

التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية:

القرصنة الالكترونية نموذجا

د. بعوني ليلي

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير،

جامعة الجزائر 3

الملخص

تعتبر القرصنة الالكترونية من بين التهديدات المتفشية في الفضاء السيبراني المتصل بشبكة الانترنت، حيث اتسع نطاقها بسبب التطور التكنولوجي في مجال التواصل الاجتماعي وإدخال الرقمنة في التعاملات الاقتصادية والخدمات بشكل كبير لاسيما خلال جائحة كوفيد-19. هذا التحول شكل بيئة خصبة للقرصنة للاعتداء على خصوصيات الأفراد والشركات وعلى سيادة الدول التي تتعرض بشكل مستمر للاختراقات وهو ما يضر بمصالحها وأمنها القومي، وهو الأمر الذي يستدعي التنسيق بين الدول وتعزيز نظم الحماية والرقابة على الفضاء السيبراني لمواجهة أي تهديد محتمل.

الكلمات المفتاحية: القرصنة الالكترونية، السيادة الرقمية، الانترنت، الفيروسات، الاقتصاد الرقمي.

Abstract:

Electronic hacking is considered as an active threat in cyberspace which is connected to the web. Its scope has been widened due to technological development in the field of social communication and the introduction of digitization in economic transactions and services, especially during the COVID-19 pandemic. This transformation has provided a favorable environment for pirates to undermine the privacy of individuals and companies, as well as the sovereignty of countries suffering from constant violation, which undermine their national security and interests. This requires countries to coordinate and to consolidate their security and control systems in cyberspace to deal with any possible threats.

Keywords: Electronic hacking, digital sovereignty, Internet, viruses, digital economy.

المقدمة

لقد ارتبط ظهور الفضاء الرقمي بالتطور التكنولوجي السريع في مختلف المجالات لاسيما فيما يخص حفظ البيانات والمعلومات الخاصة بالأشخاص والمؤسسات. كما كان للعولمة دور كبير في تغيير العلاقات الدولية والاجتماعية، ولعل ما ساهم في هذا التغيير هو تطور وسائل الإعلام والاتصال؛ هذه التقنيات ذات الأهمية في حياتنا اليومية أصبحت في متناول أغلبية أفراد المجتمع الذين يبحثون دائما عن الجديد من خلال وسائل التواصل الاجتماعي والتي استطاعت التأثير على المجتمعات في أنحاء العالم، حيث قربت المسافات من خلال العالم الافتراضي، وأصبح بالإمكان توجيه سلوك الأفراد إما عن طريق البرامج الإعلامية والدعائية المختلفة أو عن طريق الاستخدام المكثف للبرامج والتطبيقات التي تنتجها شركات رائدة في هذا المجال، وذلك حسب الأهداف التي تسعى لتحقيقها خاصة وأنها تتحكم في مثل هذه الوسائل والتقنيات.

إن العالم اليوم مرتبط بشبكة عنكبوتية جعلت منه قرية صغيرة بسبب التدفق الكبير للمعلومات وسهولة الحصول عليها، ولكن نظرا لوجود ثغرات في الكثير من البرامج المرتبطة بهذه الشبكة، فقد ظهر أشخاص يتقنون مجال الإعلام الآلي والبرمجيات ويمتھنون مجال القرصنة لحسابهم الخاص أو لحساب أشخاص آخرين، حيث أصبحت القرصنة الإلكترونية واحدة من أخطر الأدوات والأسلحة التي تهدد أمن الدول وسيادتها الرقمية.

خلال العقدين الأخيرين من القرن الواحد والعشرين، واستجابة لمتطلبات العولمة اتجهت العديد من الدول إلى رقمنة بياناتها وتخزينها ووضع ميكانيزمات لحمايتها من أي اختراق محتمل قد يضر بمصالحها ومصالح أفرادها، وهو ما تعرضت له الكثير من الدول والمؤسسات والتي تكبدت خسائر كبيرة إما بسبب تدمير البيانات أو تخريبها أو سرقتها واستغلالها للابتزاز أو لبيعها مقابل أموال والتي يتم تقديرها حسب نوع المعلومات وأهمية البيانات المتحصل عليها.

وبالرغم من أن النسبة الأكبر من البيانات الرقمية تحتكرها شركات كبرى أغلبها متواجد في الولايات المتحدة الأمريكية على غرار غوغل ويوتوب وميكروسوفت وأبل وفيسبوك وتويتر وغيرها، إلا أن هذه الشركات هي بدورها تتعرض للهجمات الإلكترونية وسرقة بياناتها من طرف القراصنة والذين أغلبهم من خارج حدود الدولة التي تنتمي إليها هذه الشركات.

لقد أصبحت مسألة القرصنة الإلكترونية محل اهتمام الكثير من الباحثين وفي مختلف التخصصات نظرا لخطورتها وصعوبة تقني أثر أصحابها، كما أنها تصنف ضمن الجرائم الإلكترونية التي يعاقب عليها القانون، وبالتالي أصبح لزاما على الدولة اتخاذ التدابير

التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية:
القرصنة الالكترونية نموذجا

والإجراءات اللازمة لحماية بياناتها في الفضاء السيبراني وبالتالي الحفاظ على سيادتها الرقمية.

من خلال ما سبق، يمكن طرح التساؤلات التالية: ماذا نقصد بالقرصنة الالكترونية؟ ومن هم المستهدفون من هذه القرصنة؟ متى تصبح القرصنة الالكترونية تهديدا للسيادة الرقمية؟ وما هي الآليات الكفيلة لمواجهة هذه التهديدات؟

للإجابة على هذه التساؤلات قمنا بوضع الفرضيات التالية:

- كلما تطورت وسائل الاتصال والبرمجيات كلما زادت صعوبة الرقابة عليها.
- الثغرات الأمنية وضعف نظم الحماية الالكترونية تؤدي إلى تهديد السيادة الرقمية.
- التنسيق بين الدول في مجال محاربة القرصنة الالكترونية يساهم في الحد من التهديدات على السيادة الرقمية، لأن القرصنة غالبا ما تكون خارج الحدود الوطنية.

في هذه الدراسة سنتطرق إلى الإطار المفاهيمي للقرصنة الإلكترونية ومخاطرها، من خلال تقديم لمحة عن تطور مجال القرصنة الالكترونية والذي ارتبط بالتقدم التكنولوجي والمجال الرقمي، ثم سنحاول التركيز على الاختراقات الأمنية من خلال التطرق إلى بعض الأمثلة عن ذلك. وبما أن أغلب دول العالم تتجه نحو رقمنة مختلف القطاعات لاسيما الحساسة منها، فسننتقل إلى السيادة الرقمية وذلك انطلاقا من المفاهيم إلى غاية تطورها وكيفية حمايتها.

إن الهدف من هذه الدراسة هو محاولة تحديد المجالات الرقمية التي تدخل في إطار سيادة الدولة وبالتالي أي تعدي أو خرق لهذه المجالات يعد تعديا على سيادتها. إضافة إلى ذلك، سنقوم بتحديد القطاعات الأكثر استهدافا من طرف القراصنة لاسيما خلال السنوات الأخيرة والتي عرفت زيادة في عدد مستخدمي شبكات التواصل الاجتماعي بسبب جائحة كوفيد-19، وفي الأخير سنقدم خلاصة مع بعض الاقتراحات التي يمكن أن تساعد على تفادي الوقوع في فخ هذا النوع من الجريمة الالكترونية.

أولا - القرصنة الالكترونية: المفهوم والتهديدات

تعتبر القرصنة الإلكترونية من بين التهديدات التي تشكل خطرا على خصوصية وأمن البيانات بمختلف أنواعها نظرا لاستغلالها من طرف أشخاص معينين هدفهم إلحاق الضرر بأشخاص آخرين أو لأسباب تتعلق بالفضول، ولهذا يتم إطلاق تسميات مختلفة على القرصنة في الفضاء الرقمي حسب خلفياتهم وأهدافهم.

1. القرصنة الالكترونية وتطورها

لقد تم التطرق إلى مسألة القرصنة الالكترونية في العديد من الكتب والدراسات وبالتالي نجد عدة تعاريف تحاول تحديد هذا المفهوم من وجهة نظر كل تخصص، فهناك من عرف القرصنة الالكترونية بأنها «سرقة المعلومات من برامج وبيانات مخزنة في ذاكرة الكمبيوتر بصورة غير شرعية أو نسخ برامج معلوماتية بصورة غير شرعية بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر أو بواسطة التقاط الموجات الكهرومغناطيسية الصادرة عن الحاسب الآلي أثناء تشغيله وباستخدام هوائيات موصلة بحاسبة خاصة»⁽¹⁾.

وفي تعريف آخر، «يشير مفهوم القرصنة الالكترونية إلى استخدام وسائل الاتصال وتكنولوجيات المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التحايل على أنظمة المعالجة الآلية للبيانات، لكشف البيانات الحساسة (المصنفة) أو تغييرها والتأثير على سلامتها أو حتى إتلافها»⁽²⁾. وحسب الكاتب "ماجد محمد الحنيطي" فإن «القرصنة الالكترونية تعني الوصول إلى أجهزة الآخرين بطريقة غير مشروعة من خلال ثغرات نظام الحماية»⁽³⁾.

أما في الجزائر فقد تبنى المشرع بموجب القانون 04 / 09 من المادة 2 المؤرخ في 14 شعبان 1430 و الموافق لـ 5 غشت سنة 2009 تعريفا للجرائم المعلوماتية واعتبر أنها «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية»⁽⁴⁾ وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء بل توسع نطاقها ليشمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها⁽⁵⁾.

من خلال التعاريف السابقة نلاحظ أن أغلبية المختصين يتفقون على أنها عملية دخول غير مصرح بها إلى أجهزة الغير وشبكاتهم الالكترونية بغرض المساس بالسرية وبخصوصية الأشخاص أو المساس بسلامة المحتوى إما بتغييره أو إتلافه.

ارتبطت القرصنة الالكترونية باستخدام أجهزة الإعلام الآلي والأنترنت، كون هذه الأخيرة تعد حلقة وصل بين شعوب العالم، علما أن فكرة إنشاء شبكة رقمية لنقل المعلومات تعود إلى سنة 1969 حيث كانت تستعمل في القوات المسلحة الأمريكية والتي بدورها قامت بربط الشبكة مع عدد من الجامعات قصد تطوير هذه الشبكة وفق تقنيات جديدة تسمح باستمرار تدفق المعلومات، ولكن نظرا للضغط المتزايد على الأنترنت من طرف الجامعات ومراكز البحث، تم انشاء شبكة جديدة سنة 1983 والتي أطلق عليها اسم الشبكة العسكرية (MILNET) موجهة للقوات المسلحة فقط، ليتم ربطها فيما بعد مع

وبالرغم من اكتشاف الانترنت التي تعد أفضل وسيلة لتقريب المسافات ونقل المعطيات كالصور والفيديوهات بأقل تكلفة وسرعة أكبر، إلا أن هذه الوسيلة تم استغلالها من طرف أشخاص لديهم قدرات كبيرة في مجال برمجة أنظمة الحاسوب، كما أن فضولهم دفعهم إلى ارتكاب جرائم الكترونية ألحقت أضرار بالعديد من المؤسسات والأشخاص. ومن بين قرصنة المعطيات الذي ينشطون بطريقة غير مشروعة من خلال استهداف أنظمة المعلومات نجد أشخاص يطلق عليهم "الهاكر".

2. تصنيف "الهاكر" وتحديد أهدافهم

في السنوات الأخيرة زاد التواصل بين المستخدمين والمبرمجين في الحاسوب، وظهر خلال هذه الفترة مفهوم المخربين والمخترقين للمواقع والأنظمة المختلفة وذلك حسب الأهداف المراد تحقيقها، ومن هنا بدأ استخدام كلمة هاكر، حيث ارتبطت هذه التسمية في البداية بالأعمال الإيجابية التي تقوم بها هذه الفئة من المجتمع التي كانت تكشف الثغرات الأمنية وتقوم بالتبليغ عنها، ولكنها أيضاً لا تخلوا من النتائج السلبية وذلك لكونها تؤثر على مختلف الأشخاص والمؤسسات. وعليه فإن الهاكر «هو شخص يمتلك إمكانيات برمجية وقدرات عالية في التعامل مع برامج الحاسوب الخاصة بالاختراق والشبكات، فيستطيع أن يستغل الثغرات المتاحة أمامه بكل سهولة سواء كان في المواقع أو البرامج أو الأجهزة المختلفة، لأهداف متنوعة، منها سرقة الحسابات أو البيانات أو لأهداف تخريبية»⁽⁷⁾.

وهناك من يعرف الهاكر «على أنهم أشخاص متسللون يتابعون عن كثب آخر الأخبار وبرامج الحماية الأمنية والمعلومات إلى حد أنهم ينشئون النوادي لتبادل المعلومات، وهؤلاء يستطيعون الاجتياز الأمني لمختلف المواقع بقصد التخريب والاختلاس والتزوير»⁽⁸⁾.

من خلال التعاريف السابقة، يمكن القول أن الهاكر أو القرصنة الإلكترونية هي تسمية ارتبطت بالبرمجيات وأنظمة الحاسوب، وأصبحت مع مرور الزمن تصنف من بين أخطر الظواهر التي تهدد البيانات الشخصية في عالمنا الحالي، خاصة مع تغير حياة الأشخاص وارتباطهم بشكل أكبر بالعالم الافتراضي، مما زاد من أعداد ضحايا الاختراق، ليصبح ما كان مخفياً مكشوفاً، وهو ما تشهده يومياً شبكات التواصل الاجتماعي.

يصنف الهاكر إلى ثلاث أنواع وهي هاكر القبعات البيضاء والسوداء والرمادية، والتي تم تعريفها على النحو التالي⁽⁹⁾:

- **هاكر القبعات البيضاء:** هذا النوع من الهاكر يختلف عن غيره من حيث المبدأ والهدف من العمل الذي يقومون به، فهناك من يسميهم بالمخترقين الأخلاقيين على الانترنت، لأن هدفهم هو حماية المستخدمين من أي هجمات الكترونية، كما يقومون باختراق من أجل

الكشف عن الثغرات التي تهدد الأنظمة الالكترونية المتصلة بشبكة الانترنت، ويقترحون الحلول لإصلاحها، وبالتالي فإن هدفهم هو الإصلاح والحماية وليس التخريب.

- **هاكر القبعات السوداء:** يعتبرون من أخطر أنواع الهاكر، حيث يقومون بعمليات الاختراق لأهداف خبيثة وتخريبية، فيخترقون أجهزة وأنظمة المستخدمين من أجل سرقتها أو العبث بها أو تخريبها، وغالبا ما يكون هدفهم هو الحصول على مبلغ مالي عن طريق نشر فيروس الفدية، أو لأهداف سياسية مختلفة تقف ورائها جهات أجنبية أو من خلال أطراف من الداخل مدعومين من الخارج والتي تعتبر كجزء من الحرب السيبرانية.

- **هاكر القبعات الرمادية:** هذا النوع من الهاكر يتوسط النوعين السابقين كونه محايدا، حيث يكون أحيانا ذو توجهات أخلاقية وأحيانا أخرى ذو توجهات غير أخلاقية وتخريبية. فالقبعات الرمادية يستغلون الثغرات الأمنية لتحقيق أهداف معينة وحسب الجهة التي تقف وراء ذلك.

ثانيا- الفضاء الرقمي والتهديدات التي يواجهها

إن اتساع الفضاء الرقمي وصعوبة مراقبته بسبب زيادة عدد المستخدمين عبر العالم وسرعة تدفق المعلومات وتطور وسائل الاتصال، جعله عرضة لمختلف التهديدات السيبرانية التي يقف ورائها قراصنة لديهم أهداف خبيثة تهدد خصوصية الأشخاص وبيانات المؤسسات والدول.

1. مجالات الفضاء الرقمي

يمكن وصف الفضاء الرقمي وفقا لثلاثة مجالات وهي: البيانات التي تعتبر الرهان الرئيسي في هذا الفضاء، والتطبيقات التي تتيح معالجة هذه البيانات، والشبكات التي من خلالها تتم عمليات التواصل والتبادل. هذه المجالات هي على النحو التالي⁽¹⁰⁾:

- **البيانات:** تعتبر البيانات المادة الأولية كونها تشمل مختلف الجوانب السياسية والاقتصادية والاجتماعية والثقافية والأمنية، ولهذا نجد الشركات الكبرى المتخصصة تستثمر أموالا معتبرة من أجل جذب أكبر عدد من المستخدمين وبالتالي بيانات رقمية أكثر؛
- **التطبيقات:** بدون وسائل معالجة البيانات لا يمكن معرفة محتواها وهو ما يتطلب استخدام تطبيقات جد متطورة يمكنها قراءة وتصنيف البيانات ومعالجتها؛
- **الشبكات:** إن البيانات والتطبيقات تتطلب توفير الخوادم Serveurs التي لديها سعة معتبرة للتخزين وقوة المعالج من أجل إرسال هذه البيانات من الفضاء الرقمي إلى

التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية:
القرصنة الإلكترونية نموذجاً

الفضاء الحقيقي أي إلى مختلف أفراد المجتمع، وبالتالي يجب توفر وسائل نقل هذه البيانات إما عبر الأقمار الصناعية أو عبر الكوابل التي تربط مختلف دول العالم.

2. أنواع التهديدات الرقمية

يمكن تقسيم التهديدات الرقمية التي تواجه الدول والأفراد على حد سواء إلى أربعة أنواع، وهي كما يلي⁽¹¹⁾:

- **هجمات الحرمان من الخدمة:** ويتم فيها إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقفه بشكل جزئي أو كلي أو إبطاء عمله، وهذا ما ينتج عنه ضرراً للمستخدم النهائي، وتستعمل هذه الهجمات بكثرة ضد مواقع الانترنت أو البنوك أو المؤسسات بهدف التأثير عليها أو لدفع فدية مالية؛
- **إتلاف المعلومات أو تعديلها:** وهي هجمات تهدف إلى الوصول لمعلومات الضحية عبر شبكة الانترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة، وقد تؤدي إلى نتائج كارثية خاصة إذا تمثلت البيانات في معلومات أمنية أو مواعيد أو خرائط سرية أو خاصة بالصناعات الحساسة لاسيما الصناعات العسكرية؛
- **التجسس على الشبكات:** والمقصود بها الدخول غير المصرح والتجسس على شبكات الخصم أو المنافس، دون تدمير أو تغيير في البيانات والمعلومات، والهدف من الهجمة هو الحصول على معلومات قد تكون تجارية أو خطط تسويقية أو اقتصادية أو مالية أو أسرار حربية أو سياسية، مما يؤثر سلباً على مهام الخصم؛
- **تدمير المعلومات:** حيث يتم في هذه الأخيرة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، ويصطلح عليه «تهديد لسلامة المحتوى» ويتمثل في إحداث تغيير في البيانات والمعلومات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين لذلك.

ثالثاً- السيادة الرقمية والأمن السيبراني

نحن اليوم نعيش في بيئة جديدة ظهرت فيها خريطة جغرافية غير تقليدية تحدد السيادة الرقمية للدول وهو ما يضاف إلى الحدود البرية والجوية والبحرية، وبالتالي أصبحت الدول ملزمة برسم حدودها الرقمية والتي تمارس بداخلها سلطتها وتحافظ على هويتها الوطنية، ومواجهة أي عدوان يهدد أمنها ووحدة أراضيها وشعوبها⁽¹²⁾، وعليه فإن أي فعل يستهدف الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون هي جرائم ضد السيادة الوطنية⁽¹³⁾.

1. من السيادة التقليدية إلى السيادة الرقمية

تعتبر السيادة ركنا أساسيا من أركان الدولة، إلى جانب الإقليم، الشعب، السلطة السياسية والاعتراف الدولي، علما أنه منذ نشأة الدولة القومية على إثر معاهدة «واستفاليا» التي أنهت حروب الثلاثين عاما الدينية في أوروبا خلال الفترة 1618-1648، أصبحت سيادة الدولة على إقليمها تعتبر مبدأ مقدسا في العلاقات الدولية، علما أن مضمونها في ذلك الزمن انحصر في العلاقات بين الدول، غير أن مبدأ السيادة شهد في الفترات اللاحقة عدة تحولات وانتقل نحو النسبية نتيجة التحولات التي عرفها النظام الدولي⁽¹⁴⁾.

وللسيادة بعض الخصائص التي يمكن أن نحصرها فيما يلي⁽¹⁵⁾:

- **مطلقة:** إذ لا توجد سلطة فوقها لسن القوانين أي أنها هي السلطة العليا؛
- **الشمولية:** لأنها تطبق على كافة المواطنين في الدولة ورعاياها وكذلك على المنظمات المتواجدة داخل حدودها الإقليمية مهما كانت صفة هذه المنظمة؛
- **عدم التنازل:** لا يمكن لأي دولة التنازل عن سيادتها، فالدولة والسيادة متلازمان ومتكاملتان؛
- **الديمومة:** أي أن السيادة قائمة مادامت الدولة موجودة، بغض النظر عن تغيير الأشخاص الممارسين لهذه السلطة، أي أن السيادة مرتبطة بدوام قيام الدولة وليست الأشخاص الممارسين لها، وهذا يعني أن توقف السيادة يعني زوال الدولة واختفائها؛
- **عدم قابلية التجزئة:** السيادة تتضمن عدم المشاركة والتقسيم، حيث لا يمكن أن توجد أكثر من سيادة واحدة في الدولة.

علما أن كل من العولمة والتطور الكبير في الفضاء الرقمي فرضا إعادة التفكير في مفهوم السيادة الوطنية والأمن القومي (أمن الدول) بمختلف أبعاده، حيث أصبح لكل بعد محتوى ومجالا أمنيا قوميا لأي دولة في العالم، جانبا معلوماتيا ورقميا يجب الحفاظ عليه، كما أن الأمن الرقمي (السيبراني) أصبح يغطي جميع المجالات العسكرية، الاقتصادية، الاجتماعية، الثقافية، الإنسانية والسياسية، ويعمل على تحقيق منظومة أمنية متكاملة هدفها الحفاظ على الأمن القومي للدولة من كافة التهديدات التي يمكن أن تطالها من الفضاء السيبراني.

يشير بعض المختصين إلى أن مفهوم السيادة الرقمية ظهر مع نهاية العقد الأول من القرن الواحد والعشرين ويقصد به «قدرة الدولة على تنظيم الفضاء السيبراني»⁽¹⁶⁾ والذي ارتبط بشكل مباشر بالفضاء السيبراني الذي هو مفهوم مشتق من مصطلح الأمن السيبراني

الأكثر شيوعاً والذي يتعلق بحماية البنية التحتية والعمليات المتصلة بالإنترنت، وهو مفهوم غامض يعرف جدلاً كبيراً بين الأكاديميين وحتى السياسيين. وبشكل عام يستخدم المصطلح في الأغلب للتعبير عن قوة الدولة واستقلالها في الفضاء السيبراني، بهدف وصف أشكال مختلفة من الاستقلالية والتحكم والسيطرة على البنى التحتية الرقمية والتقنيات والمحتويات الرقمية والاتصالات، وكل الأشياء التي ترتبط بالفضاء السيبراني والتعامل معه⁽¹⁷⁾.

2. أبعاد الأمن السيبراني

يمكن تعريف الأمن السيبراني بأنه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات، والأجهزة المتصلة بالإنترنت، وبذلك فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها أو الالتزام بها لمواجهة التهديدات أو للحد من آثارها في أسوأ الأحوال⁽¹⁸⁾.

تتمثل أبعاد الأمن السيبراني فيما يلي⁽¹⁹⁾:

- **البعد العسكري للأمن القومي:** يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر شبكات الاتصال العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها، علماً أن المحتوى المعلوماتي الرقمي العسكري يعد من أكثر الأبعاد تأثيراً على الأمن القومي، وذلك يرجع لحساسية ما يحتويه من معلومات وبيانات رقمية تتعلق بالجانب التنظيمي العسكري البري والجوي والبحري وتسليح الدولة. لذلك فإن أغلب المعدات ومنظومات الأسلحة تعمل حالياً من خلال ربطها بوسائل الاتصال الحديثة وشبكات الإنترنت، وقواعد البيانات وأنظمة المعلومات، والتي تمكن مستخدميها التحكم بها عن بعد؛
- **البعد السياسي للأمن القومي:** يتمثل في المعلومات والبيانات الرقمية التي تخص الدولة وأجهزتها السيادية التي تحوز معلومات حساسة قد تنتج عنها مشاكل كبيرة إذا تم اختراقها أو العبث بها، الأمر الذي من شأنه زعزعة ثقة الشعب بمؤسسات الدولة، وبرز ذلك من خلال فكرة «إسقاط النظام من الداخل» بدلاً من استخدام القوة العسكرية الخارجية؛
- **البعد الاقتصادي للأمن القومي:** يعتبر من أكثر القطاعات القومية عرضة للهجمات الإلكترونية، حيث أصبحت الإنترنت أساساً للمعاملات التجارية والمالية، كما تستخدم الحواسيب والرقمنة على نطاق واسع في الاقتصاد، من حيث التسيير والتطوير والتسويق والتحكم في الاقتصاد ككل؛ لقد أصبحت أغلب النشاطات التجارية مرتبطة بشبكات الحاسب الآلي، خاصة مع التحول إلى الاقتصاد القائم على المعرفة والتي أصبحت فيه المحرك الأساسي للإنتاج والنمو، لبناء اقتصاديات الدول والتطور والنهوض بها من

أجل تنمية مستدامة تحقق الرفاهية بمختلف أبعادها، وهذا ما نتج عنه تسابق الدول للاستثمار في المعرفة والحصول عليها، وبذلك أصبحت عصنة الاقتصاد مرتبطة بشكل وثيق بالتحكم في الاقتصاد الرقمي من طرف الفاعلين الاقتصاديين والاجتماعيين، ونتج عن هذا التطور الرقمي ضرورة ملحة لتوفير الأمن السيبراني لضمان حماية المعلومات والبيانات؛

- **البعد الاجتماعي والثقافي للأمن القومي:** إن التدفق الكبير والحر للمعلومات عبر الفضاء السيبراني أصبح سلاحا قويا في يد الفواعل المختلفة، ومن خلاله يمكن التأثير على أفراد المجتمع وثقافتهم وعاداتهم سواء في الدول المتقدمة أو النامية، غير أن هذه الأخيرة هي الأكثر استهدافا، نظرا لتأثر أغلب أفراد المجتمعات النامية بالمجتمعات المتطورة، مما قد ينتج عنه طمس واضمحلال للهوية والثقافة الأصلية للمجتمعات المخترقة؛

- **البعد القانوني:** إن التطورات التكنولوجية الكبيرة والمتسارعة التي شهدتها العالم أصبحت تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات توصف الأعمال القانونية وغير القانونية في الفضاء السيبراني، غير أن العديد من الدول تفتقد للأطر القانونية الصارمة للتعامل مع الجريمة السيبرانية، كما أنه من الضروري تفعيل التعاون الدولي المشترك لمكافحتها.

رابعاً- الاختراقات الرقمية والفئات المستهدفة منها

عملية القرصنة لا تستثني أي أحد في العالم، فكل شخص متصل بشبكة الانترنت قد يكون معرضا للاختراق، خاصة وأن الكثير من مستخدمي هذه الشبكة يجهلون مصادر المعلومات والمواقع الالكترونية التي تحمل فيروسات أو برمجيات خبيثة من مختلف الأنواع والتي أحيانا تدمر أنظمة الأجهزة الالكترونية بشكل كامل مما يتسبب في فقدان كل المعطيات المخزنة في القرص الصلب، وبالتالي إعادة تثبيت نظام تشغيل جديد على الجهاز.

1. إختراق حسابات الأفراد خلال جائحة كوفيد-19

تعرف فترة جائحة كوفيد-19 انتعاشا لنشاطات ما يعرف بالهاكر الذين استطاعوا اختراق العديد من الحسابات الشخصية للأفراد بسبب الحجر الصحي الذي فرض على المواطنين البقاء في بيوتهم وبالتالي وجدوا متنفسا عبر مختلف مواقع التواصل الاجتماعي، وفي نفس الوقت كانوا فريسة لبعض البرامج والتطبيقات التي أثرت على عقولهم وسهولة التلاعب بهم واستدراجهم قصد قرصنة بياناتهم.

«الاختراق الأمني هو أي حادث ينتج عنه وصول غير مصرح به إلى بيانات الكمبيوتر

أو التطبيقات أو الشبكات أو الأجهزة، كما ينتج عنه الوصول إلى المعلومات دون إذن، ويحدث عادة عندما يتمكن المتسلل من تجاوز آليات الأمان»⁽²⁰⁾.

لقد شهد العالم زيادة كبيرة في هجمات التصيد الإلكتروني Phishing وتحديدًا خلال الثلاثي الأول من سنة 2020 وهي الفترة التي عرفت انتشار الموجة الأولى من فيروس كورونا⁽²¹⁾، حيث حذرت منظمة الصحة العالمية من البريد الإلكتروني الذي كان يستهدف الإيطاليين، والذي يتضمن ملفات يزعم الهاكر أنها تحتوي على أسماء أدوية تستخدم لعلاج كورونا، لكن هذه الملفات تحتوي على برمجيات ضارة، إذ بمجرد تحميلها على جهاز الكمبيوتر يتم اختراق الجهاز من قبل القرصنة. وعلى سبيل المثال، فقد ازداد اعتماد نظم الرعاية الصحية على الرقمنة والاتصال بالإنترنت خلال فترة جائحة كوفيد-19، ولكن هذه النظم تفتقر إلى الحماية في غالب الأحيان، ولذلك فهي معرضة بشكل خاص للهجمات السيبرانية، حيث ينفذ قرصنة الإنترنت عن طريق برمجيات الفدية هجمات ضد المستشفيات والمراكز الطبية والمخابر والتي طغت عليها الأزمة الصحية وأصبحت غير قادرة على تحمل تكاليف الخلل الذي يصيب أنظمتها بسبب الفيروسات وهو ما يجعلها تستسلم وتدفع الفدية.

وتعد البيانات التي تم جمعها من قبل مركز الإبلاغ الخاص بمجموعة عمل مكافحة التصيد Anti-Phishing Working Group (APWG) والتي تأسست في الولايات المتحدة الأمريكية سنة 2003 مثالا جيدا عن الدور الذي تقوم به في مجال التحقيق حول الجرائم الرقمية، حيث تقوم بالإبلاغ عن الروابط URL الاحتيالية لمطوري شبكة الإنترنت وشركات برامج مكافحة الفيروسات، وتقوم بإعادة توجيهها إلى صفحة خاصة تتيح للأشخاص معرفة أنهم وقعوا ضحية لمحاولة تصيد احتيالي ومن ثم تحذيرهم قصد أخذ احتياطات الأمان خلال تصفحهم في شبكة الإنترنت⁽²²⁾.

كما شهدت السنوات الأخيرة، انتشار فيروس الفدية Ransomware والذي يعتبر من أكثر أنواع الاختراقات انتشارا وأخطرها، والتي برمجت لاختراق الأجهزة الإلكترونية المختلفة والمتصلة بشبكة الانترنت، حيث تقوم بنشر الفيروسات وذلك بعد استغلال الثغرات الأمنية في النظام، ثم تقوم بتشفير الملفات داخل الجهاز ومن ثم يقوم الهاكر بطلب مبالغ مالية من الضحية مقابل حصوله على مفتاح فك الشفرة، والذي يكون أحيانا غير موجود أي لا توجد ضمانات لإعادة البيانات. إن هذا النوع من الفيروسات لا يستهدف الأشخاص فقط، بل حتى الشركات العمومية والخاصة والحكومات والمنظمات الحكومية وغير الحكومية والتي تكبدت خسائر كبيرة في أنظمة معلوماتها، وهذا بالرغم من وجود مضادات للحماية من الفيروسات، حيث يقوم هؤلاء القرصنة بتطوير فيروسات جديدة في كل مرة بعد اكتشاف مضاد للفيروس السابق.

وبما أن كل مستخدم شبكة التواصل الاجتماعي لديهم حسابات بريدية، فإن

القرصنة لديهم حيل عديدة من بينها رسائل البريد العشوائي، وذلك من خلال خداع المستخدمين الذين يقومون بالنقر على الروابط المجهولة والتي تقوم بعد ذلك بتنزيل البرامج الضارة على أجهزة الكمبيوتر أو الأجهزة المحمولة الخاصة بهم⁽²³⁾.

2. قرصنة بيانات المؤسسات الاقتصادية

مع ظهور وانتشار فيروس كورونا المستجد والذي تحول إلى جائحة بعد انتشارها في أغلب دول العالم، اضطرت العديد من الشركات الاقتصادية إلى تغيير نمط عملها بعد قيام الدول بغلق كلي أو جزئي لمختلف المؤسسات الاقتصادية وتحولها إلى العمل عن بعد أو بالاقتصاد الرقمي. ومن أجل تفادي الخسائر المادية، بدأت العديد من الشركات العالمية على غرار فيسبوك وغوغل ومايكروسوفت، بإدخال تعديلات من أجل السماح لأكثر عدد من المشتركين بالاستفادة من خدماتها عن بعد. وكاستجابة لمتطلبات مرحلة تفشي جائحة كورونا، قامت عدد من الشركات الاقتصادية العالمية التوجه نحو الرقمنة بإجراء تحسينات على خدماتها الرقمية لتفادي خسارة زبائنها وبالتالي إفلاسها⁽²⁴⁾.

ولكن الفضاء الرقمي لا يخلو من المخاطر، حيث يقوم القرصنة الإلكترونيون باختراق بيانات الشركات وتشفيرها، ثم يطلب القرصنة بعد ذلك مبالغ مالية ضخمة من هذه الشركات مقابل استرجاع البيانات مرة أخرى، ولكن أحيانا نجد بعض القرصنة يعملون لصالح الشركات المنافسة.

لقد تسببت القرصنة الإلكترونية في زيادة التوتر بين العديد من الدول، على غرار الشركة الاقتصادية العملاقة في مجال الهواتف النقالة هواوي الصينية، والتي تسببت في توتر العلاقات التجارية والسياسية بين الصين والولايات المتحدة الأمريكية بسبب اتهام هذه الأخيرة للصين بقرصنة أعمالها ووضع برمجيات التجسس داخل هواتفها النقالة الذكية المنتشرة عبر العالم، وهو ما لم تتقبله الصين والتي وجهت نفس التهمة لأمريكا؛ للإشارة، فإن القرصنة لا تقتصر على الشركات الصغيرة وإنما حتى الشركات الكبرى لم تسلم من عملية القرصنة، حيث تعرضت شركات عالمية كبرى للاختراق خلال السنوات الأخيرة من بينها⁽²⁵⁾:

- شركة (CVS Health) المختصة في الرعاية الصحية الأمريكية والتي تمتلك صيدليات منتشرة في جميع أنحاء الولايات المتحدة الأمريكية، تعرضت سنة 2015 لاختراق موقعها الإلكتروني مما تسبب في اختراق بيانات البطاقات الائتمانية لآلاف العملاء؛
- شركة آبل (Apple) تعرضت هي بدورها للاختراق رغم أن الشركة محصنة وتمتلك أقوى مضادات للحماية من الفيروسات والقرصنة. ولكن من قام بعملية الاختراق هو مراهق أسترالي يبلغ من العمر 16 عاما فقط، والذي استطاع اختراق خوادم الشركة وقام بنسخ حوالي 100 جيجابايت من البيانات؛

التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية:
القرصنة الإلكترونية نموذجاً

- شركة إكسون موبيل الأمريكية (Exxon Mobil) التي اتهمت قراصنة من الصين بسرقة بيانات مهمة منها، وقد تبين في وقت لاحق أنها كانت من بين الشركات المتضررة من هذه الهجمات التي أطلق عليها اسم عملية «التنين الليلي»؛
- رويال داتش شل (Royal Dutch Shell)، التي تم اختراق بياناتها سنة 2011، حيث قام نفس القراصنة الذين اخترقوا شركة إكسون موبيل من خلال هجمات «التنين الليلي»، باختراق هذه الشركة النفطية متعددة الجنسيات (بريطانية - هولندية) وسرقوا معلومات مهمة منها؛
- تشاينا ناشيونال بتروليم (China National Petroleum) تعرضت شركة الطاقة الصينية لهجوم إلكتروني في سنة 2017، وهو ما أثر على أكثر من عشرون ألف محطة وقود في الصين، حيث لم تعد المحطات قادرة على قبول البطاقات الائتمانية للعملاء، وتعرضت الشركة للهجوم بواسطة أحد برامج الفدية يدعى (WannaCry)، ويقوم القراصنة من خلال هذه البرامج بإغلاق أنظمة الشركة وتعطيلها، ثم يطلبون فدية ضخمة من عملة البيتكوين لإعادة تشغيل هذه الأنظمة؛
- شركة بي بي (BP)، تعرضت شركة الطاقة البريطانية لهجمة إلكترونية على بوابة التوظيف الخاصة بها عام 2018، مما تسبب في اختراق بيانات أكثر من 60 ألف شخص، كانوا قد تقدموا بطلب للحصول على وظائف منذ عام 2008، وتمت سرقة بيانات شخصية خاصة بالمتقدمين للوظائف؛
- شركة تويوتا (Toyota) اليابانية والتي تعتبر رائدة في مجال صناعة السيارات، تعرضت هي أيضاً لعدة هجمات إلكترونية، وكانت أكبر عملية اختراق تعرضت لها الشركة في سنة 2019، حيث تم اختراق المعلومات الشخصية لـ 3.1 مليون من عملاء الشركة.

3. تهديد أمن ورموز الدولة

إن التهديدات الناتجة عن التجسس وقرصنة المعلومات لا تتوقف عند المؤسسات الاقتصادية أو قرصنة المعلومات الشخصية للمواطنين، وإنما تتجاوز ذلك من خلال كشف أسرار أمن الدول واختراق مواقع المؤسسات الحكومية والبريد الإلكتروني لرؤساء بعض دول العالم. فقد شهد هذا الأخير في العشر سنوات الأخيرة تسريبات غير مسبقة تتسم بالطابع السري وبأدق التفاصيل حول شخصيات دولية مستهدفة قصد الإطاحة بها أو خلق مشاكل واضطرابات داخل الدول التي ينتمون إليها. ومن بين المواقع التي سربت هذه المعلومات نجد موقع ويكيليكس لصاحبه الأسترالي "جوليان بول أسانج" (Julian Paul Assange) والذي قدم معلومات في غاية من السرية لوسائل الإعلام الدولية، ما تسبب في أزمات دبلوماسية واضطرابات في العلاقات الدولية بسبب الاتهامات بين العديد من الفاعلين الدوليين⁽²⁶⁾.

في هذا السياق، صرح مدير اليوروبول⁽²⁷⁾ (Europol) السيد "Rob Wainwright" بأن الجرائم الإلكترونية ارتفعت خلال سنة 2015 إلى نفس مرتبة الإرهاب من حيث التهديد للأمن القومي، وهو ما يسلط الضوء على المخاوف المشتركة فيما يتعلق بهذا الشكل من الجرائم⁽²⁸⁾، كما أصبحت سياسة التدخل في الشؤون الداخلية للدول ميزة أساسية في العلاقات الدولية، ولكن هذه المرة في الفضاء الرقمي والذي يعد انتهاكا لسيادتها الرقمية.

فالصينيون كقوة عظمى يرون أن الولايات المتحدة الأمريكية تهدد مصالحهم في هذا الفضاء، وأنها تتدخل في شؤونها الداخلية، حيث وجهت انتقادات لأمريكا بسبب اتهامها لها بالتجسس على خصوصية الأفراد. وفي هذا السياق، صرحت الصين بأنها تؤيد حق الدول في الرقابة على المعلومات الخاصة بالأفراد داخل حدودها لأنه يدخل ضمن نطاق سيادتها الرقمية⁽²⁹⁾.

لقد أصبحت التهديدات الناجمة عن الفضاء السيبراني تشكل تهديدا مباشرا للسيادة الرقمية للدول، التي يجب أن تتجنبها وتتصدى لها؛ وعليه أصبح أمن الدول نسبيا في عصر العولمة وفي الفضاء الرقمي، فهو ولا يعتمد على الجيوش والترسانة العسكرية فحسب بل يتعداه إلى الحفاظ على أمنها الرقمي (بالحفاظ على بياناتها ومعلوماتها الرقمية السرية والهامة) وتفادي التهديدات عبر الفضاء الرقمي والتصدي لها. وكمثال على اختراق الأمن القومي العسكري، نجد اختراق أنظمة المنشآت النووية بإيران وتعطيلها عن العمل في سنة 2010، والذي تم من خلال فيروس يعتبر الأقوى والأكثر قدرة على الاختراق وهو الفيروس الصهيوني (stuxnet)، والذي استهدف بشكل مباشر أنظمة التحكم الصناعية في المفاعلات النووية الإيرانية⁽³⁰⁾.

ولمواجهة مختلف التهديدات الرقمية، تسعى الدول للوصول إلى الحد الأقصى من الأمن، للحفاظ على حدودها واقتصادها وحتى هويتها، وذلك بتبني أحدث التكنولوجيات وتطويرها ووضع استراتيجيات تجعلها في موقع القوة وليس الضعف، وبذلك أصبحت أي دولة مجبرة على أن تراعي العناصر التالية بالنسبة لأمنها الوطني⁽³¹⁾:

- النسبية: يعتبر الأمن عاملا نسبيا، والدولة لا تكون دوما قادرة على تحقيقه دون اللجوء للتعاون الدولي؛
- المرونة: والتي من خلالها يمكن للدولة مواكبة التحولات المستقبلية؛
- وضوح مصدر التهديد: إن معرفة مصدر التهديد والتحدي، أو معرفة العدو، في الحاضر والمستقبل أمر ضروري لبناء إستراتيجية واضحة وفعالة؛
- التحكم الجيد والاستثمار في عوامل القوة على اختلاف أنواعها وأهدافها؛

في حال مراعاة الدولة لهذه العناصر تصبح مواكبة لكل التحولات والمستجدات الحاصلة، وبذلك تحقيق حماية أفضل وأنجع.

الخاتمة

من خلال ما سبق يمكن القول أن القرصنة الإلكترونية التي تصنف ضمن الجريمة السيبرانية بدأت تأخذ حيزا متزايدا في النقاش العام المثار من قبل معظم الخبراء ووسائل الإعلام في ظل عالم يعرف استعمالا مكثفا للأجهزة الرقمية ووسائل التواصل الاجتماعي، حيث لم تعد ظاهرة القرصنة الإلكترونية مقتصرة على الأعمال المنعزلة ولكنها الآن تشكل خطرا أمنيا كبيرا على الأفراد والشركات والدول.

وبما أننا اليوم نعيش في عالم يتسم بالرقمنة في مختلف جوانب الحياة السياسية والاقتصادية والاجتماعية وحتى الأمنية كون الكثير منها مرتبط بشبكة الانترنت، وهو ما يطرح التساؤل حول الإجراءات الواجب اتخاذها لمواجهة الجرائم الإلكترونية الناجمة عن القرصنة، وعليه فإن الاهتمام بإدراج هذه المخاطر في المناهج التعليمية يعد من الأولويات قصد توعية أفراد المجتمع منذ التنشئة الأولى، وذلك بضرورة أخذ الحيطة والحذر خلال تصفح مواقع الانترنت لاسيما مجهولة المصدر، ولكن هذا لا يكون كافيا إلا إذا تم تدعيم المنظومة الرقمية للدولة بأجهزة حماية ورقابة مستمرة لمواجهة أي تهديد قد يمس بأمنها وسيادتها، وأيضا تعزيز التعاون الدولي في مجال تبادل المعلومات حول مختلف التهديدات المتوقعة.

أما بالنسبة للاقتصاد الرقمي فاستهدافه يعني إلحاق الضرر بالدولة خاصة وأن التجارة الدولية والمعاملات المالية تسير نحو الرقمنة والتي أغلبها مرتبط بشبكة الانترنت، حيث يترتب من خلالها القرصنة ضحاياهم وذلك حسب الأهداف المراد تحقيقها■

الهوامش

- 1- رابحي عزيزة، «الأسرار المعلوماتية وحمايتها الجزائية»، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد - تلمسان، 2017-2018، ص 182.
- 2- ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة، دار الآن ناشرون وموزعون، عمان، 2021، ص 26.
- 3- نفس المرجع، ص 27.
- 4- الجريدة الرسمية للجمهورية الجزائرية، قوانين، العدد 47، 25 شعبان عام 1430 هـ الموافق 16 غشت سنة 2009، ص 26.
- 5- نعيم سعيداني، «آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري»، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013، ص 47.
- 6- منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص 11.

- 7- أحمد بطو، «ما هو الهكر hacker وما أنواع الهكر؟»، تم التصفح يوم 07 جانفي 2021. أنظر في الموقع: <https://cyberone.co/ma-هو-الهكر-Hacker/>
- 8- سعيد بن دنيدينة و عامر بوعكاز، «سبل ووسائل حماية المستهلك الالكتروني من مخاطر الاقتصاد الرقمي»، مجلة البناء الاقتصادي، العدد 01، جوان 2018، ص 74.
- 9- أحمد بطو، مرجع سبق ذكره.
- 10- Gregoire GERMAIN et Paul MASSART, «Souveraineté numérique», in : Etudes, octobre 2017, pp20-52.
- 11- إسماعيل زروقة، «الفضاء السيبراني والتحول في مفاهيم القوة والصراع»، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، أبريل 2019، ص 1023.
- 12- أسامة الدليل، «السيادة الرقمية تعيد تشكيل العالم»، بوابة الأهرام، 13 جانفي 2021، أنظر في الموقع: <https://gate.ahram.org.eg/News/2558833.aspx>
- 13- دلال مولاي ملياني، «الإنترنت والسيادة»، مجلة الدراسات الحقوقية، المجلد 07، العدد 01، مارس 2020، ص 398.
- 14- فرحات علاء الدين، عمروس عمارة، «الفضاء السيبراني وتآكل مفهوم السيادة الوطنية»، المجلة الجزائرية للدراسات السياسية، المجلد 08، العدد 02، 2021، ص 172.
- 15- جمال بن مرار، «مفهوم السيادة الوطنية في ظل العولمة»، مجلة مدارات سياسية، المجلد 1، العدد 2، سبتمبر 2017، ص ص 22-23 (بتصرف).
- 16- Martin UNTERSINGER, «L'incertaine mais nécessaire: souveraineté numérique», le Monde, du 20 novembre 2019. In : https://www.lemonde.fr/idees/article/2019/11/20/l-incertaine-mais-necessaire-souverainete-numerique_6019810_3232.html
- 17- فاطمة بيرم، «السيادة الوطنية في ظل الفضاء السيبراني والتحويلات الرقمية: الصين نموذجا»، المجلة الجزائرية للأمن الإنساني، المجلد 05، العدد 01، جانفي 2020، ص 799.
- 18- منى الأشقر جبور، مرجع سبق ذكره، ص 25.
- 19- استعنا بالمراجع التالية: فاطمة بيرم، مرجع سبق ذكره، ص ص 796-798 (بتصرف).
- إسماعيل زروقة، مرجع سبق ذكره، ص ص 1022-1023.
- 20- <https://me.kaspersky.com/resource-center/threats/what-is-a-security-breach>
- 21- ظهرت أول حالة مصابة بفيروس كورونا المستجد (كوفيد-19)، مسجلة رسميا في الصين في ديسمبر 2019،

التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نموذجا

وتم ربطها بسوق هوانان للمأكولات البحرية بمدينة ووهان، غير أن مصدر الداء لازال مختلفا فيه، حيث يرجح مصدره إلى الخفافيش وربما تم تطويره في المخابر.

أنظر في الموقع:

/دراسة-أول-حالة-كورونا-ربما-ظهرت-بالصين-في-أكتوبر2019- / <https://arabic.rt.com/health/1245528>

22- Bilel BENBOUZID et Daniel VENTRE, « Pour une sociologie du crime en ligne Hackers malveillants, cybervictimations, traces du web et reconfigurations du policing », Réseaux, n° 197-198, 2016/3, p20.

23- Interpol, « Cybermenaces liées au COVID-19 », consulté le 07 janvier 2022. URL : <https://www.interpol.int/fr/Infractions/Cybercriminalite/Cybermenaces-liees-au-COVID-19>

24- سفيان قعلول و الوليد طلحة، «الاقتصاد الرقمي في الدول العربية: الواقع والتحديات»، صندوق النقد العربي، أبو ظبي، أكتوبر 2020، ص ص 21-22.

25- «أكبر الشركات العالمية التي تعرضت للقرصنة»، السعودية، 31 جانفي 2021 (بتصرف). أنظر في الموقع: <https://www.argaam.com/ar/article/articledetail/id/1438872>

26- فؤاد صباغ، «الاقتصاد الرقمي والعلاقات الدولية: الإيجابيات والسلبيات»، 2019. أنظر في الموقع: <https://www.almayadeen.net/articles/blog/956039-والسلبيات-و-الإيجابيات-الدولية-والعلاقات-الدولية>

27- يوروبول هي وكالة تطبيق القانون الأوروبية، وظيفتها حفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوروبي في مجالات مكافحة الجرائم الدولية الكبيرة والإرهاب.

28- Anne-Marie COTE, Maxime BERUBE, Benoit DUPONT, « Statistiques et menaces numériques : Comment les organisations de sécurité quantifient la cybercriminalité », Réseaux, n° 197-198, 2016/3-4, p205.

29- سكوت وارين هارولد، ومارتن سي لبيكي وأستريد ستوث سيفالوس، «التوصل إلى اتفاق مع الصين بشأن الفضاء الالكتروني»، RAND Corp، كاليفورنيا، 2016، ص 09.

30- Gregoire GERMAIN et Paul MASSART, op.cit, p45.

31- فرحات علاء الدين، عمروس عمارة، مرجع سبق ذكره، ص171.