالتواصل الرقمي أصبح من المهم جدا الاهتمام ببرامج الدفاع السيبراني، من اجل الحفاظ على المعلومات وسلامتها، وكذلك حماية الأجهزة والشبكات من الاختراقات والقرصنة الالكترونية والجرائم الالكترونية. وهنا تكمن أهمية البحث في رفد الأكاديميين والباحثين والمختصين في قضايا الامن السيبراني التي يمكن ان يتنبؤوها في سياساتهم التنموية والوقائية، ولاسيما بقضايا القرصنة الالكترونية والامن السيبراني.

أهداف البحث:

يهدِف البحث في التَّعَرُّف على الأبْعاد الاجْتماعيَّة لِلْقرْصنة الإلكْترونيَّة، وَمعرِفة دَوْر الامن السِّيبْراني في مُوَاجهَة تِلْك المخاطر الاجْتماعيَّة، والتَّعرُّف على الآثَار السَّلْبيَّة لِلْقرْصنة الإلكْترونيَّة، وَمعرِفة الآليَّات المتْبعة مِن قِبل الدَّوْلة لِمحاولة إِيقَاف تِلْك الهجمات لِحماية أَفرَاد المجْتمع، والتَّعرُّف على الاسْتراتيجيَّات الهادفة لِلْحدِّ مِن مَخاطِر القرْصنة الإلكْترونيَّة في مُجْتمعنَا العراقِيّ.

منهجية البحث:

١. مفاهيم ومصطلحات الابعاد الاجتماعية والقرصنة الالكترونية والامن السيبر اني:

١-١. الابعاد الاجتماعية:

البعد لغة هو أتساع المدى ويقولون في الدعاء عليه (بعداً له) هلاكاً، ويقال انه لذو بعد اي ذو رأي عميق وحزم، ويقال (بعدك) يحذره شيئا من خلفه والبعد خلاف القرب وهو أقصر امتداد بين الشيئين (الحنفي، ٢٠٠٠، ١٦٠). أما البعد اصطلاحا: وكل ما يكون بين نهايتين غير متلاقيتين وهو امتداد اما قائم بجسم وهو عرض، واما بنفسه وهو جوهر مجرد، والأبعاد الثلاثة هي الطول والعرض والعمق، وأضاف أينشتاين الى هؤلاء بعداً رابعاً هو الزمن والبعد هو الامتداد موهوماً أو موجوداً، لأن في البعد اختلافاً، فانه موهوم أي لا شيء محض عند المتكلمين النافين للمقدار (مصطفى، ٦٣).

وتعرف الابعاد الاجتماعية: هو المسافة بين مختلف الفئات في المجتمع مثل الطبقة الاجتماعية والعرق والجنس والأديان والمذاهب ... وهو مقياس القرب أو الحميمية الذي يشعر به الفرد أو المجموعة تجاه فرد أو مجموعة أخرى في شبكة اجتماعية أو مستوى الثقة التي تتمتع بها مجموعة لأخرى ومدى التشابه المدرك للمعتقدات والثقافة (Boguna, 2004, 8).

التعريف الاجرائي للأبعاد الاجتماعية: الأبعاد الاجتماعية للرابط الاجتماعي تعني المعايير والعوامل التي تؤثر على العلاقات والروابط بين الأفراد في المجتمع. وتشمل هذه الأبعاد العديد من العوامل المختلفة مثل العرق والانتماء القومي، الجنس الجندر، الطبقة الاجتماعية...

١-٢. القرصنة الالكترونية:

عملية اختراق لأجهزة الحاسوب أو المواقع او الهواتف الذكية تتم عبر شبكة الانترنت غالبا لان اغلب الحواسيب والاجهزة الذكية في العالم مرتبطة عبر هذه الشبكة أو حتى عبر شبكات داخلية يرتبط بها أكثر من جهاز حاسوب ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في اختراق برامج الحاسوب والأجهزة الذكية

وطرق ادارتها أي أنهم مبرمجون ذو مستوى عال يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين او أي جهاز ذكي موصول بالأنترنت للتعرف على محتوياته ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة (عبد الرزاق، ٢٠١٢، ٣٠).

التعريف الاجرائي للقرصنة الالكترونية: هي عملية اختراق أنظمة الكمبيوتر والشبكات بشكل غير قانوني للحصول على معلومات أو تعطيل الخدمات أو الوصول إلى بيانات سرية. يتنوع القراصنة بين هاكر Hacker أخلاقي او ابيض White Hacker يعمل على اختبار أنظمة الأمان ويسعى لحمايتها وبين هاكر Hacker ضار او اسود Black Hacker يقوم بأعمال غير قانونية لأغراض شخصية أو مالية. تختلف أهداف القرصنة بين سرقة المعلومات، التجسس، الابتزاز، وتعطيل الخدمات الإلكترونية. من المهم اتخاذ إجراءات أمنية قوية لحماية الأنظمة والشبكات من هذه الأنشطة غير المشروعة.

١-٣. الامن السيبراني:

أمن لغة: أمن البلد اي اطمان به أهله فهو أمن (قرطاس، ٢٠٢٣، ٦)، اما الامن اصطلاحاً: هو عدم توقع مكروه في الزمن الآتي (الجرجاني، ٢٠١٣، ١٩)، وعرف كذلك: هي القدرة التي تتمكن بها الدولة من إطلاق مصادر قوتها الداخلية والخارجية والاقتصادية والعسكرية في شتى المناحي لمواجهة مصادر الخطر في الداخل والخارج في حالتي السلم والحرب، مع استمرار الانطلاق المؤمن لتلك القوى في الحاضر والمستقبل (قرطاس، ٢٠٢٣، ٧).

اما الأمن السيبراني: فهو أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها لمواجهة التهديدات، ومنع التعديات، أو للحد من اثارها في أقسى واسوا الاحوال (الزهراني، ٢٠٢٠، ١١).

إما التعريف الاجرائي للأمن السيبراني: كل الاجراءات التي تتخذ لحماية الاتصالات والشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من برمجيات وأجهزة ، وما تقدمه من خدمات، وما تحتويه من بيانات ، سواء كانت حماية سابقة وقائية بواسطة وضع أنظمة حماية من المخاطر المحتملة أو حماية لاحقة من أي هجوم سيبراني أو اختراق أو تعطيل للبرامج أو تعديل غير مصرح أو دخول غير قانوني أو استخدام مسيء غير مشروع ويشمل أيضاً المحافظة على البنى التحتية الحساسة للدولة من أي هجمات الكترونية وغيرها وسواء ارتكبت الجريمة السيبرانية عن طريق الجهات الحكومية أو غير الحكومية.

٢. الاثار الاجتماعية للقرصنة الالكترونية:

٢-١. الابعاد الاجتماعية لظاهرة القرصنة الالكترونية:

تطورت عمليات القرصنة الإلكترونية غير المشروعة، وعرفت كظاهرة عالمية تتضمن في معظم الأحيان أكثر أشكال الجريمة المنظمة تقدما. وقد نمت جرائم القرصنة الإلكترونية كشكل جديد من الجرائم- في العقد الماضي بشكل لم يسبق له مثيل على شبكة الإنترنت ووسائل التواصل الاجتماعي. والحقيقة أن الجرائم الإلكترونية أو ما يسمى بـــ Cyber Crimes هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعو الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية (الحريري، ٢٠١٨، ٨٥).

وتنتمي اليوم أعمال القرصنة إلى شبكة عالمية لها قيادتها ومنظماتها، وتعمل وفق مخططات معينة وتمتلك وسائل اتصال ونقل حديثة وأسلحة، وتستخدم أحدث التقنيات في الاتصال عبر الأقمار الاصطناعية مما يثير الكثير من التساؤلات حول عملها وخلفيات نشاطها وتداعياته، مما يضع منظمات عالمية، ودولاً، وسياساتها في دائرة الشك والاتهام (بانيثي، ٢٠٠٥، ٤٤). وقد أثبت الواقع العملي أن الهجمات الإلكترونية المنظمة تمثل خطراً حقيقياً؛ لأنه غالباً ما يتم تنفيذ الهجوم بعد استعداد طويل متضمنا استراتيجيات الهروب،

والاستعداد للاختراق المضاد، وعمليات التمويه، مما يصعب مهمة المدافعين في صد هذا الهجوم. ويترتب على جرائم القرصنة الإلكترونية العديد من الآثار السلبية حيث بات هذا النوع من القرصنة خطراً يهدد اقتصاديات العالم والتي تتنوع أشكالها بدءاً من اختراق البريد الشخصي، والقرصنة المصرفية على حسابات مالية، وصولا إلى التجسس الاقتصادي والسياسي للحصول على الأسرار، أو خطط شركات وأنظمة تطوير منتجاتها (الحريري، ٢٠١٨، ٨٦).

وتعد قرصنة برامج الحاسوب مشكلة عالمية، وقد بلغت الخسائر في اقتصاديات الدول المتقدمة والنامية قيمة هائلة بسبب هذا النوع من القرصنة الإلكترونية؛ لأن تطوير البرمجيات يتطلب استثمارات مالية كبيرة. كما أن الفيروسات والبرمجيات الخبيثة تلحق أضراراً بالغة بالأجهزة والحواسيب المستهدفة تتراوح بين التعطيل الجزئي، وبين التشفير الكامل لكل ما تحتويه ذاكرة التخزين من ملفات، وفي بعض الحالات الأكثر خطورة تكون الإصابة بالبرمجيات الخبيثة مرتبطة بعمل منظم، حيث يطلب الجناة من الضحايا دفع مبالغ مالية مقابل إزالة التشفير واستعادة الملفات الرقمية المتضررة، وهو ما يطلق عليه «جرائم الفدية في مجال الجرائم الإلكترونية (عبد الصادق، ٢٠٠٩، ٥٠).

القرصنة الإلكترونية لها أبعاد اجتماعية متعددة تؤثر على الأفراد والمجتمعات بطرق مختلفة. فيما يلي بعض الأبعاد الاجتماعية الرئيسية للقرصنة الإلكترونية (شلوش، ٢٠١٨، ١٩١):

١. **الأمان الشخصي:** يمكن أن تؤدي القرصنة الإلكترونية إلى سرقة المعلومات الشخصية والمالية، مما يعرض الأفراد لخطر الاحتيال والابتزاز.

٢. **الثقة في التكنولوجيا:** تساهم الهجمات الإلكترونية في تقويض الثقة في التكنولوجيا الرقمية والبنية التحتية الإلكترونية، مما يؤثر على استخدام الناس للإنترنت والخدمات الإلكترونية.

٣. **العلاقات الاجتماعية:** يمكن أن تؤدي القرصنة إلى انتهاك الخصوصية، مما يؤثر على العلاقات الشخصية والعائلية والاجتماعية. على سبيل المثال، يمكن أن تؤدي تسريبات الرسائل الخاصة أو الصور الشخصية إلى مشاكل اجتماعية كبيرة.

٤. **الاقتصاد:** تؤثر القرصنة الإلكترونية على الاقتصاد من خلال تكبيد الشركات والحكومات تكاليف كبيرة نتيجة للاضطرابات الأمنية والخسائر المالية. هذا بدوره يؤثر على العمال والموظفين والمستهلكين.

٥. **الثقافة الرقمية:** تؤدي القرصنة الإلكترونية إلى خلق بيئة من الخوف وعدم الأمان في الفضاء الرقمي، مما يعيق التقدم والابتكار في استخدام التكنولوجيا.

٦. **القانون والنظام:** تحتاج الحكومات إلى تطوير سياسات وتشريعات لمكافحة القرصنة الإلكترونية، مما يتطلب تعاونًا دوليًا وتنسيقًا بين الدول لملاحقة القراصنة وتقديمهم للعدالة.

٢-٢. القرصنة الالكترونية في القانون العراقي:

التطور التكنولوجي، أصبح اليوم علما يتسابق الإنسان في استخدامه وتطويره وتطويعه، وسواء كان هذا التطور فعلا يساهم الإنسان بنشاطه أو تطويع الأجهزة المستخدمة للمساهمة أو المساندة لهذا النشاط، ويستغل بعض الناس استخدام هذه التقنيات بشكل سيئ أو خاطئ سهوا أو عمدا، وبهذا الشكل يتحول هذا الاستخدام إلى فعل إجرامي يعاقب عليه القانون ويستهجنه المجتمع.

ويتباين هذا الفعل الإجرامي المرتكب في التوصيف القانوني للفعل المخالف للقانون من حيث جسامة الفعل بين الجناية والجنحة والمخالفة، ويتم ارتكاب الفعل من قبل شخص أو عدد من الأشخاص أو شركات، مثلما تتباين الأسباب والقصد الجرمي. ولما كان أي فعل مخالفا للقانون ينبغي تجريمه ومعاقبة فاعلة بوجود نص قانوني نافذ ينص على ذلك، كما ينبغي أن يكون هذا الفعل نتيجة السلوك المخالف للقانون، وأن تكون إرادة الفاعل متوجهة لارتكاب هذا الفعل، أي أن القصد الجرمي متوفر وهادف إلى تحقيق النتيجة الإجرامية، وسواء كان الفاعل وحده أو كان شريكا أو مساهما أو محرضا، لذا فان الأفعال الالكترونية المخالفة للقانون،

يجب أن تتوفر لها النصوص القانونية الرادعة المتناسبة مع جسامتها وخطورتها في أمن واستقرار المجتمع. والأجهزة الالكترونية المتنوعة، والتي تتحكم بها الشبكات الالكترونية من أجهزة الكمبيوتر وأنواعها وصولا إلى أجهزة الهاتف المحمول، التي تم اختراعها وتصنيعها لخدمة الإنسان وتسهيل حياته وتلبي خدماته وحاجاته، بما يتناسب مع التطور العلمي في جميع الأصعدة الصناعية والثقافية والاجتماعية (عبيس، ٢٠٢٢، ٤٣٣) ولهذا فإن بعض الافراد يتخصصون في هذا المجال لما تتميز به قدراتهم ومهاراتهم الفنية والعلمية، غير أن بعض الأفراد من بين المتخصصين بمعرفة وتقنية هذه الأجهزة يرتكبون أفعالا مخالفة للقانون بالإساءة إلى أفراد آخرين بقصد شخصي أو بتكليف من آخر أو من مجموعة أخرى، أو يمكن ارتكاب أفعال السرقة والاحتيال واختراق أجهزة الحاسوب لأفراد أو لشركات أو جهات سياسية أو جهات أخرى، ويتم ذلك عبر أساليب الاحتيال والاستغفال عبر المراسلة الالكترونية في الأجهزة، أو اختراق جهات أو شركات لأجهزتها وسرقة ما تخزنه من معلومات وإعادة استخدامها بشكل سيئ أو مضر بتلك الجهات، أو الاستحواذ على الصور الشخصية وإعادة ترتيبها بشكل مسيء أو مخجل وتهديد أصحابها لكسب المال أو الايغال بالإساءة لهم، وكانت قد انتشرت قبل فترة عمليات سرقة المقالات والكتابات وإعادة ارسالها بأسماء أخرى، كما يحدث أحيانا ان يقوم فرد باختراق موقع أو شبكة لبث أخبار أو صور مسيئة أو مخالفة للأخلاق ويرفضها المجتمع، أو ان يقوم بتعطيل عمل الموقع أو ما توفره الشبكة الالكترونية للمستخدمين (عبيس، ٢٠٢٢، ٤٣٤).

قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل لم يكن مواكبا لهذه الجرائم مع انه نص في المادة ١٨٢ علي معاقبة من ينشر أو يذيع اخبار بأية صورة وعلي أي وجه وبأية وسيلة معلومات أو صور أو وثائق أو مكاتبات أو غير ذلك، خاصة بدوائر الدولة والمصالح الحكومية وكانت محظور نشرها أو اذاعتها، كما ورد في بعض مواده تعريف الاصطناع في المادة ٢٩١ عقوبات (انشاء محرر لم يكن له وجود من قبل ونسبته إلى غير محرره دون ما ضرورة لتعمد تقليد محرر بالذات وخط انسان معين)، وعاقب في المادة ٣٦١ من عطل عمدا وسيلة من وسائل الاتصال السلكية أو اللاسلكية المخصصة للمنفعة العامة، وفي المادة ٤٠٣ عاقب صانع أو مستورد أو حائز المطبوعات والكتب والرسوم المخلة بالحياء والآداب العامة، وفي المادة ٤٠٤ عاقب كل من جهر بأغاني أو اقوال فاحشة أو مخلة بالحياء بنفسه أو بواسطة جهاز آلي وفي محل عام، وفي المادة ٤٣٢ عاقب كل من هدد بالقول أو الفعل أو الإشارة كتابة أو شفاها، واعتبر في المادة ٤٣٤ أفعال رمي الغير بما يخدش الشرف أو الاعتبار أو جرح المشاعر وان لم يتضمن اسناد واقعة معينة من الظروف المشددة اذا وقع بطريق النشر بالصحف أو المطبوعات أو طرق الاعلام الأخرى (العلوي، ٢٠٢٤، ٣٠٠).

ولما كان قانون مكافحة الجرائم الالكترونية يهدف إلى مكافحة هذه الجرائم التي تشكل تهديدا لأمن المجتمع وامن الدولة والاستقرار، بالإضافة إلى أن التطور السريع في مجال تقنية المعلومات تستوجب توفير الحماية القانونية ومعاقبة كل من يرتكب فعلا يخالف القانون واقتران تلك العقوبات بالظروف المشددة عند فرض العقوبة، خصوصا بعد ظهور حالات الابتزاز والانتحال والاحتيال والتعدي على الشرف والأخلاق وقيم المجتمع، وظهور صور جديدة تتمادى في أفعالها تتحدى القانون والمجتمع وتتطوع العقل العلمي والفني إلى عقل إجرامي مقترن بخلل نفسي، ليكون ضرره كبيرا، وتمس بالحياة الخاصة للأفراد وتهدد الأمن الوطني والسيادة الوطنية وتضعف الثقة بالتقنيات الحديثة وتهدد ابداع العقل البشري.

من اهم سبل الوقاية من عمليات القرصنة الالكترونية والتي يجب العمل عليها هي (مبالطة، ٢٠٢٢، ١٨):

١. **الحماية من الفيروسات:** وترجع أهمية الحماية من الفيروسات لما تحتويه هواتفنا من معلومات شخصية مرتبطة بالحياة الخاصة والعمل، ويجب حمايتها دائما وأبدا من القرصنة الالكترونية لذلك يمكن اعتبار الحماية من الفيروسات هو خط دفاعك الأول ضد هذه القرصنة

٢. **تشفير الرسائل النصية:** وأيا كان نوع هاتفك الذكي أو مدى أهمية الرسائل النصية والمكالمات وحساسيتها لابد أن تجعلها دائما في وضع الإخفاء، ويتم ذلك عن طريق استخدام خاصية التشفير سواء لرسائلك النصية أو مكالماتك الخاصة.

٣. **قفل الشاشة:** تشير التقارير إلى أن ما يقارب من ٤٠ بالمئة من مالكي الهواتف الذكية لا يهتمون بقفل الشاشة أو ميزات الأمان الأخرى مع أن قفل الشاشة الرئيسية هي الطريقة الأسهل والأكثر وضوحا للحفاظ على حماية هاتفك بانتظام، بالإضافة إلى ذلك يوصي الخبراء بان تبذل قصارى جهدك لتأكد من عدم وجود كلمة مرور ضعيفة وتعلم كيفية قفل التطبيقات على هاتفك.

٤. **شبكات الانترنت العامة:** قد تكون في مكان عام أو في أحد المقاهي (الكافيهات) والتي تسمح لك باستخدام شبكة الانترنت بالمكان ولكنها تشترط عليك ادخال بياناتك أو حتى بريدك.

٣. الامن السيبر اني في مواجهة القرصنة الالكترونية:

٣-١. ابعاد الامن السيبر اني:

أولاً: الابعاد الاجتماعية: أن معظم تطبيقات شبكة المعلومات الدولية كالمدونات ومواقع التواصل الاجتماعي منحت الفرصة لأغلب المستخدمين بأن يعبروا عن آرائهم السياسية ومتطلباتهم الاجتماعية. بالإضافة الى السمات التي يتمتع بها الانترنت من امكانات تكنولوجية هائلة في جميع الحقول الخدمية والمعلوماتية والتي تصل الى جميع بقاع الأرض ولأغلب الشرائح، والذي يمكن ان يعمل على تبادل المعلومات في أوقات الازمات الانسانية والكوارث بل تتعدى الى المحافظة على الايدولوجية المجتمعية وكان حرص المؤسسات والتنظيمات الدولية على بث صورة تثقيفية وتوعوية للأمن في الفضاء السيبراني وضمان تفعيله وحث المجتمع الدولي على اهمية تحقيق (عادل، ٢٠١٧، ٢٤).

ثانياً: الابعاد الاقتصادية: يرمى إلى توفير المناخ المناسب لتأمين احتياجات الشعب وتوفير سبل التقدم والرفاهية له فمجال الأمن الوطني هو الاستراتيجية العليا الوطنية التي تهتم بتنمية واستخدام كافة موارد الدولة لتحقيق اهدافها السياسية كذلك النمو الاقتصادي والتقدم التكنولوجي هما الوسيلتان الرئيسيتان والحاسمتان لتحقيق المصالح الأمنية للدولة وبناء قوة الردع الاستراتيجية وتنمية التبادل التجاري وتصدير العمالة والنقل الأفقي للتكنولوجيا وتوطينها وبخاصة التكنولوجيا العالية و الحيوية وفي ظل أمن المعلومات الأمن السيبراني برز مفهوم اقتصاد المعرفة"، الذي يعتمد على استخدام تقنيات المعلومات والاتصالات بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة، على كل المستويات. إذ عملت تقنيات المعلومات والاتصالات على تعزيز التنمية الاقتصادية لبلدان كثيرة، عبر افادتها من فرص الاستخدام، التي تقدمها الشركات الدولية، والشركات الكبرى، التي تبحث عن ادارة كلفة انتاجها، بأفضل الشروط الا ان هذا الواقع، يطرح مسائل مختلفة، سواء منها ما يتعلق بحماية مقدم الخدمة، والعمل، أو بحماية المستهلك على الانترنت (محمد، ٢٠٠٠، ٩٨).

ثالثاً: الابعاد القانونية: يؤدي الدور الشخصي والنشاطات والهيئات الحكومية دوراً جداً فاعل في الفضاء الخارجي الالكتروني ويعطي حلولاً ونتائج تساعد في نزع فتيل الأزمات والحروب التي تشكلت بسببها. لهذه الأسباب تستدعي الحاجة الى وضع دراسة متوازنة بين التغييرات التي اصابت المجتمع الدولي وبين تعزيز حقوق الانسان وحريته الشخصية التي دونت في القانون الدولي ومنظمات مراقبي حقوق الانسان وحقوق اخرى تم اضافتها كحق الوصول الى الانترنت والحق في انشاء مدونات الكترونية ، وضمان الملكية للمعلومات، وتوأمة القوانين مع الاقتصاد كحق الاحتفاظ بالبيانات الابلاغ عن جرائم الاختراق والابتزاز الالكترونية وجرائم تخص المحتوى ذات اثار اقتصادية سلبية لذا يجب الحفاظ على سرية البيانات والمعلومات للأفراد وخصوصيتها (جبور، ٢٠١٦، ٦٢).

رابعاً: البعد السياسي: يلعب التطور المتزايد في مجال الفضاء السيبراني دورا كبيرا في التأثير على الأنظمة السياسية للدول في عمليات التجسس والقرصنة الالكترونية التي تقوم بها بعض الشبكات من الاضرار بأنظمة تلك الدول والسيطرة على منظومة المعلومات السرية الخاصة بها ، كما هو الحال بالتدخل الروسي السيبراني في الانتخابات الأمريكية عام ٢٠١٦ ، فضلا عن التسريبات للوثائق الحساسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول ، كما أن القضاء السيبراني اصبح بنية خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين (ايكن، ٢٠١٨ ، ٥٦).

خامساً: البعد العسكري: تنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات وحالة من عدم الاستقرار والنزاعات المسلحة واختراقات أنظمة المنشاة النووية وما قد يحدث عنها من تهديدات لأمن الدول والحكومات وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات السكرية ببعضها البعض على الشبكات العسكرية في الفضاء الالكتروني بما يسمح بسهولة تدفق المعلومات وتناقلها وسرعة اتخاذ القرارات العسكرية وتحقيق الأهداف عن بعد (عبد الصادق، ٢٠٠٩ ، ٩٩).

٣-٢. الوسائل الحكومية لتعزيز الأمن السيبراني في العراق:

تتمثل الوسائل الحكومية بوضع سياسة عامة سليمة تحد من مخاطر التهديدات السيبرانية وتندرج تحت هذه السياسة اطر تشريعية وتفعيل لدور المؤسسات التنفيذية والقيام بحملات توعوية وسيتم التطرق اليها كالاتي:

أولاً: الأطر التشريعية لتعزيز الأمن السيبراني في العراق: ان تعزيز الأمن السيبراني والمعلوماتي في العراق يتطلب اصدار تشريعات حكومية خاصة وتبني قوانين فعالة يتم تطبيقها على القطاع الحكومي والخاص فالتدخل التشريعي يتم من خلال تجريم ما تقوم به المنظمات الارهابية بجميع اعمالها التخريبية والتجسسية والحربية وتشديد العقوبات على هذه الاعمال، فمواجهة الارهاب تشريعيا يكون من المهم والضروري مواكبة التطور الحاصل في مجال القرصنة الالكترونية من خلال القوانين والتشريعات الكافية والتصدي الملائم لهذه الجرائم (سلطان، ٢٠٢٣ ، ٢٦٤).

ثانياً: تفعيل دور المؤسسات الحكومية الخاصة: تعد الاجهزة الأمنية الخاصة في أي دولة الداعم الاساس لحفظ امن الوطن وسلامته والسهر على راحته وتتمثل هذه الاجهزة ب (وزارة العلوم والتكنولوجيا / وزارة الاتصالات، وزارة الداخلية، وزارة المالية، البنك المركزي العراقي، ديوان الرقابة المالية، هيئة الاعلام والاتصالات، فريق الاستجابة للأحداث السيبرانية CERT) فلا بد من تعاون وتكاتف جهود كل تلك الجهات لتنفيذ الاستراتيجية الوطنية العراقية للأمن السيبراني والعمل وفق منهجية خاصة لحفظ سرية بيانات الدولة وحمايتها (سلطان، ٢٠٢٣ ، ٢٦٥).

ثالثاً: تطوير الدور التوعوي الحكومي لتعزيز الأمن السيبراني العراقي: ان الأمن السيبراني كشف عن حقيقة اخرى الا وهي أن الناس هم أضعف حلقة في سلسلة الأمن السيبراني، فهذا يتطلب قيام الحكومة ومؤسساتها بنشر بناء ثقافة امنية وزيادة وعي المستخدمين بالمخاطر السيبرانية المعاصرة فعلى الحكومة توعية شعوبها وتبني استراتيجيات للأمن السيبراني ووضع نظام أمني وقانوني مناسب يتم تطبيقه في المؤسسات الحكومية وعمل حملات توعية كبيرة وفقا لكوادر متقدمة في مجال التكنولوجيا والمعلومات والاتصال (العلوي، ٢٠٢٤ ، ٢٩٨).

٣-٣. الامن السيبراني في ظل القرصنة الالكترونية:

في عصرنا الحديث، تزداد أهمية الأمن السيبراني بشكل متسارع. مع التقدم التكنولوجي والتحول الرقمي المستمر، تنشأ تحديات جديدة تتعلق بالقرصنة الالكترونية وتهديدات أمن المعلومات. تمتد نطاق هذه الجرائم من الاختراقات الإلكترونية والاحتيال الإلكتروني إلى سرقة الهوية والقرصنة الإلكترونية، مما يضع الأفراد والمؤسسات وحتى الدول في خطر.

إنه في ظل تنامي التوتر والصراعات في العلاقات بين الدول على المستويين الإقليمي أو الدولي، يتوقع أن تلجأ الدول إلى توظيف الحروب الإلكترونية كأدوات إضافية في إدارة صراعها مع خصومها، خاصة مع تنامي أدوار الفواعل المسلحة من غير الدول، وهو ما يؤشر إلى زيادة التهديدات التابعة من الفضاء السيبراني مستقبلا، مما يتطلب من الدول كافة اتخاذ إجراءات لضبط سلوكها في الفضاء السيبراني، فضلا عن تطوير قدرات دفاعية لتأمين نفسها في مواجهة تلك التهديدات، وفي هذا الصدد فإنه يمكن الإشارة إلى أن الدفاع السيبراني الوقائي يتحقق من خلال ثلاثة أساليب رئيسية وهي (كلاع، ٢٠٢٢، ٣٠٧):

١. الكشف المبكر عبر الهجمات في وقتها الحقيقي وهو ما يتم من خلال استخدام حساسات" (Sensors) على الشبكات والبرامج والتطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يصنفوا على أنه هجمات سيبرانية، وبداية مواجهتها واحتواءها قبل أن تبدأ نشاطها في الشبكة أو النظم المستهدفة.

٢. الهجوم السيبراني الاستباقي وذلك من خلال استخدام ونشر الديدان البيضاء (White Worms)، وهي برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمات سيبرانية محتملة، كما تقوم أيضا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمات نفسها، وتحديد هوية ومصدر الهجمة، بما يمكن من إطلاق هجمة إلكترونية مضادة فيما تعرف بـ الاختراق العكسي.

٣. التضليل والإخفاء والخداع وهو ما يتحقق عن طريق إخفاء هويات الأهداف الاستراتيجية للدولة على الأنترنت وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها من خلال أدوات التمويه والخداع وتغيير ملامح الأهداف الاستراتيجية للدولة، بما يساعد على تضليل الخصم وتشتيت الانتباه عن الهدف الرئيسي.

فإن التحديات توازي التقدم التكنولوجي، وهناك حلول مبتكرة تُطوَّر لمكافحة الجرائم القرصنة الالكترونية وتحسين الأمن السيبراني. يتطلب ذلك نهجاً شاملاً يجمع بين الوعي والتعليم والتكنولوجيا والتعاون الدولي (سالم، ٢٠٢٢، ٢٥).

أولاً: يأتي توعية المجتمع بأهمية الأمن السيبراني كخطوة أساسية في مكافحة جرائم القرصنة الالكترونية. يجب على الأفراد فهم التهديدات والمخاطر المحتملة واتخاذ التدابير الوقائية المناسبة. يمكن تحقيق ذلك من خلال حملات توعية وتثقيف الناس بأفضل الممارسات في استخدام التكنولوجيا والوقاية من الهجمات الإلكترونية.

ثانياً: يجب تطوير التشريعات والقوانين لمكافحة القرصنة الالكترونية وحماية الأفراد والمؤسسات. يجب أن تكون هذه القوانين محدثة ومتطورة لمواجهة التهديدات الجديدة وتوفير عقوبات رادعة للمتسببين في القرصنة الالكترونية. ينبغي أن تشمل هذه التشريعات أيضًا تعزيز التعاون بين القطاع العام والخاص في مجال مكافحة القرصنة الالكترونية.

ثالثاً: يعد التعاون الدولي أمرًا حاسمًا في مكافحة القرصنة الالكترونية. يجب على الحكومات والمؤسسات الدولية التعاون في تبادل المعلومات والخبرات وتطوير إطار عمل مشترك لمكافحة الهجمات السيبرانية. يمكن تحقيق ذلك من خلال تبني معايير دولية وتنظيم المؤتمرات والجلسات التعليمية لتبادل المعرفة وتوحيد الجهود.

رابعاً: يمكن استخدام التكنولوجيا المتقدمة والحلول المبتكرة لتعزيز الأمن السيبراني. يمكن استخدام الذكاء الاصطناعي وتحليل البيانات الضخمة للكشف عن أنماط الهجمات والتهديدات. يمكن أيضًا تطوير أنظمة مراقبة وكشف تلقائي للاختراقات لتحديد الهجمات المحتملة واتخاذ التدابير الوقائية. تتضمن هذه الحلول أيضًا تطوير تقنيات التشفير والحماية لضمان سلامة البيانات والمعلومات الحساسة.

خامساً: يجب تعزيز الأمن السيبراني في المؤسسات التعليمية. يعد التدريب والتعليم في مجال الأمن السيبراني ضروريًا لتمكين الأفراد من التعامل بشكل آمن مع التكنولوجيا والوقاية من الهجمات السيبرانية. يجب توفير

برامج تعليمية تركز على أمان المعلومات وحماية البيانات الشخصية، ويجب تدريب الطلاب والمعلمين على استخدام التكنولوجيا بشكل آمن ومسؤول.

وأخيرًا، يمكن أن يلعب القطاع الخاص دورًا هامًا في مكافحة القرصنة الالكترونية وتعزيز الأمن السيبراني. يمكن للشركات تطوير حلول تكنولوجية متقدمة للكشف عن الهجمات والحماية منها. يجب أن تتعاون المؤسسات الحكومية والخاصة في تبادل المعلومات والخبرات والعمل بشكل مشترك لتعزيز الأمن السيبراني في المجتمع الحديث.

٤. النتائج والتوصيات:

٤-١. النتائج:

من النتائج التي تم التوصل لها ما يلي:

١. هنالك ابعاد اجتماعية سلبية للقرصنة مهمه تؤثر في حياة الناس المتواصلين عبر الفضاء الرقمي.

٢. هنالك ابعاد اجتماعية إيجابية مهمه وضرورية للأمن السيبراني للمستخدمين وللدولة على حد سواء

٣. الامن السيبراني الوقائي من الإستراتيجيات المهمة والضرورية والمهمة لكل دولة من اجل الحفاظ على المجتمع والدولة.

٤. فرض الفضاء السيبراني واقعا ملحا مليئا بالتحديات وله اثار اجتماعية سلبية إذا ما كان التصدي له بالطرق التكنولوجية والعلمية من اجل الحفاظ على المجتمع والدولة وتحويله الى منافع ايجابية.

٤-٢. التوصيات:

١. ضرورة إقامة دورات مكثفة وتوعية المجتمع من مخاطر القرصنة وبالمقابل أهمية الأمن السيبراني من اجل سلامة المعلومات والخصوصية وسلامة الامن المجتمعي.

٢. ضرورة العمل على تطوير التطبيقات والبرامج المضادة للقرصنة الإلكترونية.

٣. العمل انفاذ قانون يجرم العمل او التعامل بالقرصنة الإلكترونية وتحديد عقوبات وغرامات واضحة تجاه المخترقين والمتعاملين بالقرصنة الالكترونية.

٤. العمل على دعم كل الجهود المبذولة في سبيل تحقيق الامن السيبراني في المؤسسات الرسمية وغير الرسمية.

المصادر:

الحنفي. ع (٢٠٠٠)، المعجم الشامل لمصطلحات الفلسفة، ط٣، مكتبة مدبولي القاهرة، ص ١٦٠.

مصطفى. أ، وآخرون المعجم الوسيط، ج ١، دار الدعوة، اسطنبول، ب ت، ص ٦٣.

عبد الرزاق ع، (٢٠١٢) القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني"، مجلة السياسة الدولية، (العدد٣٠)، ص٣٠.

قرطاس. م (٢٠٢٣)، الامن السيبراني وحقوق الانسان، المفوضية العليا لحقوق الانسان، بغداد، ص٦.

الجرجاني. ع (٢٠١٣)، التعريفات، دار الكتب العلمية، بيروت لبنان، (الطبعة الأولى)، ص١٩.

الزهراني. ع (٢٠٢٠)، استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة دراسة مقارنة، رسالة قدمت لنيل درجة الماجستير في العلوم الإستراتيجية، جامعة نايف العربية، للعلوم الأمنية، كلية العلوم الإستراتيجية قسم الدراسات الاستراتيجية، السعودية، ص ١١.

الحريري. م (٢٠١٨)، الإطار القانوني لتجريم القرصنة الإلكترونية في مملكة البحرين، ص٨٥.

بانيثي. د (٢٠٠٥)، استمرار القرصنة وآثارها على الإبداع والثقافة والتنمية المستدامة دراسة معدة بناء على طلب أمانة منظمة الأمم المتحدة للتربية والعلوم والثقافة في الجلسة الثالثة عشرة للجنة الدولية لحقوق المؤلف، باريس ص ٤٤.

عبد الصادق. ع (٢٠٠٩) الإرهاب الالكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية، ص ٥٠.

شلوش. ن (٢٠١٨)، القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول ،مجلة مركز بابل للدراسات الانسانية ، (المجلد٨)، ص ١٩١.

عبيس. ق (٢٠٢٢)، دور الرسائل الالكترونية في إثبات الجريمة المعلوماتية، مجلة كلية القانون جامعة الكوفة، (العدد، ٥٤)، ص٤٣٣.

العلوي. أ (٢٠٢٤)، الأمن السيبراني العراقي الواقع وآفاق المستقبل، المجلة السياسية الدولية ملحق (العدد٥٨)، ص٢٩٨.

مبالطة. م (٢٠٢٢)، الأمن المعلوماتي في مواجهة القرصنة الالكترونية، دراسات في حقوق الانسان، جامعة ٢٠ اوت ١٩٥٥ سكيكدة الجزائر، (العدد ١)، ص ١٨.

محمد. أ (٢٠٠٠)، السيبرانية كمدخل لتحول مفهوم التصوير إلى فن ما بعد الحداثة للقرن الحادي والعشرين، كلية التربية الفنية، ص ٩٨.

جبور. م (٢٠١٦) السيبرانية هاجس العصر، جامعة الدول العربية المركز العربي للبحوث القانونية والقضائية، بيروت، ص ٦٢.

آيكن. م (٢٠١٨). التأثير السيبراني (كيف يغير الإنترنيت سلوك البشر)، الدار العربية للعلوم ناشرون، بيروت، لبنان، ص ٥٦.

سلطان. أ (٢٠٢٣)، الدور الدولي في تعزيز الأمن السيبراني في ضوء التحديات المعاصرة، المجلة العراقية للعلوم السياسية، (العدد ٩)، ٢٦٤.

كلاع. ش (٢٠٢٢)، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، جامعة الجزائر، مجلة الحقوق والعلوم الإنسانية، (المجلد١٥ / العدد١)، ص٣٠٧.

سالم. ط (٢٠٢٢)، الصحافة الإلكترونية والأمن السيبراني، رسالة ماجستير، جامعة أحمد دراية - ولاية أدرار، كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية قسم العلوم الإنسانية، ص٢٥.

Resources:

Al-Hanafi. A (2000), The Comprehensive Dictionary of Philosophy Terms, 3rd ed., Madbouly Library, Cairo, p. 160.

Mustafa. A, and others, Al-Mujam Al-Wasit, Vol. 1, Dar Al-Da'wa, Istanbul, BT, p. 63.

Abdul Razzaq A, (2012) Electronic Power: Weapons of Mass Deployment in the Cyber Age, International Politics Magazine, (Issue 30), p. 30.

Qurtas. M (2023), Cybersecurity and Human Rights, High Commission for Human Rights, Baghdad, p. 6.

Al-Jarjani. A (2013), Definitions, Dar Al-Kotob Al-Ilmiyyah, Beirut, Lebanon, (First Edition), p. 19.

Al-Zahrani. A (2020), Cybersecurity Strategies in Light of Modern Technologies and Challenges, A Comparative Study, A Thesis Submitted for a Master's Degree in Strategic Sciences, Naif Arab University for Security Sciences, College of Strategic Sciences, Department of Strategic Studies, Saudi Arabia, p. 11.

Al-Hariri. M (2018), The Legal Framework for Criminalizing Electronic Piracy in the Kingdom of Bahrain, p. 85.

Banithi. D (2005), The Continuation of Piracy and Its Effects on Creativity, Culture and Sustainable Development, A Study Prepared at the Request of the Secretariat of the United Nations For Education, Science and Culture in the Thirteenth Session of the International Copyright Committee, Paris, p. 44.

Abdul Sadiq. A (2009) Electronic Terrorism Power in International Relations, A New Pattern and Different Challenges, Cairo, Center for Political Studies, p. 50.

Shaloush. N (2018), Electronic Piracy in Cyberspace, the Rising Threat to State Security, Journal of the Babylon Center for Human Studies, (Volume 8), p. 191.

Abis. Q (2022), The Role of Electronic Messages in Proving Cybercrime, Journal of the College of Law, University of Kufa, (Issue, 54), p. 433.

Al-Alawi. A (2024), Iraqi Cybersecurity, Reality and Future Prospects, International Political Journal Supplement (Issue 58), p. 298.

Mbalata. M (2022), Information Security in the Face of Electronic Piracy, Studies in Human Rights, University of August 20, 1955 Skikda, Algeria, (Issue 1), p. 18.

Muhammad. A (2000), Cyber as an Introduction to Transforming the Concept of Photography into Postmodern Art for the Twenty-First Century, Faculty of Art Education, p. 98.

Jabour. M (2016) Cyber is the Obsession of the Age, League of Arab States, Arab Center for Legal and Judicial Research, Beirut, p. 62.

Aiken. M (2018). Cyber Influence (How the Internet Changes Human Behavior), Arab House for Science Publishers, Beirut, Lebanon, p. 56.

Sultan. A (2023), The International Role in Promoting Cyber Security in Light of Contemporary Challenges, Iraqi Journal of Political Science, (Issue 9), 264.

Kalaa. Sh (2022), Cyber Security and the Challenges of Espionage and Electronic Hacking of Countries via Cyberspace, University of Algeria, Journal of Law and Humanities, (Volume 15 / Issue 1), p. 307.

Salem. T (2022), Electronic Journalism and Cyber Security, Master's Thesis, Ahmed Draia University - Adrar State, College of Humanities, Social Sciences and Islamic Sciences, Department of Humanities, p. 25.

Boguna (2004) Models of social networks based on social distance attachment. Physical Review, p 8.