تأثير الهجمات الإلكترونية على فاعلية النظام الإيكولوجي الرقمي

د. أيمن محمد إسماعيل

المقدمة:

أصبح الفضاء الإلكتروني فى القرن الحادي والعشرين؛ فى ظل نظام إيكولوجي (بيئي) رقمي ؛ محيط تفاعلي للاقتصاد الرقمي (تسوق وتجارة إلكترونية وخدمات تمويل وتبادل معلومات) ولحروب الجيل الرابع (هجمات ،مخاطر ؛ قرصنة وتجسس الكتروني) ؛ فقد أدى توسع الشبكة العنكبوتية العالمية وانتشار وتطور الأجهزة الرقمية المتصلة بهاإلىسهولة الوصول والتعامل معه بسرعة وبتكلفة قليلة من قبل أطراف متعددة (دول أو أفراد أو جماعات قد تأخذ شكلاً منظماً أو غير منظم؛ متكافئة أحياناً وغير متكافئة أحياناً أخرى؛ قد يحمل بعضها طابع العدائية حيناً أو التعاون حيناً أخر) ؛وهو الأمر الذي قد يؤثر على فاعلية النظام الايكولوجي الرقمي فى أداء دوره فى الاقتصادات الوطنية؛ وهو ما يستدعى الاستعداد دائماً بالاستراتيجيات والأساليب الوقائية للمواجهة السريعة الفعالة لبسط حماية الدول على فضاءها الإلكتروني والحد من المخاطر الالكترونية التي يواجها هذا النظام للمحافظة على معدلات مرتفعة للتنمية المستدامة الشاملة وتحقيق أهدافها القومية.

مشكلة البحث:

على الرغم من مساهمة النظام الايكولوجي الرقمي وتفاعله مع محيطه من أجهزة وبرمجيات وشخصيات طبيعية واعتبارية من خلال لغة افتراضية تجمع كل الشبكات الالكترونية داخل فضاء إلكتروني واحد، استهدافاً لجمع أكبر قدر من البيانات والمعلومات داخل نطاق واحد؛ وإجراء العديد من العمليات والصفقات فى زمن وجيز بتكلفة قليلة دون اعتراف بالحدود الجغرافية والاحجام المادية تأسيساً على أسس رياضية منطقية ؛إلا إنه يحمل فى طياته الكثير من المخاطر غير المتوقعة التي يصعب تحديدها على وجه اليقين ، والتي قد تصيب الأشخاص الطبيعية والاعتبارية فتؤدى إلى أعطال؛ تخريب؛ خداع ، احتيالأوتجسس إلكتروني ؛ ومن

ثم تتناول مشكلة البحث معالجة القضايا التي تتعلق بهذا النظام الإيكولوجي (البيئي) الرقمي بتناول ابعاده المختلفة ورصد أهم تغيراته ومستجداته لتوفير استجاباتفاعلةللحد من آثارها السلبية؛ خاصة وأن زيادة انتشارالتقنيات الحديثة وتكنولوجيا المعلومات وتنوع مصادر التمويل وتطورها فى ظل هذا النظام قد أتاحت للمهاجمين قدراً أكبر من الحركة والوصول إلى جميع أنحاء العالم.

فرضية البحث:

تأسست فرضية البحث على أن استجابة الدول ستكون غير فعالة؛ وستزيد احتمالية تعرضها للمخاطرالإلكترونية فى ظل النظام الإيكولوجي الرقميمما سينعكس علىفاعليته فى التوسع فى المجالات التطبيقية؛ حال إذا لم تتمكن من تأمين مجال فضاءها الإلكتروني ورصد مصدر تلك المخاطر والتعامل معها ومعالجة نتائجها فى الوقت المناسب.

أهمية البحث:

تتزايد مع الاستخدام المتنامي للتكنولوجيا الرقمية تزايد أكبر للمخاطر الإلكترونية التي تستهدف ضرب مصالح الأخر سواء أكانت مصالح اقتصادية أم اجتماعية أم سياسية، والتي من المتوقع أن تستمر وتتطور خاصة مع التوسع فى المجالات التطبيقية للنظام الإيكولوجي الرقمي؛ وسهولة استخدام وانخفاض تكلفة الدخول عبر القنوات الرقمية المتصلة به وقدرتها على إخفاء هوية المستخدم؛ ومن ثم تتضحأهمية دراسة وبحث تأثير المخاطر الإلكترونيةعلى فاعلية هذا النظام لتوفير خيارات أفضل لمواجهة ازدياد كثافة الهجمات الإلكترونية وارتفاع تكاليفها المالية والاقتصادية.

هدف البحث:

يهدف البحث التعرف على آلية عمل النظام الإيكولوجي الرقمي وعلى أهم المخاطرالتي يفرزها وانعكاساتها على الاقتصاد الرقمي، وذلك لحماية الأصول المالية والمعنوية والحفاظ على سرية البيانات والمعلومات للأشخاص الطبيعية والاعتبارية، مع إلقاء الضوء على أهمية المخاطر الإلكترونية والآثار الاقتصادية الناشئة عنها خصوصاً وأن العالم يسعىإلى التحول الكامل لاقتصادات قائمة على

المعرفة التقنية؛والوصول إلى نتائج وتوصيات تساعد صانعي القرار فى سد الثغرات ومواجهة المخاطر الإلكترونية فى هذا المجال.

منهج البحث:

أعتمد البحث على المنهج الاستقرائي الوصفي والمنهج الاستنباطي لدراسة المشكلة من حيث طبيعة النظام الإيكولوجي الرقمي وعلاقته بالاقتصاد الرقمي، وعرض أهم الهجمات الإلكترونية وأساليب مواجهتها فى ظل هذاالنظام الذي يعمل بحكم طبيعته فى محيط افتراضيساحته الفضاء الإلكتروني.

خطة البحث:

على ضوء ما عرضه الباحث سيتم تقسيم خطة البحث إلى ما يلي:

- المطلب الأول : ماهية النظام الإيكولوجي الرقمي .....
- المطلب الثاني: الهجمات الإلكترونية والاقتصاد الرقمي .....
- المطلب الثالث : إدارة المخاطر فى النظام الإيكولوجي الرقمي .....
- الخلاصة والنتائج والتوصيات .....

المطلب الأول

ماهية النظام الإيكولوجي الرقمي

يتضمن النظام الأيكولوجي الرقمي العلاقات والشراكات والشبكات والتحالفات والمخاطر التي تدور فى الفضاء الإلكتروني، وهو يعمل على دمج الأدوات والتقنيات الرقمية لزيادة أداء الأعمال ودعم النمو وتقديم قيمة مضافة للمستهلك من خلال زيادة تدفق البيانات لتقديم خدمات ومنتجات ونماذج أعمال جديدة مبتكرة تؤثر فى مجال أعمال الاقتصاد الرقمي، كما أصبح من الممكن فى ظل هذا النظام وبشكل متزايد أن تقوم الكيانات الاقتصادية بتفعيل هجمات رقمية لتحقيق أهدافها الخاصة.

أولاً ـ النظام الإيكولوجي فى العالم الطبيعي:

صاغ عالم النبات Arthur Tansley النظم الإيكولوجية فى العالم الطبيعي فى ثلاثينيات القرن الماضي للإشارة إلى مجتمع محلي من الكائنات الحية تتفاعل مع بعضها البعض وبيئتها الخاصة من الهواء والماء والتربة المعدنية وعناصر أخرى؛ هذه الكائنات يتنافسون ويتعاونون ويتشاركون ويخلقون الموارد ويشتركون فى التطور؛ ويتعرضون حتماً لاضطرابات خارجية يتأقلمون معها معاً.[1] وقد تم استنتاج أوجه التشابه ما بين النظام البيئي الطبيعي والرقمي فتم استدعاء مفهوم فكرة النظم البيئية الطبيعية إلى العالم الرقمي.

ثانياً ـ النظام الأيكولوجي فى العالم الرقمي:

أ ـ الجذور التاريخية:

يستمد هذا النظام جذوره من المصطلح الياباني Keiretsu الذي يشير إلى شبكة شركات مختلفة ذات علاقات وثيقة، تمتلك أحياناً حصصاً صغيرة من الأسهم فى بعضها البعض مع استمرار الاستقلال التشغيلي لكل منها، وقد ظهرت هذه الطريقة بعد الحرب العالمية الثانية ؛ وفيها يمكن التمييز بين تحالف لشركات مختلفة حول بنك أساسي يوفر التمويل اللازم لها (A horizontal keiretsu)؛ وبين تشارك المصنعين

(1) http://downtoearth.danone.com/2012/08/14/arthur-tansley-the-founding-father-of-ecology-was-an-honnete-homme/

والموردين والموزعين لخفض التكاليف وزيادة الكفاءة (A vertical keiretsu) ومن ثم تحقيق الاستفادة من خبرة الشركات المتحالفة ؛ والحد من خطر المنافسة والتعرض لمحاولات الاستحواذ من قبل الغير [١]

ب- مفهوم النظام الأيكولوجي الرقمي:

أسقط James F. Moore في عام ١٩٩٣ مفهوم النظم الايكولوجية (النظم البيئية) فى العالم الطبيعي على عالم التجارة الديناميكي ؛ حيث رأى أن الأعمال الناجحة هي التي تتطور بسرعة وفعالية ؛ وأن الشركات المبتكرة لا يمكنها أن تتطور فى فراغ؛حيث يجب عليها جذب الموارد وتنظيم رأس المال والشركاء والموردين والعملاء لإنشاء شبكات تعاونية ؛ على ألا يُنظر إلى الشركة على أنها عضو فى صناعة واحدة ولكن كجزء من نظام بيئي للأعمال يشمل مجموعة متنوعة من الصناعات؛ تعمل من خلاله على تطوير قدراتها حول ابتكار جديد بالعمل بشكل تعاوني وتنافسي لدعم المنتجات الجديدة وتلبية احتياجات العملاء[٢].

ثالثاً- ماهية النظام الايكولوجي الرقمي:

أ- تعريف النظام الايكولوجي الرقمي:

هو مجموعة من مصادر تكنولوجيا المعلومات المترابطة التي يمكن أن تعمل كوحدة واحدة؛ ويتكون من الموردين والعملاء والشركاء التجاريين والتطبيقات ومقدمي خدمات البيانات وجميع التقنيات ذات الصلة؛ وكذا قابلية التشغيل البيني التي تتمثل فى قدرة أنظمة أو برمجيات الحاسوب على تبادل المعلومات والاستفادة منها التي تعدأساس نجاح النظام البيئي، وعادة ما يتم إنشاء النظم البيئية الرقمية والتحكم فيها من قبل قادة السوق من خلال شبكة أعمال تتألف من المصنعين وشركاء سلسلة التوريد والموزعين والمولين ، مما قد يؤثر على التغيير فى مختلف الصناعات بسرعة ، بما فى ذلك المنتجات الاستهلاكية والسيارات والرعاية الصحية. [٣]

(1) -See:https://www.investopedia.com/terms/k/keiretsu.asp&https://en.wikipedia.org/wiki/Keiretsu
تم الاطلاع بتاريخ ١١ يوليو ٢٠٢٠

(2)-See: James F. Moore: https://hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition/ar/1,.

(3)2-WhatisaDigitalEcosystem?(techtarget.com)PostedbyMargaretRouse&Contributor(s): Kate Brush Kate Brush. https:// searchcio.techtarget.com /definition/digital- ecosystem
.تم الاطلاع بتاريخ ١١ يوليو ٢٠٢٠

أن النظام الايكولوجي الرقمي يعبر عن هيكل ديناميكي قوى من الأنظمة والتقنيات ومساهمات الشركات يوفر تدفق وجمع البيانات والمعلومات فى الوقت الفعلي الذي تحدث خلاله صفقة أومعاملة ما، لتعزيز النمو باستمرار فى مجالات أداء الاعمال المتعددة لمواكبة احتياجات وتفضيلات الشركات والموردين والشركاء الخارجيين والعملاء سواء فى متجر فعلي أو افتراضي عبر جهاز محمول أو هاتف ذكي.

ب- استراتيجية النظام الايكولوجي الرقمي:

تعتمد استراتيجية هذا النظام على توحيد وتفاعل الأنظمة والأدوات الحديثة مع بعضها البعض، والبحث عن شركاء خارجيين لتقديم قيمة مضافة للعملاء من خلال الخدمات والمنتجات ونماذج الأعمال الجديدة. فعلى سبيل المثال استخدمت شركة تصنيع السيارات فيات بالشراكة مع كل من Face book,Tunein,TomTom البيانات الخاصة بشركائها الخارجيين لتقديم نظام ملاحي وترفيهي واتصالات متصل ومثبت فى سيارات مختارة من جيب وكرايسلر وفيات؛ من خلال الإصدار المحدث من منصة Uconnect الخاصة بها.[1]

ج- خريطة النظام الايكولوجي الرقمي:

تمثل خريطة النظام البيئي الرقمي رسم تخطيطي لجميع الأدوات والمنصات الرقمية المستخدمة داخل المنظمة ، توضح العمليات، وكيف يتم نقل البيانات بين أجزاء هذا النظام ، وما إذا كانت العملية تتم بطريقة آلية أو يدوية؛ على أن توثق أيضاً الأنظمة غير المتصلة حالياً أو القادرة على نقل البيانات بين بعضها البعض، وكذلك تحديد من هم مستخدمي كل نظام ومن المسؤول عن صيانته.[2] هذا ويعد إنشاء خريطة إيكولوجية رقمية أمراً أساسياً لإنشاء نظام بيئي رقمي قوي فعال.

د- النظام الايكولوجي السحابى:

يتكون هذا النظام من أجهزة وبرامج وعملاء ومهندسي السحابة والاستشاريين والمتكاملين والشركاء؛ ومركز هذا النظام هو مزود الخدمة السحابية العامة، وتنطلق من وسط السحابة شركات البرمجيات التي تستخدم النظام الأساسي لمنصة رقمية

(1) -Digital Ecosystem, a Step Towards Success , https://thekeenfolks.com/keensights/digital-ecosystem-success/

(2)-Digital Ecosystem, ibid

أو برنامج متعهد توفير خدمة الاتصال بالإنترنت، بالإضافة إلى الاستشاريين والشركات التي تشكل تحالفات استراتيجية مع المتعهدالأساسي لتوفير خدمة الاتصال بالإنترنت. هذا ويوفر النظام للعملاء شراء تطبيقات الأعمال والاستجابة لاحتياجات العمل المتغيرة بطريقة سهلة ميسرة عن طريق توفير برامج وخدمات البائعين المختلفين والتي سبق وتم فحصها ومراجعتها من حيث الأمان والمخاطر والتكلفة. ومن أمثلة مزودي الخدمة السحابية العامة AWS Marketplace أو Microsoft AzureMarketplace (للبرامج السحابية) أو Microsoft AppSource (لتطبيقات الأعمال) [١]

رابعاً - النظم الإيكولوجي الاقتصادي الرقمي:

تزايد الاهتمام بمفهوم النظام الإيكولوجي الرقمي لتصوير البيئة التنافسية؛ فالمفهوم لا يتعلق فقط بالمجال التكنولوجي للشركات، ولكن يتعلق أيضاً بقطاعات أخرى مروراً بالخدمات المالية إلى التصنيع [٢].وقد تأثر هذا المفهوم بشكل كبير وأساسي من انفتاح الأسواق العالمية، وانتشار وسائل النقل الحديثة، والاتصالات متنامية السرعة؛ وهو يقوم بشكل أساسي على أساس التدفقات المعلوماتية التي يتم إنشاؤها تأسيساً على الأعمال الفكرية لعلماء الأحياء والفلسفة وعلم الاجتماع والاقتصاد، خاصة فيما يتعلق بمجالات الاقتصاد سواء فى مجال الأعمال المصرفية أو التجارية أو الإنتاج؛ حيث أن التطور النظري للنظم الإيكولوجية الاقتصادية يعد أحد المسارات الأساسية للنظم الإيكولوجية الرقمية؛ حيث يتم انتهاج التقنيات الرقمية بشكل سريع وتكون لها تأثير كبير على الإدارة والأعمال،وسلوك المستهلك والتفاعلات الاجتماعية، وعلى قطاعات مختلفةأخرى. [٣].

أ - النظام الإيكولوجي للأعمال الرقمية:

يظهر مفهوم النظام الإيكولوجي الرقمي بشكل واضح وصريح للترابط بين المنظمات وبيئتها ويوفر وجهة نظر مبتكرة حول التطور المشترك

(1) -cloud ecosystem Posted by Margaret Rouse WhatIs.com Contributor(s): Jason Sparapani and Liz Herbert https://searchitchannel.techtarget.com/definition/cloud-ecosystem
تم الاطلاع بتاريخ ١١ يوليو ٢٠٢٠

(2) Deloitte. (2015, April). Business ecosystems come of age.
http://dupress.deloitte.com/dup-us-en/focus/business-trends/2015/business-ecosystems-come-of-age-business-trends.html
تم الاطلاع بتاريخ ١١ يوليو ٢٠٢٠

(3) Fumagalli, A.; Lucarelli, S.; Musolino, E.; Rocchi, G. Digital labour in the platform economy: The case of Facebook. Sustainability 2018, 10, 1757.

وخلق القيمة [١] ويشمل نظام الأعمال التجارية جميع الجهات الفاعلة التي تشارك بشكل مباشر أو غير مباشر فى الإنشاء المشترك للقيمة المضافة، هذا وتزود النظم البيئية الشركات بالموارد الضرورية وتعتبر المجال الذي تشارك فيه الشركات لخلق قيمة مضافة. هذا ويمكن فهم النظام الايكولوجي للأعمال الرقمية Digital business ecosystems على أنه « مجموعة من الشركات التي ترتبط ببعضها البعض من خلال مصلحة مشتركة فى ازدهار التكنولوجيا الرقمية لتجسيد ابتكاراتها الخاصة بالمنتج أو الخدمة » [٢]

ب- المنافسة فى ظل بيئة الاعمال الرقمية:

أدى تأثير الرقمنة على التطور واندماج الشركات بشكل متزايد فى نظام الشبكات بين المنظمات Interorganizational networks (فيما يتعلق بالعلاقات الاجتماعية والمهنية وعلاقات التبادل فيما بينهم)، إلى تغير طريقة

عمل الشركات من المنافسة إلى التعاون والشراكة [٣] حيث يشمل هذا النظام علاقات الشركة بالموردين، أو العملاء، أو المنافسين، أو الكيانات الأخرى عبر حدود الصناعات أو الدول؛ويتخذ أشكالاً مختلفة مثل التحالفات الاستراتيجية، والمشاريع المشتركة،وحقوق الامتياز، والتسويق طويل الأجل وعقود الترخيص،واتفاقيات التجارة المتبادلة، وشراكات البحث والتطوير، والعلاقات بين المشترين والموردين، والتداخل بين المديرين، والعلاقات المصرفية الاستثمارية،وروابط حركة الموظفين وروابط الاقتباس من براءات الاختراع [٤]

فعلى سبيل المثال يتنافس بعض أعضاء المبادرة العالمية لسلامة الأغذية (GFSI) بشراسة فى أسواقهم ، إلا إنهم يتعاونون بقوة للحصول على الشهادات والمعايير المشتركة والمراقبة الفائقة والتعلم المشترك والممارسات الرائدة التي تخلق صناعة أغذية أكثر أماناً وتعزز ثقة المستهلك؛وهو سلوكاً جديداً موجهاً للنظام الايكولوجي

(1)Adner R, Kapoor R (2010) Value creation in innovation ecosystems: How the structure of technological interdependence affects firm performance in new technology generations, Strategic management journal31(3) :P 309.

(2) Selander L, Henfridsson O, Svahn F (2013) Capability search and redeem across digital ecosystems. Journal of information technology 28(3): P184.

(3) Snow CC (2015) Organizing in the ages of competition, cooperation, and collaboration. Journal of leadership and organizational studies 22(4):1–10

(4) Zaheer A, Gözübüyük R, Milanov H (2010) It's the connections: The network perspective in interorganizational research. Academy of management perspectives 24(1): P62&Gulati R, Nohria N, Zaheer A (2000) Strategic networks. Strategic management journal 21: P203

يستفيد فيه كل مشارك من استثماره الجماعي فى المجالات المشتركة. وهو ما ترى معه GFSI التي تضم العديد من أكبر منتجي الأغذية والموزعين وتجار التجزئة فى العالم ؛ أن « سلامة الأغذية ليست ميزة تنافسية ». وإنما هي تنسيق ونهج عالمي وإبداعي وتعاوني لمواجهة التحدي المتزايد فى نظام غذائي عالمي لضمان سلامة المستهلكين وحماية سمعة الصناعة. (١)

إلا أن هذا التنسيق لم يكن النهج الوحيد حيث أوجد النظم الإيكولوجي الرقمي أيضاً ميزة تنافسية جديدة قوية، حيث جاء الهدف الإستراتيجي لـ Softbank اليابانية فى يوليو ٢٠١٤ ليؤكد توفير جميع أنواع الخدمات على منصته الرقمية، وإنشاء نظام بيئي شامل لن تتمكن الشركات الأخرى أبداً من القيام بنظيرة. « (٢) لتقوم شركة SABMiller في جنوب إفريقيا بإعطاء الاهتمام الأكبر « لتقوية النظم البيئية للأعمال » التي تشارك فيها لصالح الاقتصادات المحلية والإقليمية التي تعمل فيها. (٣)

كما رحب البعض بالمنافسين الذين يعملون فى نفس الأنظمة البيئية حيث اعتبره البعض أمر ضروري للصناعة ككل. (٤) هذا وقد تغيرت البيئة التنافسية بشكل كبير مع الاقتصاد الرقمي حيث أفسحت المجال أمام الاستحواذ ؛ فعلى سبيل المثال قامت شركات تصنيع السيارات Audi وBMW وDaimler ؛ فى صيف ٢٠١٥ ببناء شبكة استراتيجية فى شكل اتحاد من أجل الحصول على أعمال رسم الخرائط الرقمية من شركة Nokia « HERE » التي تعتبر أحد المزودين الرئيسيين لخدمات الخرائط والمواقع

(1) Bob Johansen and Karl Ronn, excerpt from the reciprocity advantage: A new way to partner for innovation and growth, September 24, 2014, Stanford Social Innovation Review

تم الاطلاع بتاريخ ١٨ يوليو ٢٠٢٠

http://www.ssireview.org/articles/entry/the_reciprocity_advantage_a_new_way_to_partner_for_innovation_and_growth,

(2) Masayoshi Son (chairman and CEO, Softbank Corp.) "CEO message," July 2014, http://www.softbank.jp/en/corp/irinfo/about/message/٢٠٢٠ تم الاطلاع بتاريخ ١٨ يوليو

(3) Beth Jenkins, and other, "Sustaining and scaling the impact of enterprise development programmes: SABMiller's approach to strengthening business ecosystems," 2014,

تم الاطلاع بتاريخ ١٨ يوليو ٢٠٢٠

http://api.ning.com/files/bdOTGIbNKtpXrwztIDnrPUiLaBZv-kj54t7gPGybvSP4fB6rHs2oM-mFAb-GuKJRUxkA2397jwZfNwLMj-SPdfTKVWK*Z0ehf/SABMillerEcosystem.pdf.

(4) Brian Krasserstein, "MakerBot's new CEO Jenny Lawton discusses the company's future as well as the industry with 3DPrint.com," 3DPrint.com, October 10, 2014, http://3dprint.com/18506/jenny-lawton-makerbot/٢٠٢٠ تم الاطلاع بتاريخ ٤ أغسطس

، ومكون رئيسي لتطوير تجارب القيادة الآلية ، وذلك مقابل ٢,٨ مليار يورو [١] وهو ما يعد مثال على الاستحواذ على شركة خدمات رقمية من خلال شبكة مشتركة بين الشركات المصنعة للسيارات [٢]

ج ـ الاقتصاد الرقمي الجديد فى النظم الإيكولوجية:

أوجدت الثورة الصناعية الرابعة اقتصاداً رقمياً جديداً New' Digital'(NDE) Economy مدعوماً بأنظمة «إلكترونية فيزيائية» متقدمة تغطي التصنيع «المتقدم» والنقل والخدمات وحتى النظم البيولوجية. [٣] ويتضمن التصنيع المتقدم والروبوتات وأتمتة المصانع ، ومصادر جديدة للبيانات من اتصال الإنترنت والمحمول والحوسبة السحابية، وتحليلات البيانات الضخمة، والذكاء الاصطناعي. فالمحرك الرئيسي لتجربة الاقتصاد الرقمي «الجديد هو التحسين الأسي المستمر فى أداء تكلفة تكنولوجيا المعلومات والاتصالات (ICT)، وخاصة الإلكترونيات الدقيقة.

١ـ ماهية الاقتصاد الرقمي:

الاقتصاد الرقمي هو الاقتصاد القائم على التكنولوجيا الرقمية بما فيها شبكات الاتصال، الحواسيب، والبرمجيات وتكنولوجيا المعلومات ذات الصلة، كما يُطلق عليه أيضاً اقتصاد الإنترنت، الاقتصاد الجديد أو اقتصاد المواقع الإلكترونية.

هذا وتتعدد تعريفات الاقتصاد الرقمي، ومن أهم تلك التعريفات الذي يركز على كيفية قياس الظواهر الناشئة فى الأعمال الإلكترونية والتجارة الإلكترونية؛ والذي

(1) Geiger F (2015) German car firms acquire Nokia unit. In: The Wall Street Journal, August 4:18

- Ribeiro J (2015) Nokia sells HERE maps business to Audi, BMW Group, and Daimler. PC-World, August http://www.pcworld.com/article/2955852/business/nokia-reaches-deal-to-sell-here-business-to-audi-bmw-group-and-daimler. html.

تم الاطلاع بتاريخ ٢٨ يوليو ٢٠٢٠

(2) Bharadwaj A, El Sawy OA, Pavlou PA, Venkatraman N (2013) Digital business strategy: Toward a next generation of insights. MIS quarterly 37(2):471–482

- Iansiti M, Lakhani K (2014) Digital ubiquity: How connections, sensors, and data are revolutionizing business. Harv Bus Rev 92(11):91–99

- Porter ME, Heppelmann JE (2014) How smart, connected products are transforming competition. Harv Bus Rev 92(11):64–88

(3) Schwab, K. 2015. "The Fourth Industrial Revolution What It Means and How to Respond." Foreign Affairs, Science & Technology, December 12. https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution Schwab, K. 2016. The Fourth Industrial Revolution. New York: Crown Business.

تم الاطلاع بتاريخ ١١يوليو ٢٠٢٠

يستند على المكونات الأساسية للاقتصاد الرقمي وهي «البنية التحتية للأعمال الإلكترونية (البنية التحتية الاقتصادية المستخدمة لدعم عمليات الأعمال التجارية الإلكترونية وإجراء عمليات التجارة الإلكترونية)، والأعمال الإلكترونية (أي عملية تجريها مؤسسة تجارية عبر شبكات يتوسط فيها الحاسوب (، و«التجارة الإلكترونية (قيمة السلع والخدمات المباعة عبر شبكات الحاسوب) [١]. ومن أهم تلك التعريفات أيضاً التعريف الذي يركز على تناول قضايا الاقتصاد الرقمي الرئيسية؛ الابتكار والحقوق والأمن الإلكتروني ومحو الأمية الرقمية؛ باعتباره اقتصاد قائم على التقنيات الرقمية، وإدارة الأعمال من خلال الأسواق القائمة على الإنترنت والشبكة العالمية» [٢]

كما أن هناك تعريف أخر يركز على المنافسة وتنظيم الاقتصاد الرقمي؛ باعتباره هيكل معقد مكون من العديد من المستويات والمنصات المتصلة ببعضها البعض من خلال عدد لا حصر له من النقط التي تتزايد دائماً؛ مما يتيح طرقاً متعددة للوصول إلى المستخدمين النهائيين ويكون من الصعب معه استبعاد لاعبين محددين، مثل المنافسين. [٣]

٢ ـ أهم نطاقات عمل الاقتصاد الرقمي: هناك ثلاث نطاقات رئيسية للاقتصاد الرقمي نوجزها فيما يلي:

أ. النطاق الأساسي والذي يتضمن قطاع الرقمية (تكنولوجيا المعلومات والاتصالات) ويشمل تصنيع الأجهزة؛ خدمات المعلومات؛ استشارات البرمجيات وتكنولوجيا المعلومات؛ والاتصالات.

ب ـ النطاق الضيق والذي يتضمن الخدمات الرقمية ؛ المنصات الرقمية.

ج ـ النطاق الواسع وأهم ما يتضمنه الأعمال الإلكترونية e-Business، التجارة الإلكترونية e-Commerce، حيث تهتم الثورة الصناعية الرابعة بشكل كبير بالترابط والأتمتة والتعلم الآلي وبيانات الوقت الفعلي، [٤] والزراعة الدقيقة لضمان

(1) Mesenbourg, T.L., 2001. Measuring the Digital Economy, US Bureau of the Census, Suitland, MD. https://www.census.gov/content/dam/Census/library/workingpapers/2001/econ/umdigital.pdf

(2) British Computer Society, 2014. The Digital Economy, British Computer Society, London. https://policy.bcs.org/sites/policy.bcs.org/files/digital.pdf

تم الاطلاع بتاريخ ١٨ اغسطس ٢٠٢٠

(3) European Parliament 2015: Challenges for Competition Policy in a Digitalised Economy

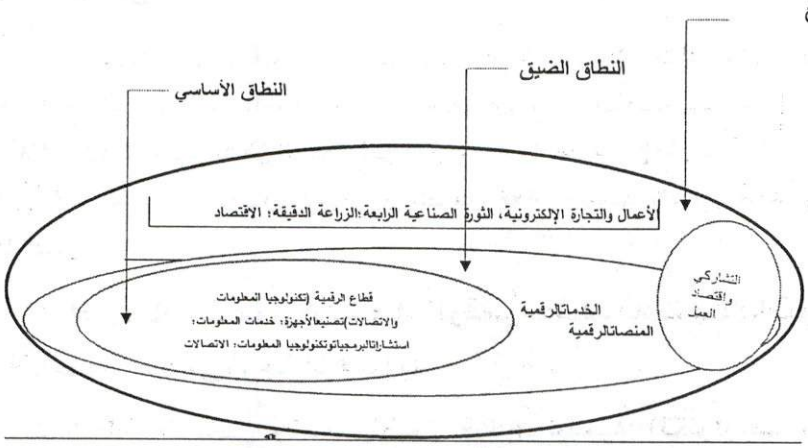
(4) https://www.epicor.com/en-in/resource-center/articles/what-is-industry-4-0/

الربحية والاستدامة وحماية البيئة. [١] وبالاقتصاد الخوارزمي لفهم وتحسين الأسواق والشبكات الاجتماعية المعقدة [٢]، وبالاقتصاد التشاركي للوصول إلى السلع والخدمات التي غالبًا ما يتم توفيرها بواسطة منصة مجتمعية عبر الإنترنت [٣]؛ وباقتصاد العمل الحرأو المستقل عبر المنصات الرقمية. [٤]

هذا ويوضح الشكل رقم (١) نطاقات العمل الرئيسية للاقتصاد الرقمي.

شكل رقم (١)

نطاقات العمل الرئيسية للاقتصاد الرقمي



Source.Bukht R,and Heeks R (2017). Defining, conceptualizing, and measuring the digital economy, Development Informatics Working Paper No,68, Centre for Development Informatics, University of Manchester, Manchester,13

خامساً ـ النظام الإيكولوجي الرقمي وحروب الجيل الرابع:

تعرف الصراعات أو الحروب غير المتكافئة Asymmetric wars and con‹icts، بحروب الجيل الرابع ، التي يكون أحد طرفيها دولة والطرف الاخر خصم قد يكون دولة أو خلايا خفية أو لا دولة (منظمات إرهابية غير وطنية) ؛ تنشط لضرب

(1) https://whatis.techtarget.com/definition/precision-agriculture-precision-farming
(2) https://www.bestcomputersciencedegrees.com/faq/what-is-algorithmic-economics.
(3) https://www.investopedia.com/terms/s/sharing-economy.asp
(4) https://zety.com/blog/gig-economy statistics

تم الاطلاع بتاريخ ١٨غسطس ٢٠٢٠

المصالح الحيوية للدولة المستهدفة لإضعافها أمام الرأي العام الداخلي،استناداً على التكنولوجيا الرقمية وشبكات الاتصال وقراصنة الحاسوب مستخدمة كافة الضغوط المتاحة (سياسية، أو عسكرية، أو اجتماعية، أو إعلامية أو اقتصادية) لإقناع صناع القرار لدى الخصم بأن أهدافهم الإستراتيجية غير قابلة للتحقيق بهدف تدمير المجتمع داخلياً (السكان والثقافة والبنية التحتية)؛ كما تستهدف مراكز الثقل الاستراتيجية بشكل كبير. [1]فهي ليست حرب عسكرية بقدر كونها حروب تقنية رقمية تقوم على الحروب النفسية تستهدف التنمية الاقتصادية وتقويض اركان الدول.

(1) Echevarria, Antulio J. (2005) "Fourth Generation War and Other Myth.P23-24." www.StrategicStudiesInstitute.anny.mil.

تم الاطلاع بتاريخ ١١ يوليو ٢٠٢٠

المطلب الثاني

الهجمات الإلكترونية والاقتصاد الرقمي

ترتكب العديد من الدول فى جميع أنحاء العالم هجمات الكترونية متعددة ومتنوعة في إطار الحروب والتهديدات وعمليات التجسس الاقتصادي *من ناحية، كما تقوم أيضاً بوضع الخطط والاستراتيجيات لحماية مواردها ومواجهة الهجمات والتجسس الإلكتروني من ناحية أخرى؛ وفى كلتا الحالتين يتم تخصيص مزيداً من مصادر التمويل لتأمين البنية التحتية،(أنظمة الكهرباء والنفط والمياه والغاز)، وحماية نطاقات الاقتصاد الرقمي من مخاطر تلك الهجمات.

أولاً - مخاطر الهجمات الالكترونية:

أشار المنتدى الاقتصادي العالمي (World Economic Forum(WEF فى تقريره عن المخاطر الدولية الى ارتفاع المخاوف من المخاطر التكنولوجية خصوصاً الهجمات الإلكترونية وتزوير البيانات؛ حيث ظهرت فى قائمة أعلى خمسة مخاطر دولية محتملة الحدوث فى عام ٢٠١٨؛كما ازدادت فى الآونة الأخيرة كثافة وخطورة الهجمات الإلكترونية الضارة سواء من ناحية الانتشار أو فى مقدرتها على التدمير والحاق الضرر بالمؤسسات الاقتصادية.[١]

أ- ماهية المخاطر الإلكترونية:

تعد المخاطرالالكترونية أحداث إلكترونية محتملة ينتج عنها نتائج غير مرغوب فيها تسبب ضرراً للأنظمة أو للمؤسسة، وقد تنشأ هذه التهديدات داخلياً أو خارجياً ومن الأفراد أو المؤسسات. [٢] أو الدول حيث تتعدد الجهات الفاعلة فى مجال المخاطر الإلكترونية (الدول القومية، الشركات المنافسة، والقراصنة، الجماعات الإجرامية المنظمة، الانتهازيون، والمطلعين على الشركة « Company insiders". [٣].

*تم استخدام الهجمات الالكترونية (التهديدات الرقمية / المخاطر الالكترونية) بمعناها الواسع الذى يتضمن تهديد سرية وسلامة وتوافر البيانات والمعلومات ، والتجسس الاقتصاديالإلكتروني. وان كان هناك بعض الادبيات التي تميز بين الهجمات الالكترونية والتجسس الإلكتروني. انظر:

William A. Owens, Kenneth W. Dam, and Herbert S. Lin, editorsTechnology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, P1-2.

(١) أنظر : د. علم الدين بانقا مخاطر الهجمات الالكترونية (السيبرانية) وأثارها الاقتصادية : دراسة حالة دول مجلس التعاون الخليج. سلسلة دراسات تنموية ، المعهد العربي للتخطيط . الكويت : العدد (٦٢) ،٢٠١٩.ص٩.

(٢) المرجع السابق ص١٢.

(3) See: Joseph S.Nye,Jr. (2010) Cyber Power. Harvard Kennedy School. BelferCenter For Science and International Affairs p9.

فالهجمات الإلكترونية هي اعتداءات ضارة ومتعمدة يتم تنفيذها عبر الفضاء الإلكتروني من قبل مهاجم (قد يكون فرد أو منظمة أو دولة) لاختراق نظام معلومات خاص بآخر (فرد أو منظمة أو دولة) أو لتعطيل شبكة وذلك بنشر برامج ضارة (فيروسات) تسفر عن أضرار بعيدة المدى، لتحقيق أهداف اقتصادية واجتماعية وسياسية، وغالباً ما يستهدف الهجوم الشركات والمنظمات التجارية والوطنية.

ب. الهجمات الإلكترونية والجريمة:

الهجوم الإلكتروني هو هجوم يقوم به مجرمو الإنترنت باستخدام جهاز حاسوب واحد أو أكثر ضد أجهزة حاسوب أو شبكات فردية أو متعددة؛ حيث يمكن تعطيل أجهزة الحاسوب بشكل ضار أو سرقة البيانات أو استخدام جهاز حاسوب تم اختراقه كنقطة انطلاق لهجمات أخرى؛ هذا ويستخدم مجرمو الإنترنت مجموعة متنوعة من الأساليب لشن هجوم إلكتروني، بما فى ذلك البرامج الضارة، والتصيد الاحتيالي، وبرامج الفدية، ورفض الخدمة، وغيرها.[١] فالهجوم الالكتروني هو محاولة للوصول غير القانوني إلى جهاز أو نظام حاسوب بغرض إحداث ضرر أو تعطيل.[٢]

هذاوتعد الهجمات الإلكترونيةوما ينشئ عنها من أثار من قبيل الجرائم الإلكترونية(Cyber Crimes)؛ حيث ان الجريمة الإلكترونية هي تلك الأفعال الإجرامية الناتجة من خلال أو بواسطة استخدام المعلوماتية والتقنية الحديثة المتمثلة فى الكمبيوتر والمعالجة الألية للبيانات [٣]أو هي كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتج بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[٤]هذا وليس من المستحيل فقط منع الهجمات الإلكترونية، بل قد يصعب اكتشافها غالباً؛حيث قد لا يتم إدراك أن هناك هجوم من الأساس؛ فضلاً عن إنه ليس من الصعوبة فقط إسناد أو نسبة الهجوم لفاعله وتحديد مصدر الهجوم، ولكن أيضاً هناك صعوبة فى تحديد النية والمسؤولية عن ذلك الهجوم. [٥] ومن ثم فهناك نوعان من الشركات الأولى تلك التي تم اختراقها بالفعل، والثانية تلك التي لا تعرف أنها قد تعرضت للاختراق.[٦]

---

(1) https://www.checkpoint.com/ cyber-hub/cyber-security/what-is-cyber-attack/

(2) https://www.merriam-webster.com/dictionary/cyberattack تم الاطلاع ٤ اغسطس ٢٠٢٠

(٣) محمد الشواء ثورة المعلومات وانعكاساتها على قانون العقوبات. الطبعة الثانية. دار النهضة العربية، القاهرة، ١٩٩٤، ص ٧.

(٤) أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي. القاهرة. الطبعة الثانية. ٢٠٠٦. ص ٨٧.

(5) Robert W. Lucky reflects on the latest fashion in end-of-the-world scenarios. 31 Aug 2010 https://spectrum.ieee.org/telecom/security/cyber-armageddon

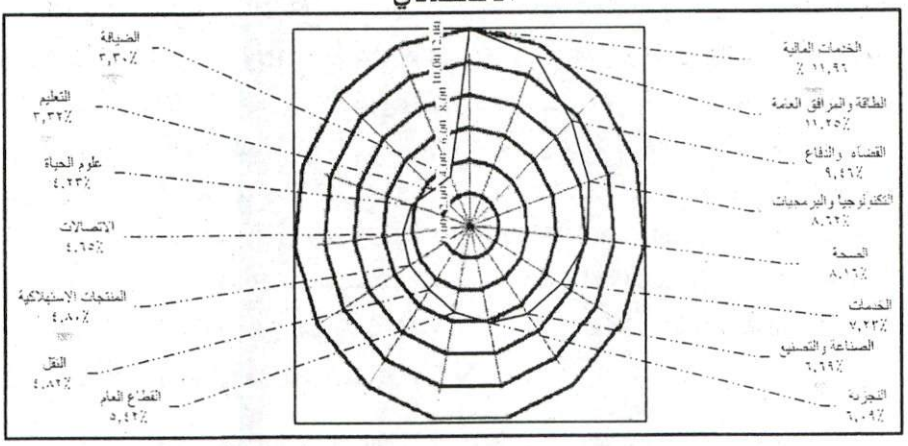
(6) John Chambers: Former Cisco CEO, https://www.checkpoint.com/ cyber-hub/cyber-security/what-is-cyber-attack/ تم الاطلاع ٢٦ اغسطس ٢٠٢٠

هذا ومن المتوقع أن ترتفع تكلفة الجرائم الإلكترونية على قطاع الأعمال فى غضون الخمسة سنوات القادمة إلى حوالي ٨ تريليون دولار؛ كما قدر حجم الخسائر الناجمة عن الأنشطة الإلكترونية الضارة فى امريكا فى عام ٢٠١٦بمبلغ يتراوح بين ٥٧-١٠٩ مليار دولار. [١] وكانت الشركات فى قطاعي الخدمات المالية والطاقة هي الأكثر تضررا، حيث بلغ المتوسط الاجمالي السنوي للتكلفة المالية للجرائم الإلكترونية لمجموعة من الشركات العالمية نحو ١٥٢,٨١ مليون دولار أمريكي فى عام ٢٠١٧؛كان نصيب قطاع الخدمات المالية منها هو الأعلى وذلك بمتوسط قيمة تبلغ نحو ١٨,٢٨ مليون دولار؛ وأهمية نسبية تبلغ نحو ١١,٩٪ مقارنة ببقية القطاعات الأخرى؛ويليه ويتقارب معه نسبياً قطاع الطاقة والمرافق العامة بمتوسط قيمة تبلغ نحو ١٧,٢ مليون دولار، وبأهمية نسبية قدرها ١١,٣٪.[٢]

ويوضح الشكل رقم (٢) الأهمية النسبية لمتوسط التكلفة الإجمالية السنوية للجريمة الإلكترونية.

الشكل رقم (٢)

الأهمية النسبية لمتوسط التكلفة السنوية للجريمة الإلكترونية حسب القطاع الاقتصادي



المصدر بتصرف من الباحث عن: Ponemon Institute LLC and Accenture

(١) د. علم الدين مرجع سبق ذكره. ص ١٠ عن: GlobalRisk Report 2018 & Council of Economic Advisors, CEA, 2018

(2) See: Ponemon Institute, 2017 Cost of Data Breach Study June 2017 & https:// www. Accenture. Com/t20170926T072837Z w_/ us- en/acnmedia /PDF-61/Accenture-2017-CostCyper-CrimeStydy.PDF

حيث تعد الهجمات الإلكترونية بالبرامج الضارة على مستوى العالم وما ينشئ عنها من إصابات هي الأعلى من حيث التكلفة ــ حيث تبلغ تكلفتها نحو ٢,٤ مليون دولار لكل حادث؛ فعلى سبيل المثال فى عام ٢٠١٧، أرتفع متوسط تكلفة الجرائم الإلكترونية علىمستوى العالم إلى ١١,٧ مليوندولار لكل منظمة مقابل ٩,٥ مليون دولار فى عام ٢٠١٦، بزيادة قدرها ٢٣ ٪، والذى يمثل زيادة بنحو ٦٢ ٪ عن السنوات الخمس الماضية ؛تأتي هذه الزيادة فى أعقاب سلسلة حديثة من هجمات البرمجيات الضارة(مثلWannaCryوPetya)، والتي كلفت العديد من الشركات العالمية مئات الملايين من الدولارات من الإيرادات المفقودة.[1]حيث قد يقوم عملاء محتملين بالحصول علىمنتج من مصدر غير قانوني ـ يوفره قراصنة الإنترنت ـ بتكلفة أقل من مثيله فى الشركة المنتجة له أو بدون تكلفة مما يفقد الشركات جزء من إيراداتها المتوقعة.

ج ـ مخاطر الاختراق:

تعد شبكة الروبوت Botnetــ وهي كلمة مشتقة من ((Robot Networkــ أحد أهم وأخطر المشاكل الأمنية التي تواجه الافراد والشركات والدول؛ وهي عبارة عن شبكة من الأجهزة متصلة بالإنترنت (تعدادها قد يصل للملايين) ومصابة ببرامج ضارة؛ يتحكم بها المهاجمين دون علم المالك الأصلي [2]فهي تطبيق مبرمج يقوم بمهام معينة ذات تأثير سلبي كبير على المواقع الإلكترونية أو التطبيقات، ويتم إدارته باستخدام قناة أوامر وتحكم من خلالها تقوم الأجهزة المصابة ــ بشكل تلقائي ــ بتنفيذ الهجمات المطلوبة منها[3]. حيث يستخدم المهاجم فيروسات ـ كفيروس أحصنة طروادة ـ لاختراق أمن العديد من حواسيب المستخدمين والسيطرة على كل حاسوب وتنظيم جميع الأجهزة المصابة فى شبكة يمكن إدارتها عن بعد. وفي بعض الحالات، يقوم بتأسيس شبكة كبيرة من تلك الأجهزة، ونقل حق الوصول إليها لمهاجمين آخرين، سواء بالتأجير أو بالبيع الفوري؛ كما قد يعمد مرسلو البريد الإلكتروني العشوائي إلى استئجار إحدى تلك الشبكات أو شرائها للقيام بحملة بريد إلكتروني عشوائي واسعة النطاق. [4]وقد كشف قطاع الشركات العالمية فى عام ٢٠١٦

(1)https://newsroom.accenture.com/news/accenture-and-ponemon-institute-report-cyber-crime-drains-11-7-million-per-business-annually-up-62-percent-in-five-years.htm

(2) https://www.checkpoint.com/ cyber-hub/cyber-security/what-is-cyber-attack/

(3) Bot Definition: https://www.cloudflare.com/earning/bots/what-is-a-bot/

(4) https://me.kaspersky.com/resource-center/threats/botnet-attacks

عن حدوث أكثر من أربعه مليار اختراق لسجلات البيانات وهي تعادل أكثر من ضعفي مجموع الاختراقات فى العامين السابقين.[١]، ومن أبرز أمثلتها الهجوم الإلكتروني على دولة إستونيا عام ٢٠٠٧، حيث تعطلت مواقع الوزارات والشركات لثلاث أسابيع أتاحت للمهاجم التجسس وسرقة المعلومات (الحصول على رقم أي بطاقة ائتمانية يتم إدخالها، استقبال المعلومات التي يرغب فى الحصول عليها من جهاز الضحية، تغيير الرقم السري للجهاز المستهدف، الاطلاع على كل ما يفعله الضحية، وأخذ صور لما يعرض على الجهاز، وهو ما يحصل عادة فى الابتزاز)[٢].

كما يمكن من خلال تلك الشبكة أيضاً القيام بهجوم رفض الخدمة الموزع (DDoS Distributed Denial-of-Service attack) الذي يتم من خلال استخدام العديد من الأجهزة المخترقة فى إغراق الأنظمة أو الخوادم أو الشبكات بحركة مرور (إمتلاء ذاكرة الأجهزة بالمعلومات) فيتم حجب الخدمة التي يقدمها الموقع الإلكتروني ويجعله غير قادر على تنفيذ الأوامر الصادرة اليه من المستخدم الأصلي؛ ومن أشهر الأمثلة على هذه الهجمات الإلكترونية المتكررة والمتنوعة على المواقع هجمات مجموعة القرصنة أنونيموس Anonymous Hacking Group ضد العديد من الحكومات والمؤسسات والوكالات الحكومية، والشركات[٣]. هذا وقد ارتفعت عالمياً نسبة الحرمان من جراء هجوم رفض الخدمة الموزع بنسبة ١٤٠٪ فى عام ٢٠١٦ وحدها.[٤] كما يمكن للمهاجم أيضاً الهجوم عن طريق إرسال رسائل إلكترونية مزعجة Spam (رسائل تجارية غير مرغوب فيها) عن طريق البريد الإلكتروني أو الرسائل النصية أو منشورات الإنترنت إلى جهاز أو هاتف محمول؛ وهو يعد وسيلة رئيسية لإضافة المزيد من الأجهزة المصابة لشبكة الروبوت.[٥]

د ـ أهم أنواع الهجمات الإلكترونية:

من أهم أنواع الهجمات الإلكترونية؛ هجمات الوسيط، هجمات حقن تعليمات الاستعلام الهيكلية، هجمات يوم الصفر؛ هجوم نظام اسم المجال، فعلى سبيل المثال ارتفعت عدد الهجمات على نفس الضحية المستهدفة إلى ٣٢ مره خلال ثلاثة أشهر فى عام ٢٠١٧؛ وقد بلغ متوسط التكلفة السنوية المقدر ـ فى إحدى الدراسات التي

(١) د. علم الدين مرجع سبق ذكره، ص ١٠

(2) https://en.m.wikipedia.org/wiki/Botnet تم الاطلاع بتاريخ ١٥ اغسطس ٢٠٢٠

(3) https://en.wikipedia.org/wiki/Anonymous_(group)

(٤) د. علم الدين المرجع السابق.

(5) https://en.m.wikipedia.org/wiki/Botnet

تمت فى عام ٢٠١٧ على عينة من ٢٥٤ شركة فى سبعة دول عالمية ـ للتصدي للهجمات الإلكترونية فى الشركة الواحدة لنحو ١١,٧ مليون يورو بزيادة سنوية قدرها ٢٧,٤٪[١]؛ وفيما يلى أهم أنواع الهجمات الإلكترونية :

١ ـ هجمات الوسيط:

يقوم المهاجم بهجمات الوسيط (Man-in-the-middle (MitM attack (التنصت) وسرقة البيانات بمقاطعة حركة المرور بين جهاز الزائر والشبكة حيث يقوم الزائر دون علمه بتمرير جميع المعلومات عبر المهاجم؛ وهي تحدث عند الدخول فى شبكة لاسلكية (Wi-Fi) عامة غير آمنة؛ أو تتم بمجرد اختراق أحد البرامج الضارة للجهاز، حيث يمكن للمهاجم تثبيت برنامج لمعالجة جميع معلومات الضحية.[٢]

٢ ـ هجمات حقن تعليمات الاستعلام الهيكلية:

تستغل هجمات حقن تعليمات الاستعلام الهيكلية (SQL attack) وجود ثغرة أمنية فى تطبيق له اتصال بقاعدة بيانات، حيث يقوم المهاجم بخداع خادم قاعدة البيانات بإرسال تعليمات برمجية ضارة لتنفيذ استعلام غير مصرح به مما يتيح له انتحال الهوية ، والتلاعب بالبيانات الموجودة، والتسبب فى مشكلات التنصل مثل إلغاء المعاملات أو تغيير الأرصدة، والسماح بالكشف الكامل عن جميع البيانات الموجودة على النظام، أو إتلاف البيانات أو جعلها غير متاحة بطريقة أخرى، وأن يصبح مسؤول عن خادم قاعدة البيانات.[٣]

٣ ـ هجمات يوم الصفر:

يؤدى هجوم يوم الصفر(Zero-day attack) أو (الهجوم دون انتظار) الى أضرار جسيمة؛ وذلك حين يكتشف المهاجم وجود نقاط ضعف فى برمجيات أو ثغرة أمنية فى شبكة (قبل اكتشافها وتصحيحها من قبل مطوري تلك الشبكة) فيبدئ هجومه أو مشاركة تلك النقطة أو الثغرة فوراً مع قراصنةHackersأخرين لشن هجمات إلكترونية؛ وكلما تأخر اكتشاف الثغرة من قبل المطورين، كلما منح المهاجمين مزيد من

---

(١) د. علم الدين المرجع السابق.

(2)What Are the Most Common Cyber Attacks? Cyber Attack - What Are Common Cyberthreats? https://www.cisco.com /c/en/us/products/security/common-cyberattacks.html.
Cisco - Global Home Page تم الاطلاع بتاريخ ١١ يوليو ٢٠٢٠

(3) Ibid

الوقت فى توسيع نطاق الهجوم ونشر أدواتهم الضارة وإحداث الضرر المطلوب وإضافة ضحايا جدد. [١]

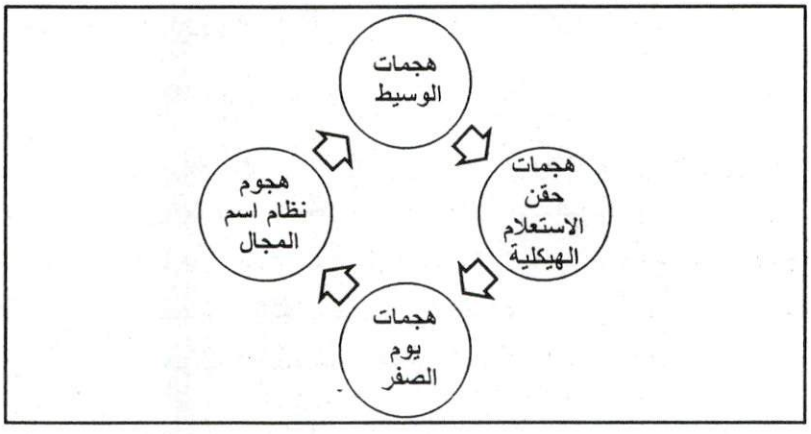
٤ ـ هجوم نظام اسم المجال:

يتم من خلال هجوم نظام اسم المجال Domain Name System DNS التلاعب (بروتوكول عناوين URL؛ وIP المتوافقة مع الأجهزة) بطلبات النظام لاستخراج البيانات من نظام مخترق إلى البنية التحتية للمهاجم ؛ كما يمكن استخدامه أيضاً في عمليات استرجاع الأوامر والتحكم من البنية التحتية للمهاجم إلى نظام مخترق؛ حيث يدرك مهاجمي الإنترنت أن اسم المجال يستخدم على نطاق واسع وموثوق به؛ وانه غير مخصص لنقل البيانات، فإن العديد من المؤسسات لا تقوم بمراقبة حركة مرورنظام اسم المجال الخاصة بها بحثاً عن أي نشاط ضار؛ ومن ثم قد يمكن أن يكون هناك عدد من الهجمات المستندة إلىنظام اسم المجال فعالة إذا تم إطلاقها ضد شبكات الشركات. [٢]

هذا ويوضح الشكل رقم (٣)أهم أنواع الهجمات الإلكترونية:

شكل رقم (٣)

أهم أنواع الهجمات الإلكترونية



المصدر من اعداد الباحث

(1)-https://ar.wikipedia.org/ wiki/هجوم_دون_انتظار

(2) https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

تم الاطلاع بتاريخ ٢٨ يوليو ٢٠٢٠

ثانياً ـ مخاطر التجسس الاقتصادي الرقمي:

ان وضع تعريف جامع مانع للتجسس الاقتصادي فى ظل النظام الإيكولوجي الرقمي يعدمن الصعوبة بمكان حيث أن هناك العديد من التعريفات التي يصعب حصرها؛ وعدة عوامل تؤثر على تحديد ماهية التجسس الإلكتروني مثل مدى وطبيعة الضرر الناجم عنه، وتحديد هوية المهاجم وطبيعة الهجمات، وكيفية استخدام المعلومات المسروقة من جراء عملية التجسس الاقتصادي، وعلى كيفية إدراك وقوع تجسس إلكتروني فى حد ذاته.

أ. ماهية التجسس الاقتصادي:

بصفة عامة يمكن تعريف التجسس الاقتصادي بأنه الاستهداف والسرقة غير القانونيين للمعلومات الاقتصادية الهامة، مثل الأسرار التجارية والملكية الفكرية؛ بالاستحواذ السري أو السرقة المباشرة والتي لا تقدر بثمن فى عدد من المجالات، بما فى ذلك التكنولوجيا والتمويل والسياسة الحكومية؛ حيث يحصل الجناة على وصول سهل إلى المعلومات الهامة ، مما يؤدي إلى تكبد الضحايا خسائر اقتصادية فادحة. [١]، ومن تلك التعريفات أيضاً إنه « فعل يتم ارتكابه سراً أو تحت ذرائع كاذبة يستخدم القدرات الإلكترونية لجمع (أو محاولة جمع) معلومات بقصد إبلاغها إلى طرف آخر»[٢]

كما عرف مكتب التحقيقات الفيدرالي التجسس الاقتصادي بأنه» نشاط استخباراتي منسق ترعاه القوى الأجنبية وموجه إلى حكومة الولايات المتحدة أو الشركات أو المؤسسات أو الأشخاص الأمريكيين، ويهدف إلى التأثير بشكل غير قانوني أو خفي على قرارات السياسة الاقتصادية الحساسة أو للحصول بشكل غير قانوني على معلومات مالية أو تجارية أو اقتصادية حساسة؛ كالمعلومات الاقتصادية مسجلة الملكية أو التقنيات الحرجة؛حيث يمكن أن تمد هذه السرقة ـ من خلال الطرق المعلنة والسرية ـ الكيانات الأجنبية بمعلومات اقتصادية ذات الملكية الحيوية مقابل جزء بسيط من التكلفة الحقيقية لأبحاثها وتطويرها، مما يتسبب فى خسائر اقتصادية كبيرة ". [٣]ولطالما اعتبرت العديد من الدول التجسس الاقتصادي مهماً للأمن القومي والتنمية الاقتصادية.[٤]

(1)https://www.investopedia.com/terms/e/economic-espionage.asp.

(2) The Tallinn Manual, (Cambridge University Press) published in 2013. See: Nation State Cyber Espionage and its Impacts,https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage.pdf

(3)https://www.investopedia.com/terms/e/economic-espionage.asp.

(4)https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law- controversies-involving#_edn3تم الاطلاع بتاريخ ١٥اغسطس ٢٠٢٠

ب ـ التجسس الاقتصادي والحروب الإلكترونية:

يؤدى التجسس الاقتصادي الإلكتروني إلى زيادة المخاطر ـ خاصة إذا ما تعهدته دول بالرعاية بتوفير التنظيم والموارد والرعاية للمتسللين ـ فضلاً عن التأثير على الاقتصادات الوطنية بالحصول على ميزة اقتصادية كأن يتم نقل الثروة بشكل منهجي من دولة إلى آخري من خلال سرقة معلومات قيمة لصالح الشركات المنافسة ، هذا كما ساعدالتطور التكنولوجي على القيام بالتجسس الاقتصادي على نطاق واسع ، دون الحاجة إلى عبور الحدود الوطنية بشكل مادي، وبتكلفة منخفضة نسبياً، وغالباً ما يتم إخفاء هويه المتسلل بشكل نسبى.[١]

هذا كما يمكن إدراج عمليات التجسس الاقتصادي فى إطار الحروب الإلكترونية حيث قامت دول بدمج الحروب الإلكترونية فى عقيدة الحرب لديها ؛ وهو ما بدأته على سبيل المثال ـ الولايات المتحدة الأمريكية لأول مرة فى عام ٢٠٠٢، حيث قامت بتحديد الاستراتيجيات والعقائد والإجراءات والبروتوكولات للحرب الإلكترونية؛ ووضعت خارطة طريق لعمليات المعلومات،والتي نشرتها وزارة الدفاع فى عام ٢٠٠٣،وبدأت فى دمج الاستعدادات للحرب الالكترونية، مثل تدريب العسكريين على الدفاع الإلكتروني، كجزء من العمليات العسكرية العادية ؛ وفي عام ٢٠٠٩ ، أنشأ الجيش الأمريكي القيادة الإلكترونية وبدأ فى تخصيص المزيد من التمويل لتأمين البنية التحتية التي قد تكون عرضة للهجمات الالكترونية.[٢]

ج ـ أهم أدوات التجسس الإلكتروني:

من أهم أدوات التجسس الإلكتروني التي لا غنى عنها للعمليات العسكرية الحديثة؛ والتي تستخدمها بعض الدول [٣]هجمات رفض الخدمة الموزع(DDoS) التي تستخدم بشكل أساسي لتعطيل أنظمة اتصال الدولة المستهدفة؛ والتي يمكن تنفيذها بموارد محدودة للغاية ضد ضحية أكبر وأكثر قوة، كما يتم ايضاً استخدام

(1) Brenda I. Rowe: Transnational statesponsored cyber economic espionage: a legal quagmire, Published online: 13 September 2019.P:64. https://link.springer.com/content/pdf/10.1057/s41284-019-00197-3.pdf

(2) investopedia.com: ibid.

(3) See: Watney, Murdoch. "Challenges Pertaining to Cyber War Under International Law", IEEE Explore; 2014 Third International Conference on Cyber Security, Cyber Warfare, and Digital Forensics, p 15.

-See also: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/.

تم الاطلاع بتاريخ ١٥ اغسطس ٢٠٢٠

البرامج الضارة (الفيروسات والديدان وأحصنة طروادة) لتعطيل عمليات الحاسوب العادية أو جمع البيانات سراً أو تدميرها بالكامل؛ وهى لها آثار مدمرة إذا ما تم تنفيذها على نطاق واسع؛وهناك ايضاً هجمات «القنابل المنطقية» وهي برامج ضارة مصممة لتظل كامنة حتى وقت محدد أو حتى يتم تشغيلها بواسطة حدث معين؛هذا فضلاً عن استخدام أداة انتحال عنوان(IP)، فمن خلاله يتمكن المهاجم من التستر وراء عنوان أخر لإخفاء هويته الأصلية من أجل الوصول إلى معلومات خاصة أو الاستفادة من صلاحيات العنوان الأصلي المستغل أو الوصول لتأمين شبكات معينة؛كما تؤثر التكنولوجيا الرقمية على التجسس الإلكتروني بطرق غير متوقعة؛ بسبب التقدم التقني فى التلاعب بالصور والفيديوهات، فبمجرد وصول المهاجم إلى شبكات الضحية، يمكنه التلاعب بما تراه فى الوقت الفعلي، وبالتالي المساس بمصداقية الاستخبارات المضادة للدولة الأخرى.

د ـ التجسس الاقتصادي على معلومات الملكية:

معلومات الملكية Proprietary Information (الأسرار التجارية)، هي معلومات ترغب الشركة فى الحفاظ على سريتها؛ وقد تتضمن الصيغ والعمليات والأساليب السرية المستخدمة فى الإنتاج؛ وقد تشمل أيضاً خطط أعمال الشركة والتسويق، وهيكل الرواتب، وقوائم العملاء،والعقود، وتفاصيل أنظمة الحاسوب الخاصةبها؛وفي بعض الحالات،قد تعتبر المعرفة والمهارات الخاصة التي تعلمها الموظف اثناء تأدية الوظيفة بمثابة معلومات مملوكة للشركة. [1]ومع انتهاج المجتمعات واعتمادها على التقنيات الإلكترونية ، وقد اعتبر الخبراء أن التجسس الاقتصادي الإلكتروني يمثل تهديداً متزايداً ؛ وقد تضمنت سياسة الأمن الإلكتروني الأمريكي ـ على سبيل المثال ـ التجسس الاقتصادي كمشكلة. [2]

(1) https://www.inc.com/encyclopedia/proprietary-information.html

تم الاطلاع ١٥ أغسطس ٢٠٢٠

(2) See, e.g., White House, National Strategy to Secure Cyberspace viii (Feb. 2003), http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf; see also: White House, Cyberspace Policy Review i (May 8, 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; see also White House, International Strategy for Cyberspace 17 (May 1, 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

تم الاطلاع ٢٦ أغسطس ٢٠٢٠

هـ- مواجهة مخاطر التجسس الاقتصادي:

هناك ثلاث طرق رئيسية للتجسس الاقتصادي - فعلى سبيل المثال ،ووفقاً لمكتب التحقيقات الفيدرالي - هي:

١- تجنيد المطلعين العاملين فى الشركات والمؤسسات البحثية الأمريكية التي تشترك عادة فى نفس الخلفية الوطنية.

٢- استخدام أساليب مثل الرشوة والهجمات الإلكترونية و«الغوص فى القمامة dumpster diving »[١] والتنصت على المكالمات الهاتفية.

٣- إقامة علاقات تبدو بريئة مع الشركات الأمريكية لجمع المعلومات الاقتصادية، بما فى ذلك الأسرار التجارية.

وعليه ينصح مكتب التحقيقات الفيدرالي الشركات بالبقاء فى حالة تأهب؛ ويوصى بعدد من الخطوات، بما فى ذلك تنفيذ خطة استباقية لحماية الأسرار التجارية، وتأمين النسخ المادية والإلكترونية للملكية الفكرية، وتدريب الموظفين.

هذا وقدقدر تقرير صدر عام ٢٠٠٣ عن اللجنة المعنية بسرقة الملكية الفكرية الأمريكية أن التجسس الاقتصادي للملكية الفكرية - على سبيل المثال - له تأثير اقتصادي يبلغ نحو ٣٠٠ مليار دولار سنوياً،ويكلف سوق العمل فى الولايات المتحدة حوالي ٢,١ مليون وظيفة.[٢]

وبشكل عام يتم تنفيذ التجسس السيبراني فى الدول الحديثة؛ من خلال كيانات كبيرة وقوية تتمتع بالسلطة والموارد اللازمة لتطوير أدواته؛ تأسيساً على مجال الفضاء الإلكتروني،وهو ما نوجزه فيما يلي:[٣]

١- أن التجسس الإلكتروني أصبح أكثر تقدماً وفعالية واحترافية؛ فعلى سبيل المثال كان اكتشاف فيروس(Stuxnet)فى عام ٢٠١٠ بمثابة نقطة تحول رئيسية فى التجسس الإلكتروني؛ حيث أستهدف أنظمة التحكم الإشرافي والحصول على البيانات ؛ويعتقد إنه هجوم إلكتروني من جهة غير معلومة على أنظمة المعلومات فى

(١) في عالم تكنولوجيا المعلومات،هي تقنية تستخدم لاسترداد المعلومات التي يمكن استخدامها لتنفيذ هجوم على شبكة الحاسوب. تم الاطلاع بتاريخ١٨ اغسطس ٢٠٢٠ https://searchsecurity.techtarget.com/definition/dumpster-diving

(2) investopedia.com: ibid.

(3) See: Dunn Cavelty, Myriam. "The Militarization of Cyberspace: Why Less May Be Better", IEEE Explore, 2012 4th International Conference on Cyber Conflict (CYCON), P 1-13.

دول متعددة، ويقدر إنها أصابت حوالي ٤٥ الف حاسب آلي فى أنحاء العالم ؛ والذى يمكن اعتباره كأول سلاح رقمي ينذر بقدوم عصر الحروب الالكترونية.[1]

٢ ـ أصبح التجسس الإلكتروني وسيلة حرب مقبولة ومفضلة ــ وان كان هذا لا يعني أنه سيحل محل الوسائل التقليدية للحرب ـ يؤثر على طبيعة صراع الدول القومية؛ وقد ظهر مع الحرب الباردة،بتركيز جهود كل من الولايات المتحدة وروسيا على جمع المعلومات السرية حول الحرب المباشرة والصريحة بينهما؛ خاصة وأن الحرب الشاملة بين القوى العالمية الكبرى أصبحت أقل قبولاً فى العالم الحديث.

(1) https://en.wikipedia.org/wiki/Stuxnet تم الاطلاع بتاريخ ٢٨ يوليو ٢٠٢٠

المطلب الثالث

إدارة المخاطر في النظام الإيكولوجي الرقمي

مع اتجاه النظام الايكولوجي الرقمي إلى المزيد من التطور والتنوع والتعقيد ظهرت هجمات ومخاطر مستجدة الكترونية زادت من حدة مخاطر التشغيل ومستوى تحديدها وطرق إدارتها؛ وبشكل عام فإن المخاطر لها جانبان، الأول احتمالية التعرض لخطر ما، والثاني مقدار أو حجم الخسائر المحتملة الناجمة عن التعرض لهذا الخطر.[١]

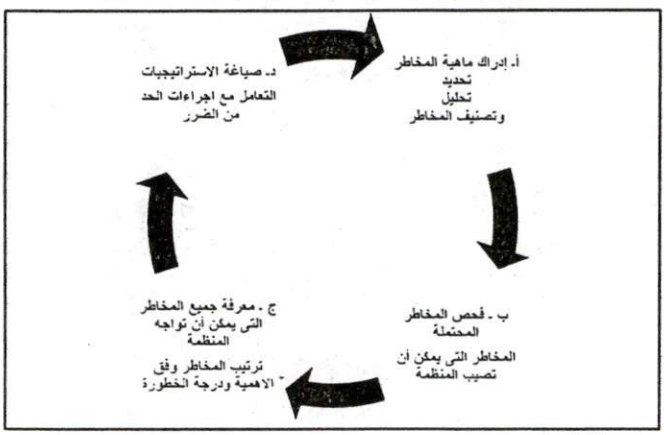
أولاً - ماهية مخاطر التشغيل:

مخاطر التشغيل هي المخاطر التي يكون مصدرها الأخطاء البشرية أو المهنية أو الناشئة عن التقنية أو الأنظمة المستخدمة أو القصور فى أي منها؛ وتنتج عن عوامل داخلية أو خارجية،وتؤدى الى خسائر مباشرة وغير مباشرة.[٢]

فعلى سبيل المثال؛ ووفقاً لتقرير الخسائر المصرفية السنوي لعام ٢٠١٨؛ والذي تم تجميعه من ٨٦ مصرفاً، يتبين خسارة نحو ١٧٠ مليار يورو بسبب مخاطر التشغيل بين عامي ٢٠١٢-٢٠١٧، كما تحققت خسائر بلغت نحو ٢٠٦ آلاف يورو فى المتوسط لكل حدث ضمن مخاطر التشغيل الذي تم الإبلاغ عنه فى عام ٢٠١٧[٣].

هذا ويوضح الشكل التالي مراحل عملية إدارة المخاطر:

شكل رقم (٤) مراحل عملية إدارة المخاطر



المصدر من إعداد الباحث.

(١) راجع صندوق النقد العربي، ورقة بعنوان «مبادئ إدارة المخاطر»، الاجتماع السنوي العاشر للجنة العربية للرقابة المصرفية، ٢٠٠١.
(2) https://www.bis.org/publ/bcbsca07.pdf &https://financetrain.com/definition-of-operational-risk/
(3) https://www.wavestone.com/en/insight/operational-risk/

ثانياً: إدارة المخاطر التشغيلية:

المخاطر التشغيلية هي نشاط إداري يهدف للتحكم بالمخاطر بإدراك ماهيتها وتحديدها وتحليلها وتصنيفها وفق درجة خطورتها ومدى تكرارها والعمل على الحد منها وربطها بأسباب حدوثها وتحديد مصدرها قدر الإمكان وخفضهاإلى مستويات مقبولة من خلال التحديد(فهم وإدراك المخاطر على مستوى كل عملية أو نشاط من أنشطة)؛والقياس(حجم الخطر، ومدته، واحتمالية حدوثه) والضبط (تجنب أو تخفيض الخسائر المحتملة) والسيطرة (نظام معلومات قادر على تحديد وقياس المخاطر بدقة وقادر على مراقبة التغييرات المهمة فى وضع المخاطر)ومن ثم خفض درجة خطورتها؛ وطرح خيارات وخطط مرنة لمواجهتها وخفض تكلفتها المالية وتجنب فقد أو تذبذب جزء من الإيرادات المحتملة نتيجة تلك المخاطر. ومن ثم فقد يكون من الضروري دمج مخاطر الهجمات الإلكترونية ضمن إدارة المخاطر الكلية التي تواجهها المؤسسة ووفقاً للمبادئ والتعليمات الدولية لبناء المنعة ضد المخاطر الإلكترونية[١]

ثالثاً المشكلة الاقتصادية للهجمات الإلكترونية:

تتمثل المشكلة الاقتصادية للهجمات الإلكترونية فى عدم قصورها على المؤسسة المستهدفة وحدها وانما فى امتدادهاوانتشار آثارها الخارجية السلبية إلى قطاعات ومؤسسات ومنظمات أخرى ترتبط بها اقتصادياً (كالموردين)، خصوصاً فى المؤسسات التي تعمل فى مجال البنية التحتية والتي قد تنتشر عبرها الآثار السلبية للهجمات إلى أنشطة اقتصادية مختلفة مما يعوق عمل تلك الأنشطة ويفاقم الخسارة الناشئة عنها مما يتسبب فى زيادة خسائر الاقتصاد الكلي فى الدول الضحية، ومن ثم يجب أخذ الآثار السلبية لتلك الهجمات فى الاعتبار بضخ الاستثمارات فى مجال الأمن الإلكتروني للحد من المخاطر الكلية التي تتعرض لها الدولة المستهدفة ومؤسساتها.[٢]

رابعاً - تصنيف الهجمات الإلكترونية:

يساعد تصنيف الهجمات الإلكترونية فى إدارة المخاطر بشكل أفضل وحماية الأصول المادية والمعنوية للأشخاص الطبيعيين والاعتباريين؛ خاصة إذا ما تم تنفيذ

(١) للمزيد: د. علم الدين،مرجع سبق ذكره، ص ٢٢.
(٢) المرجع السابق، ص ١٠-١١.

الهجوم من مهاجم ذو ماهرة تقنية عالية وعلى مراحل متكررة؛ وهو ما يمكن معه أن تصنف تلك الهجمات الى نوعين:

أ. الهجمات الإلكترونية غير الهادفة:

يحاول المهاجمون فى الهجمات الإلكترونية غير الهادفة استهداف أكبر عدد ممكن من الأجهزةوالخدمات والمستخدمين بشكل عشوائي دون الاهتمام بهوية الضحية بقدر الاهتمام بأن يتم استهدافأكبر عدد من الاجهزة أوالخوادم والبرمجيات التي تحتوي على نقاط ضعف؛ ويستخدمون.فى ذلك التقنيات الرقمية تأسيساً على انفتاح النظام الايكولوجي الرقمي على الفضاء الإلكتروني، ومن أهم تلك الهجمات ؛ الخداع أو التصيد الاحتيالي Phishing التي يكون الهدف منها سرقة بيانات حساسة (معلومات البطاقات الائتمانية) أو التشجيع على زيارة مواقع إلكترونية مزيفة (لتنزيل برامج ضارة على الاجهزة المستهدفة)؛وهناك ايضاً هجمات بئر المياه WateringHoleبإعداد مواقع مزيفة أو إعطاء انطباع بشرعية موقع إلكتروني ما لاستغلال المستخدمين والزائرين ؛ هذا فضلاً عن برامج الفدية Ransomware التي تقوم بتشفير الملفات على الجهاز المصاب وجعلها غير متاحة للمستخدم الأصلي، ومن ثم تطلب فدية (مال) مقابل فك التشفير وإعادتها مرة أخرى، [1] أو تستهدف مساحات كبيرة من الإنترنت بشكل عشوائي.

ب. الهجمات الإلكترونية الهادفة:

يتم فى هذا النوع استهداف مؤسسة معينة يكون للمهاجم اهتماماً خاصاً بمجال عملها أو تم الدفع له لاستهدافها؛ وقد يتطلب الأمر التحضير والتخطيط لهذا الهجوم عدة شهور لإيجاد الطريقة الأمثل لتوجيه الهجوم بشكل مباشر لأنظمتها أو مستخدميها، وغالباً ما تكون الهجمة المستهدفة أكثر تخريباً وضرراً من الهجمة غير المستهدفة لأنها تستهدف أنظمة مؤسسة محددة أو عملياتها أو شؤون موظفيها فى المكتب وأحياناً فى المنزل.ومن أهم تلك الهجمات هجوم التصيد الاحتيالي-Spear Phishing(إرسال بريد الكتروني يحتوي برمجيات ضارة أو رابط يؤدي إلى تنزيل برمجيات ضارة) . وهجوم شبكة الأجهزة المصابة Botnet الذي يعتمد على اختراق أجهزة معينة وحرمانها من الخدمات أو تعطيل نظام الأمان الخاص بها؛فضلاً عن

(1) https://ar.safetydetectives.com/blog/what-is-ransomware-ar/

تم الاطلاع بتاريخ ١٥ اغسطس ٢٠٢٠

هجوم تخريب سلسلة التوريد Subvertingthe Supply Chain التي تهاجم أجهزة أو برامج تم إيصالها بغرض إلحاق الضرر بمنظمة ما عبر استغلال نقاط الضعف فى شبكة سلسلة التوريد.

خامساً : مخاطر الاحتيال والتصيد الإلكتروني:

تعد مخاطر الاحتيال والتصيد الإلكتروني من أهم مخاطر الهجمات الالكترونية؛ وبصفة عامة يعد الاحتيال عمل خادع متعمد يهدف إلى تزويد المهاجم بمكاسب غير مشروعة أو إنكار حق الضحية؛ ومن أشهر أنواعه الاحتيال الضريبي والاحتيال فى الأوراق المالية؛ والاحتيال فى الإفلاس والاحتيال على بطاقات الائتمان والاحتيال الإلكتروني والاحتيال المصرفي؛ هذا ويمكن تنفيذ النشاط الاحتيالي بواسطة فرد واحد أو عدة أفراد أو شركة تجارية ككل.[1].

وفيما يلي إيجاز للاحتيال الإلكتروني والاحتيال المصرفي.

أ. الاحتيال الإلكتروني:

الاحتيال الإلكتروني هو الذي يتم عبر الإنترنت، لتحقيق مكاسب شخصية بشكل غير قانوني سواء عبر البريد الإلكتروني (طلب تقديم معلومات مصرفية ومالية شخصية)؛ أو من خلال المواقع الاليكترونية المزيفة للاحتيال على الأفراد ليقوموا بالشراء من خلال تزويد تلك المواقع بالمعلومات الشخصية المصرفية أو المالية لتسوية صفقة الشراء، وبمجرد مصادرة المحتال لهذه المعلومات يقوم باستخدامها دون أي إذن مسبق لتحقيق مكاسب مالية[2]

ب. الاحتيال المصرفي:

يمكن تعريف الاحتيال المصرفي على أنه عمل غير أخلاقي و/ أو إجرامي من قبل فرد أو منظمة لمحاولة غير مشروعة لامتلاك أو تلقي الأموال من بنك أو مؤسسة مالية،وهو استخدام الخداع لسرقة الأموال أو الأصول من أحد البنوك أو المؤسسات المالية أو المودعين لدى البنك.[3] ومن أهم أنواعه:[4] التزوير (تغير الاسم أو المعلومات

(1) https://www.investopedia.com/terms/f/fraud.asp
(2) https://study.com/academy/lesson/what-is-bank-fraud-definition-prevention.html
تم الاطلاع بتاريخ ٢٦ اغسطس ٢٠٢٠.
(3) Ibid.
(4) https://jsberrylaw.com/blog/bank-fraud-definition-penalties/ تم الاطلاع بتاريخ ١٥ أغسطس ٢٠٢٠

الموجودة على وجه الشيك، أو إضافة صفر إلى المبلغ الأصلي، أو تزوير توقيع الشخص لإيداع أو صرف شيك)؛ وسرقة الشيكات (وفتح حساب مصرفي مزيف وإيداع الشيكات فى حسابات مزيفة)؛ فضلا عن الاحتيال المصرفي عبر الإنترنت (إنشاء موقع إلكتروني مزيف يشبه موقع مصرف حقيقي لخداع الأشخاص وإيداع الأموال).

وبشكل عام هناك ثلاث أطراف لجريمة الاحتيال وهي المجرم (محتال الإنترنت) والهدف (العميل المالي) وعدم وجود أوصياء (عدم وجود حماية من قبل البنوك) [١] ومن ثم يمثل الاحتيال الإلكتروني تهديداً لنظام المدفوعات الرقمية ولوضع المؤسسات المالية ذاتها وتفاعلها مع أصحاب المصلحة الخارجيين، (العملاء والموردين والممولين وشركاء الأعمال).

كما يمثل الاحتيال المصرفي تحدياً كبيراً يواجه البنوك حيث قد تتعرض المعلومات المالية للعملاء للاحتيال عند استخدامهم الخدمات الرقمية؛ وهو ما يتطلب توفير الأمن والسلامة المالية للعملاء وبناء ثقتهم فى تلك الخدمات؛ خاصة مع المحاولات العديدة التي يقوم بها مجرمو الفضاء الإلكتروني الذين يحاولون سرقة المعلومات الشخصية للعميل بمطاردة الخدمات المصرفية عبر الإنترنت [٢] خاصة وان الوصول إلى والاعتماد على الإنترنت يتزايد بسرعة كبيرة فى جميع أنحاء العالم؛ ففي عام ٢٠١٩ اشترى نحو ١,٩٢ مليار شخص سلعاً أو خدمات عبر الإنترنت؛ وخلال نفس العام، تجاوزت مبيعات التجزئة الإلكترونية ٣,٥ تريليون دولار أمريكي فى جميع أنحاء العالم. [٣] كما ومن الملاحظ أيضاً نمو معاملات الاحتيال الناشئة عن تطبيقات الأجهزة المحمولة من ٥٪ فى عام ٢٠١٥ إلى ٣٩٪ عام ٢٠١٨؛ ويعزى جزء من هذه الزيادة على الأرجح إلى زيادة رقمنه الخدمات المصرفية وغيرها من الخدمات الاستهلاكية، فمن الواضح أن قناة الهاتف المحمول لا تزال أكثر عرضة للاحتيال وتتطلب حماية أفضل. كما تم تنفيذ حوالي ٣٩٪ من جميع المعاملات الاحتيالية التي أجريت خلال الربع الأول من عام ٢٠١٨ عبر تطبيقات الجوال؛ حيث استخدم المحتالين وسائل التواصل الاجتماعي لمشاركة المعلومات والإعلان عن متاجرهم الافتراضية وبيع

(1) See: Tewksbury, R.A and Mustaine, E.E. (2010). Encyclopaedia of Criminological Theory: Cohen, Lawrence E., and Marcus K. Felson: Routine Activity Theory, In Contributors: Francis T. Cullen & Pamela Wilcox (Eds.), Encyclopaedia of Criminological Theory. pp. 187-193.

(2) See: Yazdanifard, R., Wanyusoff, W.F., Behora, A.C. & Sade, A.B. (2011). Electronic banking fraud: The need to enhance security and customer trust in online banking, Advances in Information Sciences and Service Sciences, Volume 3, Issue 10, pp. 505-509.

(3) The Statistical Portal. https://www.statista.com/ (2019). Accessed 13 Mar 2019

البيانات المسروقة.لذا يجب توخي الحذر عند الرد على رسائل البريد الإلكتروني غير المتوقعة ؛ وتجنب أي رسائل غير معلومة المصدر على منصات وسائل التواصل الاجتماعي.[١]

ج- التصيد الاحتيالي والفيروس التاجي:

كانت النسبة الأكبر من الهجمات الالكترونية فى الربع الأول من عام ٢٠٢٠ في جميع أنحاء العالم من نصيب هجمات التصيد الاحتيالي، حيث مثلت نحو ٥٤٪ من جميع الهجمات التي تم تحديدها؛وعلى الرغم من أنها تعد من أقدم الحيل الالكترونية، إلا أنه قد ارتبطت خلال هذا الربع المذكور بالفيروس التاجي حيث استهدفت أموال وصندوق الإغاثة ، وأفضل ممارسات منظمة الصحة العالمية ، كالتحديثات المتعلقة باللقاحات وغيرها.[٢]

فقد تسببت جائحة الفيروس التاجي فى خلق فرصة جيدة لنفاذ المحتالين للاستفادة من حالة الخوف السائدة من انتشارها؛ والحاجة للحصول على المساعدات المالية والرغبة فى الحصول على الادوية أو الامصال واللقاحات؛ حيث يدعى المحتالون بأن لديهم فقط علاج أو لقاح أو علاج جديد للفيروس التاجي من خلال إجراء مكالمة هاتفية أو إرسال بريداً إلكترونياً أو رسالة من مزود خدمة ما ؛ أو يتم الاحتيال عن طريق تقديم robocall، وهى مكالمة آلية هاتفية تستخدم طالباً آلياً محوسباً لتوصيل رسالة مسجلة مسبقاً بمساعدة مالية أو لتسريع استلام شيكات البطالة أو التحفيز مقابل رسوم ، أو مكالمة بشأن الحصول على مجموعة أدوات اختبار منزلية جديدة رخيصة الثمن أو مجموعة أدوات تتبع جهات الاتصال؛ أو الاتصال بالادعاء بإن المحتال شخص يمثل منظمة الصحة العالمية ، أو مراكز السيطرة على الأمراض لعرض بيع حق الوصول إلى المعلومات أو الخدمات أو الأدوية الخاصة.[٣]

---

(1) Heidi Bleau: Securing the Digital World RSA Report: Mobile App Fraud Transactions Increased Over 600 Percent in Three Years May 23, 2018. https://www.rsa.com/en-us/blog/2018-05/rsa-fraud-report-mobile-app-fraud-transactions-increased-over-600-percent-in-three-years

(2) Yael Gour,: Securing the Digital World While in Lock Down, Here's What Fraudsters Did in Q1 2020 Jul 07, 2020, https://www.rsa.com/en-us/blog/2020-07/while-in-lock-down-heres-what-fraudsters-did-in-q1-2020

تم الاطلاع بتاريخ ١٥ أغسطس ٢٠٢٠

(3)Amy Fontinelle: The Most Common Types of Consumer Fraud, Updated Jan 9, 2021 https://www.investopedia.com/financial-edge/0512/the-most-common-types-of-consumer-fraud.aspx#covid-19-scams تم الاطلاع بتاريخ ١٥ أغسطس ٢٠٢٠

وغالبا ما يتم استهداف الاحتيال المصرفي عبر الإنترنت الحسابات الخاملة sleeping Account holder، وبشكل عام تعتبر مخاطر الاحتيال نوع من المخاطر التشغيلية وتشمل أساساً التلاعب بالدافع أو المستفيد مما يؤدي إلى إصدار تعليمات الدفع من قبل الدافع الذي يتصرف بحسن نية ؛كما تشمل أيضاً الشروع فى تعليمات الدفع من قبل المحتال (الذي حصل بطريقة احتيالية على بيانات الدفع للمدفوع / المدفوع لأمره) كما تشكل كذلك اعتراض المحتال لتعليمات دفع صادرة بالفعل ومن ثم تعديل سمة من سماتها (مثل رقم الحساب، أو مبلغ المعاملة، أواسم المستفيد، أو الدافع).

وهو الامر الذي يؤثر على جميع الجهات الفاعلة فى سلسلة الدفع، (المستخدم النهائي ومقدم خدمة الدفع ونظام الدفع السريع، وقد تكون خدمات الدفع السريع (الأموال متاحة على الفور ودون قيد أو شرط للمدفوع له) هدفاً أكثر جاذبية للاحتيال من مدفوعات التجزئة التقليدية، فقد يحاول المحتال سحب الأموال بسرعة قبل اكتشاف محاولته للاحتيال، وقد يكون لتدابير عكس أو استدعاء المدفوعات السريعة الاحتيالية فعالية محدودة؛ بشكل عام، ستكون الإجراءات الأمنية القوية ومكافحة الاحتيال مهمة لتقليل المخاطر.

هذا ويوضح الجدول رقم (١) أهم طرق الاحتيال الإلكتروني التي يجب التحوط منها:

جدول رقم (١)

أهم المخاطر الإلكترونية -

المخاطر	المضمون
١- برامج التصيد الاحتيالي Phishing: يمكنها سرقة بيانات بطاقة الائتمان ومعلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية.	تستهدف عملاء الخدمات المصرفية ومواقع المزادات ووسائل الدفع عبر الإنترنت، وغيرها؛ وتتضمن استخدام أحد أشكال البريد العشوائي للوصول إلى التفاصيل المصرفية للأفراد. حيث قد يطلب المحتال الحصول على اسم العميل وكلمة المرور بادعاء تحديث قاعدة البيانات؛ أوان يقوم بإطلاق موقع مشابه لموقع بنك العميل؛ ومن ثم استخدام معلومات العملاء دون علمهم فى اجراء معاملات المالية؛ أو أن يقوم باستنساخ المواقع الإلكترونية فى شكل غرفة محادثة أو مواقع تجارية معروفة بحيث يقوم الأشخاص إما بإعطاء معلوماتهم عن غير قصد أو القيام بعملية شراء "غير حقيقية"، وتقديم المال مقابل منتج غير موجود بالفعل.

٢. البرامج الضارة Malware برامج الفدية Ransomware برامج التجسس Spyware؛ كحصان طروادة Trojan Horse	يتم تثبيت البرامج الضارة سراً على أجهزة الحاسوب ضمن روابط أو مرفقات بريد إلكتروني غير معروف؛ فتتسبب في منع الوصول للمكونات الرئيسية للشبكة (كبرامج الفدية)، أو الحصول على المعلومات والبيانات سراونقلها من القرص الصلب (كبرامج التجسس)، أو جعل النظام غير صالح لأداء مهامه بتعطيل بعض مكوناته؛فهي تقوم بإرسال المعلومات الشخصية والتجارية والنطاق الترددي ـ عند تعامل المستخدم في مواقع الخدمات عبر الإنترنت وتسجيله اسم المستخدم وكلمة المرور ـ إلى المهاجم أو إعطائها سراً إلى شخص آخر دون إذن أو علم المستخدم الأصلي.
٣. القرصنة؛ Hacking	الحصول على دخول غير قانوني واختراق نظام الحاسوب، واستخدام شخصية غير حقيقية لتنفيذ معاملات غير قانونية على الإنترنت.
٤. سرقة الهوية؛ An identity theft	حصول المجرم على المعلومات الشخصية من جهاز حاسوب خاص بشخص، ثم إنشاء حسابات مصرفية مزيفة أو الحصول على قروض باسمه.

المصدر من اعداد الباحث بتصرف عن

1- Rupesh. D. Dubey and Anita Manna: E-Banking Frauds and Fraud Risk Management Tactful Management Research Journal ISSN: 2319-7943 P21-22.

ومن ثم يجب على الأطراف المعنية في النظام الإيكولوجي الرقمي سواء عملاء أو مؤسسات مالية أو مواقع الكترونية ومنصات رقمية الذين ينفذون معاملاتهم وتسوية وسداد صفقاتهم التجارية والمالية عبر الفضاء الإلكتروني أن يكون لديهم وعي كاف بالتهديدات والهجمات الاحتيالية المحتملة حتى يمكنهم تخفيض احتمال تعرضهم للاحتيال عند إجراء وتسوية المدفوعات الرقمية؛ فضلاً عن أهمية قيام المؤسسات المالية والمواقع الإلكترونية والمنصات الرقمية بتأمين أنظمتها لاكتشاف وردع التهديدات الإلكترونية.

سادساً ـ مخاطر مدفوعات التجارة الالكترونية:

سيظل تحقيق عنصر الأمان من المشكلات الأساسية التي تواجه إجراء مدفوعات الكترونية منتظمة لتسوية وسداد مدفوعات التجارة الالكترونية عبر النظام الإيكولوجي الرقمي؛خاصة مع التهديد المستمر لانتهاكات وخرق البيانات؛ فعلى

سبيل المثال زادت معاملات الاحتيال عبر تطبيقات الهاتف المحمول فى الولايات المتحدة بنسبة تزيد عن ٦٠٠٪ خلال الفترة من عام ٢٠١٥ إلى عام ٢٠١٨ حيث استخدم المحتالين وسائل التواصل الاجتماعي لمشاركة المعلومات والإعلان عن متاجرهم الافتراضية وبيع البيانات المسروقة؛ لهذا يجب توخي الحذر عند الرد على رسائل بريد إلكتروني غير متوقعة؛ وتجنب أي رسائل غير معلومة المصدر على منصات وسائل التواصل الاجتماعي.[1]

ومن ثم قد يكون من المناسب أيضاً تنظيم ومراقبة النظام الايكولوجي الرقمي خاصة فيما يتعلق بالخدمات المالية والمصرفية التي تتم عبر الهواتف والأجهزة المحمولة لتسوية وسداد المعاملات التجارية والمالية حيث أصبحت الأجهزة المحمولة هدفاً أساسى لعمليات الاحتيال ، والتي تتزايد ومن ثم تتزايد معها مستويات التهديدات للبيانات والمعلومات وللأموال المادية والعينية، مما قد يمنع الاشخاص من الاندماج إيجابياً فى التجارة الإليكترونية.

سابعاً ـ الاحتراز من مخاطر المدفوعات الإلكترونية:

يمكن استخدام معظم الإجراءات المطبقة فى الأنظمة التقليدية لنظم المدفوعات للتخفيف من أخطار الاحتيال والكشف عنه (إجراءات مسبقة للكشف عن الاحتيال،» الفحص الأمني»؛ أو الإجراءات اللاحقة «تنبيهات الرسائل القصيرة»)؛ كما يمكن اجراء تحليل للمعلومات المرفقة بالمدفوعات السريعة؛ (كطلب معلومات مفصلة حول المرسل والمستلم ووقت المعاملة)؛ وأن كانت تلك الإجراءات قد تبدو أقل فعالية بسبب قصر الفاصل الزمني بين بدء الدفع والتنفيذ؛ فضلاً عن أن مخططات الدفع السريع قد تواجه تحديات أخرى تتمثل فى قدرتها على إكمال الفحص الأمني على المدفوعات وفي نفس الوقت تلبية توقعات المستخدم النهائي بالنسبة لعنصر السرعة ؛إلا أنه فى بعض الحالات ، قد يكون المستخدم النهائي على استعداد للتضحية بمستوى معين من السرعة أو توفر الخدمة من أجل تتبع نشاط المدفوعات بشكل أفضل وتخفيف أخطار الاحتيال.

ثامناً ـ مخاطر التقويض والحماية:

قد تقوم بعض الدول باستخدام استراتيجية التقويض والحماية للقيام بهجمات إلكترونية على أنظمه أعدائها بهدف تدميرها أو السيطرة عليها؛حيث يتم تقويض

(1) Ratna Sahay, Ulric Eriksson von Allmen, Amina Lahreche, PurvaKhera, Sumiko Ogawa, Majid Bazarbash, and Kim Beaton: The Promise of Fintech: Financial Inclusion in the Post COVID-19 Era International Monetary Fund Monetary and Capital Markets Department No. 20/09,2020, P19.

واستغلال تقنيات اتصالات الخصوم،مع حماية تقنيات الدولة؛ حيث يمكن التدخل فى أنظمة الخصم، واستغلال هذا الوصول الخفي لجمع المعلومات الاستخبارية، وفي بعض الأحيان القيام بهجوم إلكتروني مدمر.[١] إلا أن هذا الأمر قد يتطلب التضحية بأمن البنية التحتية للاتصالات العالمية؛ حيث أن المنطق الاقتصادي للإنترنت وأجهزة الحاسوب والهواتف الذكية والعالم المدفوع بالبرمجيات كان فى اتجاه العمل نحو مجموعة واحدة من المعايير التقنية والبنية التحتية العالمية المشتركة؛ ومن ثم يستخدم الخصوم نفس التقنيات التي يتم استخدامها من قبل الدولة التي تتبع سياسة التقويض،وعليه فقد تكون الأنظمة المستهدف تقويضها هي نفس الأنظمة التي يراد حمايتها. [٢]وهو ما قد يفرض ضرورة مقايضة الأمن بالخصوصية، والتضحية بأمن البنية التحتية للاتصالات العالمية لتعقب وتقويض الخصوم، وهو ما يثير مخاوف خبراء أمن الحاسوب. [٣]

تاسعاً ـ الأمن الإلكتروني والأمن القومي:

يمكن تعريف الأمن الإلكتروني بأنه «أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالأنترنت؛ وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها أو الالتزام بها لمواجهة التهديدات ومنع التعديات أو على الأقل الحد من اثارها [٤]؛ومن ثم تظهر أهمية تضمين الأمن الإلكتروني في تعريف الأمن القومي؛وما يتضمنه من مخاطر تتعلق بالسيادة والاستقلالية الاقتصادية والهوية الثقافية وكل ما من شانه تعريض الامن القومي للخطر؛ وتحديد من له الحق فى الوصول إلى البيانات والمعلومات ومن له الحق فى الالتزام بالكشف أو عدم الكشف عنها ومن له صلاحية الوصول الى الأجهزة الالكترونية أو صيانتها، مع تحديد الإجراءات الرقمية للحفاظ على النظام الأيكولوجي الرقمي المطبق من المخاطر والتجسس الإلكتروني؛ على أن يتم تحديد نطاق الملاحقة القضائية وتوقيع العقوبات الخاصة بجرائم الفضاء الإلكتروني عند الإخلال بمتطلبات الحماية الضرورية لأمن المعلومات والأجهزة الرقمية؛ وكل ما يتصل بالنظام الإيكولوجي الرقمي.

---

(1) Joshua A. Kroll, https://prospect.org/world/cyber-conundrum/تم الاطلاع بتاريخ ٢٨ يوليو ٢٠٢٠

(2) https://www.merriam-webster.com/dictionary/cyberattackتم الاطلاع بتاريخ ٤ اغسطس ٢٠٢٠

(3) Joshua A. Kroll, :Ibid

(٤) منى الأشقر جبور،السيبرانية هاجس العصر. المركز العربي للبحوث القانونية والقضائية.بيروت. ٢٠١٧ص ٢٥.

الخلاصة والنتائج والتوصيات:

تواجه معظم الدول على الصعيد العالمي حالة من ازدياد التحديات الالكترونية التي تنوعت أشكالها وتعددت آثارها، خاصة مع تنامى الهجمات الإلكترونية التي تجد فى الفضاء الإلكتروني محيط تفاعلي لها مما قد يسبب خسائر اقتصادية ومالية كبيرة تهدد النظام الايكولوجي الرقمي؛ حيث أصبحت الهجمات الإلكترونية تشكل تهديداً خطيراً ضد أمن المعلومات والبنية التحتية والاقتصاد الرقمي ، وتمثل جرائم إلكترونية تؤثر على اقتصادات الدول (المخاطرالإلكترونية،التجسس الإلكتروني) وهو الأمر الذي يستدعىإدارة ومواجهة تلك المخاطر ؛ وردع التهديدات الالكترونية بكافة الطرق والوسائل المناسبة؛ من خلال الاهتمام بإدارات المخاطر وتطويرها؛ ووضع نظم تتبع لكل خطر على حدا؛ وتوفير وتبادل كافة المعلومات المتعلقة به وإعداد البيانات الخاصة بالخسائر التي تسبب فيها داخلياً وخارجياً لوضع بدائل مرنه للتعامل مع الأخطار المستقبلة والمحتملة، والاستفادة من التجارب السابقة.

أ- أهم النتائج:

١- النظام الايكولوجي الرقمي يعمل في إطار ديناميكي ومتطور باستمرار؛ يقوم على تفعيل التكامل فى الفضاء الإلكتروني على مستويات الوحدات الإنتاجية والاقتصادية والسياسية والعسكرية والاجتماعية ، وبين الإدارات الداخلية والموردين والأنظمة والتقنيات المستخدمة والشركاء الخارجيين لزيادة تدفق وجمع البيانات ؛ودفع أداء الأعمال لتعزيز النمو الاقتصادي فى كافة المجالات ، ويمتد إلى كافة أوجه الاقتصاد والسياسة (بنية تحتيه ؛ اقتصاد رقمي ، حكومة إلكترونية، حروب الجيل الرابع، ...) والذي يستخدم اساساً المنصات الرقمية والإنترنت أو الهواتف المحمولة أو أجهزة الحاسب المكتبية والمحمولة والأقمار الصناعية.

٢- الهجمات الإلكترونية هي محاولة متعمدة من مهاجم قد يكون فرد أو منظمة أو دولة لاختراق نظام إيكولوجي رقمي لتحقيق فائدة ما من وراء تعطيل شبكة؛ أو تحقيق أهداف اقتصادية واجتماعية أو سياسية، وغالباً ما يستهدف الهجوم الشركات والمنظمات التجارية والوطنية من خلال نشر برامج ضارة (فيروسات) تسفر عن أضرار بعيدة المدى.

٣- تواجه معظم الدول على الصعيد العالمي حالة من ازدياد التحديات، خاصة مع تنامى المخاطر الإلكترونية (التجارة غير المشروعة، والجريمة المنظمة، والتجسس الاقتصادي والجرائم الإلكترونية، والجيل الجديد من الحروب، الارهاب الدولي، انتشار التلوث البيئي والتغييرات البيئة الحادة، وتفشى الامراض والاوبئة (الفيروس التاجي وما يلحق به من محاولات الاحتيال الرقمي وغيرها)؛ إلا أن المخاطر التشغيلية الإلكترونية تأتى فى مقدمة تلك المخاطر.

٤- تتميز المخاطرالإلكترونية بالتنوع والشدة والغموض، وتزداد كلما تسارعت وتطورت وسائل تكنولوجيا الاتصالات والمعلومات؛ وهي تمثل تهديدات عابرة للحدود الدولية تتعلق بالأمن القومي والسيادة الدولية وتعتبر من قبيل الحروب غير تقليدية وهي غير مكلفة وتتعلق بالجانب الهجومي.

٥- تطورت تكنولوجيا الهجمات الإلكترونية (المخاطر الإلكترونية ، التجسس الإلكتروني) وتنوعت أشكالها وتعددت آثارها، وأصبحت تمثل جرائم إلكترونية تمس

الأمن القومي وتؤثر على اقتصادات الدول، وأصبحت تشكل تهديدا خطيراً ضد أمن المعلومات والبنية التحتية والاقتصادات الوطنية.

ب. أهم التوصيات:

١. يجب وضع استراتيجية محددة الأهداف للأمن الإلكتروني وتطوير صناعته محلياً لمواجهة المخاطرا لإلكترونية وتضمينها فى استراتيجيات الأمن القومي.

٢. تعزيز وتنسيق مجالات واجراءات الدفاع الإلكتروني ووضع نظام لتبادل المعلومات عن المخاطر الإلكترونية على المستوى الإقليمي والدولي.

٣. زيادة الاستثمارات الوطنية فى مجال زيادة القدرات الإلكترونية التي يمكن استخدامها لأغراض عسكرية وغير عسكرية ؛ مع أهمية وضع سياسة دفاع إلكتروني ووضع إجراءات مضادة للهجمات الالكترونية واعطائها الأولية فى التنفيذ وتضمينها خطط التنمية.

٤. الاستمرار فى جهود التنمية الاقتصادية وخاصة ما يتعلق بالنظام الأيكولوجي الرقمي (التكنولوجيا والاتصالات والاقتصاد الرقمي والتجارة الالكترونية وغيرها).

٥. الاهتمام بأمن البنية التحتية للاتصالات المحلية والعالمية خاصة فيما يتعلق بالخدمات المالية والمصرفية التي تتم عبر الهواتف والأجهزة المحمولة لتسوية وسداد المعاملات التجارية والمالية تفادياً لمخاطر الاحتيال والتصيد الإلكتروني.

٦. الاهتمام بإدارات المخاطر وتطويرها على مستوى الاقتصاد الجزئي والكلى؛ ووضع نظم تتبع للمخاطر الإلكترونية كل خطر على حدا؛ يتضمن كافة المعلومات المتعلقة به والبيانات الخاصة بالخسائر التي تسبب فيها داخلياً وخارجياً لوضع بدائل مرنه للتعامل مع الأخطار المماثلة والمحتملة، والاستفادة من التجارب السابقة.

٧. وضع سياسات وأطر وأليات الحوكمة فيما يتعلق بالأمن الإلكتروني وتعميمه على القطاعات المعنية.

٨. تحديد الإجراءات الرقمية للحفاظ على النظام الايكولوجي الرقمي من المخاطر والتجسس الإلكتروني؛ على أن يتم تحديد نطاق الملاحقة القضائية وتوقيع العقوبات الخاصة بجرائم الفضاء الإلكتروني.

٩- نشر التوعية بكافة المخاطر المحتملة، وطرق التعامل معها فى حال حدوثها، وكذلك اتخاذ الإجراءات الوقائية وتفاديها.

١٠-استحداث مناهج وتطبيقات دراسية للنظام الإيكولوجي الرقمي واستخداماته فى الفضاء الإلكتروني وسبل الدفاع عنه وتطويره؛ مع تنظيم مزيداً من المؤتمرات العلمية والندوات التعريفية عنه ووضع الاستراتيجيات المناسبة للتعامل معه.

١١- رفع مستوى الوعي بالأمن الإلكتروني لدى الجماهير، خاصة فيما يتعلق بتدفق المعلومات واختراق المواقع والتجسس المعلوماتي؛وترسيخ السلوك الجيد ونشر قيم وثقافة الفضاء الإلكتروني السلمي والأمن على الصعيد العالمي.

The impact of cyber-attacks on the effectiveness of the digital ecosystem

Dr. Ayman Mohamed Ismail

Abstract

Most countries at the global level are facing a state of increasing cyber challenges that have varied forms and effects, especially with the increase in cyber-attacks that find in the cyberspace an interactive environment for them, which may cause great economic and financial losses that threaten the digital ecosystem; As it has become a serious threat against information security, infrastructure and the digital economy, and at the same time it represents electronic crimes that affect the economies of countries (cyber risks, electronic espionage), which calls for the management and confrontation of these risks; Deterring cyber threats in all appropriate ways and means; By taking care of risk management and developing them; Establish systems that monitor each risk separately; With the provision and exchange of all information related to it, and the preparation of data on the losses caused by it, to develop flexible alternatives to deal with potential dangers, and to benefit from previous experiences.

Keywords:

digital ecosystem, cyber-attacks, cyber risks, cyber espionage, cyber risk management.