# وسائل التواصل الرقمي وخداعها للجمهور المستهلك

د. حافظ لصفر

دكتوراه في علم النفس الاجتماعي

كثيرة هي الصفحات والمواقع الرقمية التي تخدع الجمهور بوضع روابط أو رموز مغرية لهم، فبمجرد الضغط عليها، يصبح مراقبا ومتجسسا عليه، فيتم السطو على أمواله، وأحيانا ممتلكاته وبياناته ومعلوماته الشخصية، فشبكات التواصل الاجتماعي، كنظام معلومات عالمي متصل ببعضه اعتمادا على برتوكول الانترنيت وتوابعه الفرعية، أي عبارة عن شبكات اتصال عالمية[1].

إنه عالم افتراضي تقني يعمل على بروتوكولات لنقل المعلومات، ويمهد للاتصال من خلال عناوين خاصة وأجهزة إلكترونية دقيقة، ومن أجل الإشاعة والدعاية لعملة رقمية معينة، فروادها ومستخدموها يلجؤون لمنصات إلكترونية عالمية، ولاستعمال مختلف شبكات التواصل الرقمي لجلب عملاء جدد للتعامل بالعملات الرقمية، فهذه الشبكات الرقمية لها سلبياتها، حيث نجملها في النقط التالية:

– بث الإشاعات والدعاية المزيفة عوضًا الحقيقية حول سبل وطرق التعامل المالي مع العملات الرقمية.

– التحايل والابتزاز والتزوير والاستغلال غير المشروع لأموال الغير، سواء كان فردا أو مؤسسة اقتصادية.

– انتهاك الخصوصية والحقوق الخاصة والعامة للمؤسسات والشركات والمقاولات من أجل قرصنة تعاملاتها التجارية والمالية.

– المخاطرة والمقامرة برؤوس الأموال سواء بالنسبة للأشخاص أو الشركات والمقاولات الاقتصادية.

– السرقة للملكية الاقتصادية والتجارية والمالية للشركات غير المؤمنة إلكترونيا.

[1] إعداد مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، نزوى – سلطنة عمان، مسابقة جائزة الأمير نايف بن عبد العزيز لعام 2016، ص: ٤٧

– عدم السيطرة على استخدامات أجهزة تقنية المعلومات[1].

سهلت وسائل التواصل الرقمي عملية الإجرام الإلكتروني، واستغلال الصفحات والمنصات الإلكترونية لتمويه وخداع الجمهور المستهلك مستعملين طرق الاقناع والإفحام المبيتة وغير المشروعة لابتزازه وإيقاعه في فخاخ نصب وقرصنة المعلومات والأموال، ومن ثمَّ إفلاس أشخاص كثر بسبب قلة الخبرة والحيطة والحذر، وعدم استعمال تقنيات حمائية لحساباتهم وأرصدتهم البنكية، فهناك تطبيقات وبرمجيات فائقة الدقة، هي الكفيلة بحماية الأنظمة المالية والتجارية للأفراد والدول والمنظمات الحكومية وغير الحكومية.

## الجريمة الإلكترونية وآليات الحماية منها

تعرف الجريمة الإلكترونية على أنها كل مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي وبقصد الإساءة لسمعة الضحية، أو لجسدها أو عقلها بطريقة مباشرة أو غير مباشرة، ويتم ذلك باستخدام وسائل الاتصالات و التكنولوجيا الحديثة مثل: الإنترنت، غرف الدردشة، البريد الإلكتروني، وتشهد التقنية والتكنولوجيا تطورات كثيرة، واستحداثها لأمور جديدة، هذا الأمر ينذر بتطور أدوات وسبل الجريمة الإلكترونية بشكل أكثر تعقيدا، الأمر الذي يلزم الدول بتطوير آليات مكافحة هذه الجرائم واستحداث خطوط دفاع، وسن قوانين وتوعية الناس بمستجداتها، وتشجيعهم للإبلاغ عنها، ويهتم بدراستها علم الجناية الرقمية[2]، ومن أهم الطرق المستعملة في الجريمة الإلكترونية ما يلي:

– تخريب المعلومات وإساءة استخدامها.

– سرقة المعلومات، ويشمل بيع المعلومات، كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني، أو الصناعي، أو العسكري، أو الأمني.

– تزييف البيانات والمعلومات وتزويرها.

– انتهاك الخصوصية.

– التصنت والتجسس.

– التشهير.

– قرصنة البيانات.

---

[1] نفس المرجع السابق ص: ٥٥

[2] M Reith، C Carr، G Gunsch (2002)، "An examination of digital forensic models"، International Journal of Digital Evidence.

– خلاعة الأطفال.

– القنابل البريدية وإفشاء الأسرار.

– التنمر والتحرش الجنسي.

– الاحتيال المالي والإرهاب الإلكتروني.

– المطاردة والملاحقة والابتزاز.

– السرقة العلمية والأدبية[1].

**بعض اشكال الجرائم الناجمة عن التعامل بالعملات الرقمية والمشفرة**

أبلغت العديد من الحكومات عن تفاقم عمليات الاحتيال في العملات المشفرة بشكل كبير، حيث أجريت مجموعة من الأبحاث والدراسات عن أنواع الاحتيال في العملة المشفرة حديثا، وعما ستكون عليه مستقبلا، إضافة إلى تقديمها تعريف لهذه العمليات، وفسرت سبب تفاقمها بشكل كبير والخسائر الناتجة عنها، ومن بين الباحثين في هذا المجال، نجد الباحث "يلي هيومو"، ومجموعة من الباحثين الأخرين الذين قاموا بدراسة حول مجالات بلوك تشين،استهدفت ١٤ من أصل ٤١ دراسة فقط، والتي تناولت تحديات أمن بلوك تشين في عملة بتكوين، ورغم هذه الدراسات إلا أن هناك فقط منشوراً واحداً الذي أجري سنة ٢٠١٥، هو الذي كشف الاحتيال المرتبط بهذه الأنظمة، وهذا يشير إلى نقص البحث في هذه الأنظمة التي هدفها الخداع والتضليل في العملات المشفرة قصد تحقيق مكاسب مالية، وفي سنة ٢٠٠٨ نشر "ستوشي ناكا موتو" مقالاً بعنوان "بتكوين"، حيث اعتبره نظاما يُمكّن الأطراف من التعامل مباشرة، دون مؤسسات مالية وسيطة، ويعتمد "نظام بتكوين" على التشفير بدلاً من البنوك المركزية، كما أن إنشاءه أثار آلاف العملات المشفرة الأخرى التي تشترك في مبادئ وتقنيات مماثلة؛ حيث يبلغ إجمالي القيمة السوقية للعملات المشفرة ١.٦ تريليون دولار، وتشترك "البيتكوين"، والعملات المشفرة الأخرى في ثلاثة مبادئ مشتركة: اللامركزية، وإخفاء الهوية الزائفة، والشفافية، إذ أن "بتكوين" تستخدم

[1] دياب موسى البداينة، الملتقى العلمي بكلية العلوم العسكرية بالأردن، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية المنظمة بين 2-4 شتنبر لسنة 2014،ورقة علمية بعنوان الجرائم الالكترونية: المفهوم والأسباب، ص: 24-23

متجزئات المفاتيح العامة من أجل تحديد المستخدمين، وتشكيل نظام "إدارة الهوية اللامركزية" المنفصلة عن هويات العالم الحقيقي[1].

تعتبر العملات المشفرة مجهولة المصدر نسبيا بسبب الطبيعة الشفافة لمعاملاتها، حيت أبلغت الحكومات على الرغم من عدم كونها مرتبطة بشكل صريح بأفراد وشركات معينة في السنوات الأخيرة عن زيادة عمليات الاحتيال التي تنطوي على العملات المشفرة، كما كشفت عن أنواع الاحتيال في العملة المشفرة الموجودة حاليًا أو المتوقع وجودها في المستقبل، فيمكن للدول التي تود حماية اقتصاداتها من تكوين مهندسي بلوك تشين، ينشئون تطبيقات وبرامج ومنصات ومواقع إلكترونية مشفرة ومؤمنة باستخدام هذه التقنية، أو محللين ماليين على دراية بعمل العملات المشفرة، بحيث يمكنهم مساعدة العملاء على إجراء استثمارات أذكى في العملة الرقمية، أو خبراء تشفير يمكنهم تطوير خوارزميات وأنظمة أمان لتشفير المعلومات الحساسة مثل: حماية البيانات في الشؤون المالية والأمن القومي من الإرهاب السيبراني، ومعطيات وبيانات الجيوش وحمايتها من الاختراق والتجسس.

الاستثمار في العملات المشفرة والرقمية غير مستقرة بسبب الخسائر العالية نتيجة عمليات الاحتيال كالقرصنة والأخطاء على الرغم من أن عمليات التشفير الأساسي أمنة بشكل عام، إلا أن التعقيد التقني لاستخدام أصول التشفير وتخزينها يمكن أن يشكل خطرا على المتعاملين الجدد، بالإضافة إلى مخاطر السوق بسبب المضاربة، فيجب على المستثمرين فيها أن يحتاطوا من المخاطر التالية:

– مخاطر المستخدم: لا يمكن إلغاء معاملة عملة مشفرة بعد إرسالها بالفعل بسب العناوين غير المضبوطة أو كلمات المرور المفقودة[2].

– المخاطر التنظيمية: لايزال الوضع التنظيمي للعملات المشفرة غير واضح، مما يواجه صعوبات في بيعها لتقلبات أسعار السوق.

– مخاطر الطرف المقابل: يعتمد العديد من المستثمرين على البورصات أو أمناء حفظ أخرين لتخزين عملاتهم المشفرة.

[1] Arianna trozze, Josh kamps, Eray Arda Acartuna , Cryptocurrencies and future financial crime ,Trozze et al.crime science,2022,p 4-10

[2] Jake frankefield,cryptocurrency explained with pros and cons for investement,updated february 04,2023.

– مخاطر الإدارة: هناك ممارسات تصدر عن ممارسات الإدارة المخادع وغير الأخلاقية لقلة الحماية المقدمة في شكل لوائح متماسكة.

– مخاطر البرمجة: تستعمل منصات التجارة والاستثمار والإقراض عقودا ذكية آلية للتحكم في حركية الودائع، فأي خطأ أو استغلال في هذه البرمجيات قد يتسبب في فقدانه لاستثماراته.

– التلاعب بالسوق: التصرفات اللا أخلاقية تشكل خطرا على رؤوس الأموال وفي أسعار المنتوجات المعروضة افتراضيا، وسيطرة المضاربات مما يسبب كسادا ومراكمة ثروات ضخمة من لدن فئة قليلة وإمكانية الترويج لعملات مشفرة بطريقة احتيالية وإجراء مناورات للتلاعب السوقي من نوع الضخ والسحب.

– العملات المشفرة تستهلك الطاقة بسبب أنشطة التعدين المتزايدة.

– خطر الانكماش والركود الاقتصادي والتضخم بسبب الخلق النقدي عير الكافي أو المفرط.

– هناك جماعات ضغط قوية عالميا متمثلة في حكومة الظل العالمية تعارض استخدام العملات الافتراضية وتدافع عن أنظمة الدفع باستخدام العملات الممنوحة الرسمية للمناقصة القانونية.

– عدم وجود حد أدنى وأعلى لسقف التحويلات والاستثمارات والتبادلات.

## الاتفاقيات المبرمة لمواجهة الجريمة الإلكترونية في مجال العملات الرقمية

أوروبا:

أقرت اللجنة الأوروبية لمجلس وزرائها في دورتها ١٠٩ بتاريخ ٠٨ نوفمبر ٢٠٠١ حول "الجريمة الإلكترونية"، وانضمت إليها دول غير أعضاء ككندا وأمريكا واليابان وجنوب افريقيا، إجراءات وأهداف من بينها ما يلي:

– التدابير اللازم اتخاذها وطنيا على مستويات القانون الجنائي الموضوعي، وقانون أصول المحاكمات، والاختصاص القضائي.[1]

– تحقيق التوافق والانسجام بين عناصر الجرائم في القوانين الجنائية المحلية الأساسية والشروط المتصلة ذات الصلة في مجال الجريمة الإلكترونية.

[1] إعداد مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها،نزوى – سلطنة عمان، مسابقة جائزة الأمير نايف بن عبد العزيز لعام 2016، ص: 62-63

– إعداد نظام فعال وسريع للتعاون الدولي

– تزويد قوانين الإجراءات الجنائية المحلية بصلاحيات ضرورية للتحقيق وتوجيه الاتهام في الجرائم الالكترونية، وغيرها من الجرائم التي ترتكب باستخدام أنظمة الحاسب الآلي، والتعامل مع الأدلة ذات العلاقة بالطابع الإلكتروني.

دول الخليج:

المراكز الوطنية الخليجية لحماية الأمن السيبراني: فرق الاستجابة لطوارئ الحاسب الآلي، ففي الإمارات العربية المتحدة أنشأت هيئة تنظيم الاتصالات لتحسين مقاييس وممارسات أمن المعلومة وحماية البنية التحتية لتقنية المعلومات من اختراقات الانترنيت[1]، فالاستخدام الآمن للانترنيت أولته الدول المتقدمة عناية كبرى عن طريق إنشاء مراكز وتضمينه ضمن تخصصات بشعب علمية وبشعب العلوم الإنسانية والاجتماعية لارتباطه بظاهرة اجتماعية ارتبطت بالاستعمال لوسائل التواصل الرقمي واستغلال المواقع والتطبيقات لتخريب بنيات تحتية وأخرى اجتماعية الشيء الذي فرض على الدول سن إطارات تنظيمية لحماية معلومات الأشخاص والشركات والأجهزة الحساسة بالدولة مثل: قانون حماية البيانات والمعلومات الشخصية وعدم قرصنتها وسرقتها.

الهيئة الوطنية للأمن المعلوماتي السعودية:

عرف تنظيم هيئة الأمن السيبراني على أنه: "حماية الشبكات وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني، والأمن الرقمي ونحوها، ومن بين أهدافها ما يلي:

١– إعداد الاستراتيجية الوطنية للأمن السيبراني، والإشراف على تنفيذها، واقتراح تحديثها.

٢– وضع السياسات وآليات الحوكمة[2] والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها.

[1] الموقع الالكتروني لمركز الاستجابة لطوارئ الحاسب الآلي بدولة الامارات العربية المتحدة

[2] الحوكمة: تعني الحكامة والحاكمية، وهي: تدعيم مراقبة نشاط المؤسسة ومتابعة مستوى أداء القائمين عليها.

٣- تصنيف وتحديد البنى التحتية الحساسة والجهات المرتبطة بها، وتحديد القطاعات والجهات ذات الأولوية بالأمن السيبراني.

٤- وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها.

٥- إشعار الجهات المعنية بالمخاطر والتهديدات ذات العلاقة بالأمن السيبراني.

٦- وضع أطر الاستجابة للحوادث المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها.

٧- بناء مراكز العمليات الوطنية الخاصة بالأمن المعلوماتي بكافة أنواعها، بما في ذلك مراكز التحكم والسيطرة والاستطلاع والرصد وتبادل وتحليل المعلومات، وكذلك بناء مراكز العمليات القطاعية الخاصة بالأمن السيبراني، وبناء المنصات الرقمية ذات العلاقة، والإشراف عليها، وتشغيلها.

٨- القيام بالأنشطة والعمليات المتعلقة بالأمن المعلوماتي.

٩- تنظيم آلية مشاركة المعلومات والبيانات المرتبطة بالأمن السيبراني بين الجهات، والقطاعات المختلفة في المملكة، والإشراف على ذلك.

١٠- تقديم المساندة للجهات المختصة خلال البحث والتحقيق في الجرائم المتعلقة بالأمن السيبراني.

١١- وضع السياسات والمعايير الوطنية للتشفير، ومتابعة الالتزام بها، وتجديدها بما يناسب العصر ومواكبة تطوراته في المجال المعلوماتي.

١٢- وضع ما يلزم من معايير وضوابط للسماح والترخيص باستيراد وتصدير واستخدام الأجهزة والبرمجيات ذات الحساسية العالية للأمن الإلكتروني التي تحددها الهيئة، ومتابعة الالتزام بها، وتحديثها، وذلك دون إخلال بأي ضوابط معتمدة لدى الجهات الأخرى ذات العلاقة.

١٣- بناء القدرات الوطنية المتخصصة في مجالات الأمن المعلوماتي، والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها، وإعداد المعايير المهنية والأطر وبناء وتنفيذ المقاييس والاختبارات القياسية المهنية ذات العلاقة.

١٤- الترخيص بمزاولة الأفراد والمنظمات غير الحكومية للأنشطة والعمليات المتعلقة بالأمن المعلوماتي التي تحددها الهيئة.

١٥- التواصل مع الجهات المماثلة خارج المملكة والجهات الخاصة لتبادل الخبرات، وتأسيس آليات للتعاون والشراكة معها، وفقًا للإجراءات المتبعة.

١٦- تبادل الإنتاج التقني والمعرفي والبيانات والمعلومات مع الجهات المماثلة خارج المملكة.

١٧- تمثيل المملكة في المنظمات والهيئات واللجان والمجموعات الثنائية والإقليمية والدولية ذات الصلة، ومتابعة تنفيذ التزامات المملكة الدولية الخاصة بالأمن السيبراني.

١٨- رفع مستوى الوعي بالأمن المعلوماتي.

١٩- تحفيز نمو قطاع الأمن المعلوماتي في المملكة، وتشجيع الابتكار والتجديد والتحديث والاستثمار فيه.

٢٠- إجراء الدراسات والبحوث والتطوير وعمليات التصنيع، ونقل التقنية وتطويرها في الأمن الإلكتروني، وما يرتبط به من مجالات.

٢١- اقتراح آليات رفع كفاءة الإنفاق في مجالات الأمن المعلوماتي.

٢٢- تطوير مؤشرات قياس الأداء الخاصة بالأمن السيبراني، وإعداد التقارير الدورية حول حالة الأمن الإلكتروني في المملكة على المستويين الوطني والقطاعي.

٢٣- اقتراح إصدار وتعديل الأنظمة والقوانين والقرارات ذات الصلة بالأمن السيبراني[1].

إن حماية المواطنين والاقتصاد العالمي من إساءة استخدام العملات المشفَّرة وشتى الأصول الافتراضية مهَمة تتطلب من أجهزة إنفاذ القانون اتخاذ إجراءات منسقة ومستدامة بالتعاون الوثيق مع السلطات الحكومية والهيئات التنظيمية والقطاع الخاص. ولهذا السبب، يكتسي هذا النوع من الفعاليات العالمية المتعددة القطاعات أهمية بالغة لضمان الأمن العالمي، وينظم الفريق العامل المعني بمكافحة الجرائم المالية وإساءة استخدام العملات المشفَّرة هذا المؤتمر السنوي الذي يشكل مبادرة ثلاثية الأطراف أنشأها معهد بازل للحوكمة والإنتربول ويوروبول في عام ٢٠١٦، ومع استحداث إدارة جديدة لمكافحة الجرائم المالية في كانون الثاني/ يناير ٢٠٢٢، يسعى الإنتربول إلى تعزيز خدمات الدعم التي يوفرها لأجهزة الشرطة في بلدانه الأعضاء ال ١٩٥ من أجل النهوض بما تبذله من جهود على الصعيد الوطني للتصدي للجريمة المالية، ومن المنتظر أن ينمو سوق الأمن الإلكتروني لسنة ٢٠٢٤، بمعدل سنوي يبلغ ٢٢.٥٪، بالإضافة إلى نمو اقتصادي ملحوظ في هذا القطاع من ١١.٤ مليار دولار سنة ٢٠١٧، إلى ٢٢.١ مليار دولار بحلول سنة ٢٠٢٣، وعلى مستوى الدولة، تهدف جهود الأمن المعلوماتي للدول الخليجية بشكل أساسي

[1] الموقع الإلكتروني للهيئة الوطني للأمن السيبراني بالمملكة العربية السعودية.

إلى منع الهجمات عبر الإنترنت من إيران ووكلائها، فهي من أكثر القوى الإلكترونية تقدماً في المنطقة إلى جانب إسرائيل من خلال برامجها المعقدة والمتطورة كبيكاسوس، وتوفر هجماتها الإلكترونية وسيلة لإلحاق الضرر بالبنية التحتية الرئيسة لخصومها الإقليميين، بينما تدعي عدم مسؤوليتها عن تلك الهجمات، فالمصدر الرئيس للتوتر بين دول الخليج، هو تطوير إيران لقدراتها الهجومية الإلكترونية التي استخدمتها في السابق، ويبدو أنها على استعداد لتطويرها أكثر مستقبلاً، ومن مهام هذه البرامج المعلوماتية الإيرانية، هو التجسس والإرهاب السياسي والعسكري، حيث استهدفت تلك الهجمات الإلكترونية منذ سنة ٢٠١٨، وما بعده أهدافًا حكومية حساسة، بما في ذلك مراكز الشرطة ووزارات الخارجية وأجهزة المخابرات في جميع الدول الخليجية، وبمنطقة الشرق الأوسط برمتها، وكتب مايكل آيزنشتات، من معهد واشنطن لسياسة الشرق الأدنى، أن الهجمات الإلكترونية أصبحت السلاح المفضل لدى إيران لدرجة أن أدوات وآليات الحرب الإلكترونية، تطورت من مجرد تقنيات أقل تطوراً من الناحية التكنولوجية إلى ركيزة أساسية في تعزيز الأمن القومي الإيراني، وهذه الهجمات من طهران، قد يكون لها عواقب وخيمة على اقتصادات دول الخليج ومجتمعاتها، وبالتالي تمثل تهديداً أمنيا حقيقيا لهذه الدول، وفي أغسطس سنة ٢٠١٩، قامت إيران بهجمات إلكترونية منظمة ضد البنيات التحتية والأهداف الحكومية الحساسة في البحرين، بما في ذلك جهاز الأمن الوطني وهيئة الكهرباء والماء، وخلال هذه الفترة تحديداً، صدرت عن نورمان رول الضابط السابق بوكالة الاستخبارات المركزية الأمريكية، تحذيرات من أن مثل هذه الهجمات كانت "ذات طبيعة جديدة"، بينما علق كريستوفر كربس، المدير السابق لوكالة الأمن السيبراني وأمن البنية التحتية، التابعة لوزارة الأمن الداخلي الأمريكي، بأن إيران تهاجم أهدافًا في منطقة الشرق الأوسط لاختبار قدراتها ومدى استعدادها لشن حرب إلكترونية في الولايات المتحدة، مشيراً إلى أن لديها بعض المهندسين الروس الجيدين الذين يساعدونهم في هذا الصدد، وفي الواقع، هناك أيضًا احتمال مشاركة دول أخرى بصورة غير مباشرة في مثل هذه التهديدات السيبرانية التي تستهدف دول الخليج، ويقصد هنا إسرائيل، وكتب كل من "منز وفارمانفرمايان"، أن إيران "طورت برنامجها الهجومي المتكامل، والمتعدد المنصات للهجمات الإلكترونية بطريقة محلية؛ بسبب العقوبات الصارمة من الولايات المتحدة، فقد تلقت بعض المساعدة من روسيا والصين، لما يتمتعون به من خبرة، لا يستهان بها في تنفيذ الهجمات الإلكترونية ضد الغرب وحلفائه"، ولعل من أبرز الأمثلة

على ذلك، مساعدة بكين لإيران في تشكيل شبكة الإنترنت الوطنية الخاصة بها، والمعروفة باسم "شوما"، للعمل بشكل مستقل عن الويب أو الشبكة العالمية للإنترنت المستخدمة لدى الغرب، بالإضافة إلى تمكن القراصنة "الهاكرز" الروس من حرية الوصول إلى الخوادم الإيرانية، وذلك طواعية وبالتعاون مع إيران للقيام بحربهم الإلكترونية تحت المبررات الديماغوجية[1] والستار المناسبين، وبدا واضحًا تعرض أكثر من ٣٥ دولة للهجوم بهذه الطريقة، وكانت الأهداف الرئيسة لهذه الحرب السيبرانية متمركزة في الشرق الأوسط، ومن بينها جامعات ومؤسسات علمية[2]، بهدف ضرب بنياتها الحيوية، والتعرف على كيفية اختراق أنظمتها الأمنية والمعرفية والبحثية بكل سهولة، ومن الثابت أنّه حتى مع استمرار دول الخليج في تطوير دفاعاتها في مجال الأمن المعلوماتي وفي مجال الاستراتيجيات الوقائية، فإن الجهود والبرامج الخبيثة للمهاجمين المحتملين، ستزداد خطورتها حدة وضراوة على الحقول الحيوية جميعها، وأصبحت التقنية مكونًا أساسيًا للنجاح الاقتصادي والازدهار في النظام العالمي الجديد المبني على مراكمة الثروة والقوة والتوسع عبر مخططات إمبريالية بعيدة المدى، حيث مارست أمريكا تأثيرا حاسما في أحداث خطيرة [3]، فإن مخاطر الجرائم الإلكترونية باختلافها تزداد شراستها، وعلى العموم، فإنه لا توجد دولة في العالم تشك بأن عمليات التجسس والتخريب وهجمات الهندسة الاجتماعية، تمر بدون اكتشاف عبر شبكات الحاسوب..، لكن السؤال المطروح: هو كيف تتم معالجة التهديدات المتزايدة، وبأي سرعة ممكنة؟ علاوة على ذلك، فإنه في حالة دول الخليج، إذا لم تواجه التهديدات الأمنية الإلكترونية باستراتيجيات أمنية ومعلوماتية فائقة التطور، وبوعي جمعي وشامل، فمستقبل الاستثمار فيها سيتأثر، وستعاني اقتصاداتها، ونفس الشيء ينطبق على باقي البلاد العربية، لأن الهجمات الإلكترونية المحتملة ستزداد خطورة، وستركز على ارتكاب الجرائم المالية، وعمليات التجسس الاقتصادي والعسكري، وعلى الشركات الخليجية والعربية الكبرى، وستراقب الجيوش الخليجية والعربية للحيلولة دون امتلاكها لأسلحة استراتيجية رادعة للعدو انسجاما مع قول الله عز وجل جلاله "وأعدوا لهم ما استطعتم من قوة ومن رباط الخيل ترهبون به عدو الله وعدوكم " (الأنفال: ٦٠)، إضافة إلى التجسس على ترسانتها في مجال التسلح لإعداد خطط

[1] الديماغوجي: هو الشخص الذي يسعى لاجتذاب الناس إلى جانبه عن طريق الوعود الكاذبة والتملق وتشويه الحقائق باستعمال شتى فنون الكلام وضروبه.

[2] المصدر: مركز الخليج للدراسات الاستراتيجية.

[3] هنري كسنجر "النظام العالمي: تأملات حول طلائع الأمم ومسار التاريخ، ترجمة فاضل جتكر دار الكتاب العربي، بيروت-لبنان، طبعة ٢٠١٥ ص: ٢٣١

تدميرية أكثر تفوقا من الناحيتين الأمنية والعسكرية، كما ازدادت وتيرة العمليات الإرهابية بكل أشكالها المباشرة والخفية وعبر الوكلاء في إطار ما يسمى "بالحرب بالوكالة" التي عرفت أوجها في الشرق الأوسط، بداية القرن الواحد والعشرين ببروز الجماعات الإرهابية التي كونتها المخابرات الأمريكية والإسرائيلية لضرب المجتمعات العربية وتخريبها بلا هوادة، وكان ضحيتها بلدين عربيين هما: العراق وسوريا، فالصناعة الجيو– بوليتيكية الأمريكية ورديفتها إسرائيل، نجحت بمخططاتها في تدمير بنى هذه الدول التي عجزت عن حماية بنيتها الاستراتيجية، لانشغالها بالصراعات السياسية والمصالح الذاتية الضيقة لزعمائها.

**المراجع المعتمدة:**


– محمد جبريل إبراهيم، جريمة التعامل في العملات المشفرة أو النقود الرقمية: "دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، العدد ٧٩.

– جريدة عربي بوست، نشرت بتاريخ 10/02/2021

– خالد وليد محمود، "قراءة في مؤشر الأمن السيبراني لسنة 2021"، الجزيرة

– موقع دار الإفتاء المصرية: http://www.dar–alifta.org/ar/Viewstatement.aspx?sec=media&ID=5617

**بالإنجليزية**

– Jonathan Bignell, Post Modern culture, published in agrment with Edinburgh, university press lid 22,George square ,First published in India,2007, publshed by A Akcer books.

– Arianna trozze, Josh kamps, Eray Arda Acartuna, Cryptocurrencies and future financial crime ,Trozze et al. crime science,2022.

– Cryptos les transactions liées a des activités criminelles ont atteint un record en 2021publié par b6 médias 06/01/2022.

– WWW.CAPITAL.FR/CRYPTO/CRYPTOS–LES–TRANSACTIONS–LIéES–A–DES–Activités– CRIMINELLE


١.