التداعيات الاقتصادية لحرب المعلومات السيبرانية

The economic implications of the cyber information war

حسين قوادرة[1]، منـى كحلوش[2]

[1] جامعة أم البواقي (الجزائر)، hocine751@yahoo.fr

[2]جامعة سكيكدة (الجزائر)، Kahlouche.mouna41@gmail.com

تاريخ الاستلام: 2021/01/20 تاريخ القبول: 2021/04/07 تاريخ النشر: 2021/04/30

ملخص:

أدت التغيرات التكنولوجية إلى إحداث ثورة في الشؤون الاقتصادية والعسكرية بإدخال أسلحة ذكية وإضافة أبعاد جديدة في فن الحرب. وبذلك أصبحت الأنشطة الاقتصادية والعسكرية تعتمد بشكل متزايد على الإنترنت والتقنيات الشبكية. ومع ذلك أدت هذه التطورات والترابط بين شبكات البنى التحتية الحيوية إلى ظهور تهديدات سيبرانية جديدة، وتنامي الهجمات الإلكترونية في سياق الحرب السيبرانية. ولهذا السبب تقوم العديد من الدول بتطوير قدرات دفاعية وهجومية بهدف تعزيز وتسريع عملية الأمننة، بما من شأنه أن ينعش سوق الأمن السيبراني في المستقبل.

كلمات مفتاحية: الحرب السيبرانية، الأمن السيبراني، الحرب اللاتماثلية، الاقتصاد الرقمي، سوق الأمن السيبراني

Abstract:

Technological changes have revolutionized economic and military affairs by introducing smart weapons and adding new dimensions to the art of war. As a result, economic and military activities have become increasingly dependent on the Internet and networking technologies. However, these developments and the interconnectedness of vital infrastructure networks have given rise to new cyber threats, and the growth of cyber attacks in the context of cyber war. For this reason, many countries are developing defensive and offensive capabilities with the aim of strengthening and accelerating the security process, which would revive the cybersecurity market in the future.

Keywords: cyber warfare, cybersecurity, asymmetric warfare, digital economy, cybersecurity market

المؤلف المرسل: حسين قوادرة، **الإيميل:** hocine751@yahoo.fr

مقدمـــــة:

أثرت التغيرات التكنولوجية السريعة – التي ميزت المجتمعات ما بعد الصناعية– على القطاع العسكري محدثة ثورة في الشؤون العسكرية. ففي أوائل التسعينيات، وبعد انتهاء الحرب الباردة، تم تعزيز التطبيقات التكنولوجية في الجيش من خلال إدخال الأسلحة الذكية التي أضافت أبعاد جديدة لفن الحرب. فباعتبار أن الإنترنت تمثل الأداة الرئيسية لمجتمع المعلومات، والتي نتجت عن سلسلة من التحقيقات العسكرية، إذ يرجع ظهورها إلى رغبة سلطات الولايات المتحدة الأمريكية في امتلاك نظام اتصالات قادر على مقاومة الحرب النووية من الاتحاد السوفيتي. وبالتالي لعبت هذه المبادرة دورًا حيويًا في إنشاء شبكة أربانيت Arpanet باعتبارها الأساس لشكل الإنترنت الحالي.

يتميز مجتمع المعلومات بالاستخدام الواسع للإنترنت من قبل شريحة متزايدة من السكان، إذ أصبحت الأنشطة الاقتصادية والعسكرية تعتمد بشكل متزايد على تقنيات الإنترنت والشبكات. وقد بلغ عدد مستخدمي الإنترنت 2.8 مليار مستخدم في جميع أنحاء العالم في عام 2014 ليصل عددهم إلى 3.8 مليار مستخدم في 2018،[1] ومن المتوقع أن يتزايد عددهم خلال السنوات القادمة، حيث أصبح الولوج إلى الإنترنت أولوية أساسية، ومع ذلك فإن الوصول إلى التكنولوجيا من شأنه زعزعة التوازن الجيوبوليتيكي.

أدى إدخال التكنولوجيا في الصناعة والترابط بين شبكات البنى التحتية الحيوية إلى مخاطر وتهديدات سيبرانية جديدة، مع تصاعد الهجمات السيبرانية أو الحرب السيبرانية. فعلى سبيل المثال في عام 2007 كانت الحكومة الإستونية ضحية لهجمات سيبرانية واسعة النطاق، مما أدى إلى انقطاع خدمات الدولة عن العمل، وبعد مرور عام أصبحت الحكومة الجورجية الضحية التالية لمثل هذه الهجمات السيبرانية، حيث قام القراصنة (الهاكرز) بمنع إقلاع طائرة عسكرية وتسببوا في مشاكل الوصول إلى المواقع الإعلامية الرسمية والوزارات والهيئات العامة. سلطت هذه الحقائق الضوء على نية تعطيل أو تدمير أنظمة المعلومات والاتصالات لدى العدو ونقاط الضعف الناشئة عن الترابط بين أنظمة الكمبيوتر، وبالتالي فإن ظهور الحرب السيبرانية هو تتويج للاستخدام الموسع للتكنولوجيا.

لذلك يهدف هذا المقال إلى إبراز الآثار الاقتصادية المحتملة لمختلف التهديدات الناتجة عن عمليات الفضاء السيبراني، خصوصا في ظل تنامي سوق الأمن السيبراني وسعي الدول نحو أمننة الفضاء السيبراني

لحماية المجال الاقتصادي. وستتم معالجة الموضوع من خلال طرح الإشكالية التالية: ما هي مختلف الآثار الاقتصادية الناجمة عن حرب المعلومات السيبرانية، وهل يمكن تجاوزها؟

فرضية البحث: كلما تم التعامل مع الحرب السيبرانية وفق منطق التكلفة–العائد كلما تم التحكم في الآثار الاقتصادية الناجمة عنها.

المنهج المتبع: سيتم إتباع كل من المنهج الوصفي–التحليلي والمنهج الاستنباطي:

– المنهج الوصفي –التحليلي: الذي يستعمل للكشف عن ماهية الظاهرة ومختلف الظواهر المرتبطة بها، حيث تقوم الدراسة باستعراض مفهوم الحرب السيبرانية، ومختلف تداعياتها الاقتصادية على الدول.

– المنهج الاستنباطي: من خلال دراسة الحرب السيبرانية في سياق كل من حقل العلاقات الدولية والاقتصاد الكلي.

تقسيم الدراسة: ويستعرض القسم الأول دراسة الطبيعة اللاتماثلية لحرب المعلومات السيبرانية مع تسليط الضوء على نماذج مختارة لهجمات سيبرانية. أما القسم الثاني فتناول الآثار الاقتصادية المترتبة عن إجراءات الحرب السيبرانية.

أولا: حرب المعلومات السيبرانية كمصدر تهديد للاقتصاد الرقمي

يحاول هذا الجزء تسليط الضوء على نوع جديد من الحرب التي تقع ضمن نطاق المجال السيبراني والتي تسمى بالحرب السيبرانية. ففي نطاق الاقتصاد الرقمي كانت هناك العديد من الهجمات السيبرانية التي استهدفت الأمن القومي لعدة دول، والتي جعلت من الحروب المعلوماتية كمصدر تهديد متنامي للمجال الاقتصادي.

1. الطبيعة اللاتماثلية لحرب المعلومات السيبرانية

اختلفت التعريفات الخاصة بمصطلح الحرب السيبرانية بسبب اختلاف وجهات نظر الباحثين والجهات المهتمة بهذه الظاهرة، فيعرّف Gartzke الحرب السيبرانية بأنها ذلك الصراع الذي يتم خوضه حصريًا في الفضاء السيبراني[2]. يعتبر هذا التعريف مقيد لأنه لا يشمل الدعاية والتجسس وزعزعة استقرار النظام المالي للدولة والنتائج النفسية المحتملة التي قد تحدث. ووفقًا لتعريف آخر أقل تقييدًا، فإن البعد العسكري للحرب

السيبرانية يتسع ليشمل مجالات وتهديدات غير عسكرية[3]. وبالتالي فهو شكل من أشكال الحرب المعلوماتية التي تم تطويرها في الفضاء السيبراني، ويمكن أن تشمل الحرب السيبرانية زعزعة استقرار الأنظمة المالية والبنية التحتية الحيوية للحكومة، من خلال التسلل إلى نظام الكمبيوتر لأغراض التجسس، ويتعلق الأمر بالتخريب للحصول على المعلومات والوصول إلى أنظمة الكمبيوتر الهامة، وكذلك المعلومات الخاطئة عن طريق استخدام الأسلحة الإلكترونية والقيام بتدخلات هجومية عبر الفضاء الإلكتروني. كما تعرّف الحرب الإلكترونية على أنها "أعمال تقوم بها دولة قومية لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى لأغراض التسبب في الضرر أو التعطيل"[4]، ولكن هناك تعريفات أخرى تشمل أيضًا الأعمال السيبرانية التي تقوم بها الفواعل غير الحكومية، مثل الجماعات الإرهابية والشركات والجماعات السياسية أو الإيديولوجية المتطرفة، ونشطاء القرصنة الإلكترونية، والمنظمات الإجرامية عبر الوطنية لتحقيق أهدافهم الخاصة.[5]

في الواقع تشير الحرب السيبرانية إلى حالات الصراع المتماثل بين دولتين أو أكثر، وكذلك إلى حالات الصراع غير المتماثل بين الدولة وواحدة أو أكثر من الفواعل غير الحكومية، إذ يوفر هذا البعد غير المتماثل قوة غير متناسبة لأي نوع من الفواعل مقارنة بقوى الصراع التقليدي. وتُعرِّف مؤسسة RAND الحرب غير المتماثلة بأنها "صراعات بين الأمم أو الجماعات التي لديها قدرات واستراتيجيات عسكرية متباينة[6]، فدمج العمليات السيبرانية مع العمليات الأرضية والبحرية والجوية والفضائية، يمكن أن يزود الدول التي تعاني من ضعف معداتها العسكرية وعدد الأفراد بعدم تماثل يعوض هذه النقائص.[7]

من الناحية العملية وعلى عكس الحرب التقليدية، يمكن لفاعل أو مجموعة من الفواعل المعزولين قيادة هجوم سيبراني، كما يمكن شن هجمات الفضاء السيبراني من قِبل دولة ضد دولة أخرى، أو من قِبل دولة واحدة ضد البنى التحتية الحيوية لأمة أخرى.

تعتبر تكلفة الهجمات الإلكترونية أقل بكثير من تكلفة الحرب التقليدية. ومع ذلك، يتطلب العمل في الفضاء الإلكتروني امتلاك بنية أساسية وأدوات تقنية وخبرة فنية، وبالتالي توفير الأصول المالية اللازمة للقيام بجميع العمليات السابقة. علاوة على ذلك يمكن أن تحدث الحرب السيبرانية في أي وقت ولا تعلن الدول ذلك. فالفعل المفاجئ واستخدام الأعمال الخبيثة (فيروس حصان طروادة) يكشف عن نوع من الهجوم، وهو تطبيق لمسلمات "صن تزو" المتعلقة بفن الحرب. بالإضافة إلى ذلك، هناك عقبات كبيرة أمام الإسناد التقني والإسناد البشري، إذ يشير الإسناد التقني إلى تحليل الوظائف الخبيثة والملفات الضارة لتحديد موقع العقدة الأولية لهذا الهجوم. أما الإسناد البشري فيشير إلى تحديد الأشخاص أو المؤسسات باستخدام

نتيجة الإسناد التقني والمعلومات الأخرى[8]. ومع ذلك فتحديد هوية المخترقين أمر مستحيل عملياً، حيث يظل المتسللون مجهولون وآمنون قانونيًا[9]، ولا يوجد أي حافز لأي شخص معني بالشفافية باعتبار أن مهاجمة العدو دون أن يكون مرئيًا هو تطبيق واضح لقواعد Sun Tzu.

ومع ذلك فإن الجهود التي تبذل في أوروبا تهدف أساسا إلى قياس وتيرة وبلدان المصدر للهجمات السيبرانية ورصد محاولات الاختراق. ففي هذا الصدد أنشأت شركة الاتصالات الألمانية (Deutsche Telekom (DTAG شبكة من المستشعرات (97 مستشعرا) لتكون بمثابة نظام إنذار مبكر لتقديم صورة في الوقت الحقيقي للهجمات الإلكترونية المستمرة، حيث يتم إدراج البلدان "الخمسة عشر الأولى" التي تم تسجيلها كمصدر للهجمات الإلكترونية بواسطة أجهزة الاستشعار[10] .

هناك خصوصية رئيسية أخرى لهذا الشكل الجديد من الحروب متمثلة في أن الحرب السيبرانية تحدث في الفضاء السيبراني، وبالرغم من عدم تحقيقها في منطقة جغرافية محددة ولكن يمكن أن تحدث عدم الاستقرار الجيوسياسي. ففي هذا النوع من الحرب تعتبر السيطرة على المعلومات ذات أهمية كبرى. وبالتالي تميل الدول المتقدمة تكنولوجياً إلى السيطرة على الفضاء السيبراني. لذلك مع تزايد نقاط ضعف الدول أمام الحرب السيبرانية فإن التدابير ضرورية لصد مختلف الهجمات.

2. نماذج مختارة للهجمات السيبرانية

في عام 2007، وقعت الحكومة الإستونية ضحية لهجمات سيبرانية واسعة النطاق، مما أدى إلى توقف عمل خدمات الدولة، حيث أفضت إزالة الحكومة الإستونية لتمثال الجندي البرونزي وجثث جنود الجيش الأحمر في الحرب العالمية الثانية من حديقة عامة في العاصمة "تالين" إلى هجوم إلكتروني قامت به كل من روسيا والأقلية الروسية في البلاد[11]، وتسبب هذا الهجوم في حدوث خلافات بين الإستونيين والروس، وفي وقت لاحق شهدت إستونيا الموجة الأولى من هجمات الحرمان من الخدمة (DDoS) مؤدية إلى إغلاق المواقع الإلكترونية لكل من: الوزارات الحكومية، مصرفين رئيسين، والعديد من الأحزاب السياسية[12].

خلال الهجوم السيبراني المفاجئ على إستونيا عام 2007 تأثرت مواقع الوكالات الحكومية[13] وبعد ذلك تم ضرب المواقع الخاصة والخوادم والبنوك والصحف. على الرغم من عدم وجود خسائر بشرية غير أن الإغلاق المطول للخدمات العامة تسبب في اضطرابات في الاقتصاد الإستوني، وكان لذلك تأثير على البنية

التحتية المدنية وأثّر على السكان الإستونيين من خلال التسبب في العديد من الاختلالات. علاوة على ذلك تم تسليط الضوء على مدى ضعف الشبكات والشكل الجديد من أشكال التهديد للأداء السليم للنظام الاقتصادي والاجتماعي. وبالتالي فإن هذا هو أول هجوم سيبراني واسع النطاق، وبالرغم من أنه لا أحد يتحمل مسؤولية هذا الهجوم السيبراني، غير أن هناك شكوك في تورط السلطات الروسية وراء هذه العملية.

بعد ذلك في عام 2008 تعرضت شبكة جمهورية جورجيا لهجوم سيبراني، إذ نفذت هجمات "تعطيل الخدمة" DDoS عن طريق شبكة مكونة من مئات أجهزة الكمبيوتر المصابة بالفيروسات (أجهزة كمبيوتر تم اختراقها) والتي أصيبت بالبرامج الضارة، حيث يسمح البرنامج الضار لخادم "التحكم والمراقبة" في الكمبيوتر بإصدار أوامر لهذه الروبوتات[14].

تم تنسيق الهجمات الإلكترونية بشكل مباشر مع هجوم حركي بحري وجوي، حيث أجبر قراصنة الإنترنت طائرة عسكرية على إلغاء الإقلاع، كما استهدفت هذه الهجمات الإلكترونية أيضًا التشغيل السلس للبنية التحتية الحيوية، واستهدفت مواقع وسائل الإعلام الرئيسية والمواقع الحكومية والمؤسسات العامة والمؤسسات المالية والتعليمية وجمعيات الأعمال، حيث كان الوصول إليها مستحيلاً، لأن هذه الهجمات استهدفت منظومة القيادة والمراقبة. بالإضافة إلى هذان الاعتداءان هناك العديد من الاعتداءات السيبرانية المبينة في الجدول التالي:

الجدول 01: توصيف لهجمات إلكترونية مختارة

السنة	مصدر الهجوم	الجهة المستهدَفة	لمحة عن الهجمة السيبرانية
2007	روسيا (المزعومة)	إيستونيا	مجموعة من الهجمات الإلكترونية ضد الوكالات الحكومية الإستونية، وضد المواقع والخوادم الخاصة
2007	الصين (المزعومة)	المملكة المتحدة، فرنسا، ألمانيا	عمليات اختراق للشبكات الحكومية
2008	القراصنة القوميون الروس	ليتوانيا	اختراق مئات المواقع الحكومية الليتوانية، ومواقع الشركات

2008	روسيا	جورجيا	هجوم سيبراني منسق مباشرة مع هجوم بري وبحري وجوي
2009	روسيا (المزعومة)	قيرغيزستان	ركزت الهجمات الإلكترونية على مزودي خدمة الإنترنت في قيرغيزستان مما يعطل حركة تدفق المعلومات على الإنترنت
2009–2010	مجهول	إيران	Stuxnet"، دودة إلكترونية، مصممة خصيصًا لتخريب المفاعلات النووية الإيرانية
2012	مجهول	شركة النفط الحكومية السعودية	أصاب فيروس شرمون 30000 جهاز كمبيوتر لشركة النفط السعودية "أرامكو"
2012	مجهول	قطر	فيروس شرمون (شركة النفط رأس غاز القطرية)

"المزعوم": تشير إلى صعوبة التحقق من الجهة المسؤولة عن الهجوم السيبراني.

Source : Flowers and Zeadally, Op.cit, p.p 17-18.

تثبت هذه الكوارث السيبرانية التي تستهدف الدول أن هناك فعلا تهديدا حقيقيا يواجهها فالهجمات السيبرانية على الأنظمة الحكومية والمدنية تحرض الدول على التفكير في استراتيجيات الأمن السيبراني، فتنامي خطر حرب المعلومات السيبرانية دفع منظمة حلف شمال الأطلسي (الناتو) إلى تبني سياسة للدفاع السيبراني، والتي بموجبها أنشأت هيئة لإدارة الدفاع السيبراني ودعمت إنشاء مركز تعاوني للدفاع السيبراني في تالين[15].

ثانيا: الآثار الاقتصادية المترتبة على حرب المعلومات السيبرانية

يتضمن الأمن السيبراني القدرة على التحكم في الوصول إلى أنظمة الشبكة والمعلومات التي تحتوي عليها، كما يعني أيضًا القدرة على الحفاظ على سرية الفضاء الإلكتروني وسلامته وتوافره، وضمان حماية أنظمة الكمبيوتر والبيانات من التداخل عبر الإنترنت. وبالتالي قد يكون لانعدام الأمن السيبراني تأثير على الاقتصاد ككل، لذلك ينطوي الأمن السيبراني على أبعاد أمنية وطنية ودولية.

1. مؤشر الأمن السيبراني العالمي

يشير الأمن السيبراني إلى حماية الشبكات وأنظمة المعلومات من الأخطاء البشرية أو الكوارث الطبيعية أو الأعطال الفنية أو الهجمات الضارة"[16]، كما أنه ينطوي على حماية الهجمات ومنع انتشار التهديدات السيبرانية، فهو مرتبط بالبرامج السياسية الوطنية والدولية والبنية التحتية للاتصالات باعتبار أن هذه الهجمات موجهة على وجه التحديد، وتندرج تحت عنوان حرب المعلومات ولها تأثير على سلاسل الإمداد والنقل والإمداد الآلي.

تنعكس هواجس الأمن السيبراني على الجهود التي تبذلها عدة دول من أجل تحديد مستوى الأمننة في الفضاء الإلكتروني. وفي هذا السياق ظهر مؤشر الأمن السيبراني العالمي باعتباره مبادرة تحاول قياس التزام البلدان بالأمن السيبراني بهدف المساعدة في تعزيز ثقافة الأمن السيبراني العالمية وتكاملها في صميم تكنولوجيات المعلومات والاتصالات[17]. إذ يقدم مؤشر الأمن السيبراني العالمي (GCI) لمحة عامة عن مستوى تطورات الأمن السيبراني في دول العالم بالتركيز على: التدابير القانونية، التدابير التقنية، التدابير التنظيمية، بناء القدرات والتعاون الدولي.

توفر التدابير القانونية إطارًا منسقًا للهيئات من أجل الامتثال للمتطلبات التنظيمية المشتركة والحد من التهديدات الإلكترونية، وتشكل التكنولوجيا دفاعًا أساسيًا ضد التهديدات السيبرانية عبر شبكة الأنترنت، أما للتدابير والميزات التقنية يمكنها اكتشاف الهجمات السيبرانية ومواجهتها من أجل الحد من ضعف الدول مثل فريق مواجهة الطوارئ الحاسوبية* CERT.

كما يتم إنشاء مؤشرات تهدف إلى تطبيق معايير الأمن السيبراني المعترف بها دوليًا في القطاع العام والبنية التحتية الحيوية، وتعتبر التدابير التنظيمية والإجرائية أساسية لتطوير استراتيجيات التنظيم والتعاون، إذ تُستخدم هذه التدابير لتنفيذ كل نوع من المبادرات الوطنية بشأن الأمن السيبراني. علاوة على ذلك يتعلق بناء القدرات بتنمية قدرات الأفراد على اعتماد تدابير قانونية وتقنية وتنظيمية حول الأمن السيبراني. إضافة إلى أن معرفة القوى العاملة بالتكنولوجيا أمر ضروري، لأن بناء القدرات البشرية والمؤسسية مفيد لتحسين المعرفة والدراية الفنية عبر القطاعات، ومن أجل لتطبيق الحلول الأكثر ملاءمة، وتعزيز تقدم كفاءات المهنيين كما يتضمن الأمن السيبراني نهج أصحاب المصلحة المتعددين. وأخيرًا ومن أجل حوار وتنسيق أفضل، يعد

التعاون شرطًا أساسيًا، كما أن تبادل المعلومات مفيد في القطاعين العام والخاص، وعلى الصعيدين الوطني والدولي أيضًا.

يقدم هذا المؤشر تصنيفًا عالميًا للأمن السيبراني لكل بلد، وقد تشترك العديد من الدول في نفس الترتيب مما يدل على أن لديهم نفس المستوى من الاستعداد. ويتراوح المؤشر بين 0 و 1 إذ يشير العدد القريب من 1 إلى أن البلد آمن، بمعنى آخر يعد الأمن السيبراني عاليًا مع مراعاة المعايير المذكورة أعلاه. على سبيل المثال تقدم كل من الولايات المتحدة وكندا وأستراليا المؤشر الأعلى: 0.824؛ 0.794 و 0.765 على التوالي، بينما بلدان مثل فرنسا (0.588) وإسبانيا (0.588) وإيطاليا (0.559) تعتبر في حالة متوسطة. وتأتي اليونان في المرتبة 22، بينما توجد دول أخرى في وضع أقل. (أنظر الجدول 2).

الجدول 2: مؤشر الأمن السيبراني والترتيب المرتبط به في دول المختارة

الدولة	المؤشر	الترتيب	الدولة	المؤشر	الترتيب
الولايات المتحدة	0.824	1	السنغافورة	0.676	6
كندا	0.794	2	لاتيفيا	0.647	7
استراليا	0.765	3	السويد	0.647	7
ماليزيا	0.765	3	تركيا	0.647	7
عمان	0.765	3	هونج-كونج	0.618	8
نيوزيلندا	0.735	4	فنلندا	0.618	8
النرويج	0.735	4	قطر	0.618	8
البرازيل	0.706	5	سلوفاكيا	0.618	8
استونيا	0.706	5	الأورجواي	0.618	8
ألمانيا	0.706	5	كولومبيا	0.588	9
الهند	0.706	5	الدانمارك	0.588	9
اليابان	0.706	5	مصر	0.588	9
جمهورية كوريا	0.706	5	فرنسا	0.588	9

المملكة المتحدة	0.706	5	موريتانيا	0.588	9
النمسا	0.676	6	اسبانيا	0.588	9
المجر	0.676	6	ايطاليا	0.559	10
اسرائيل	0.676	6	المغرب	0.559	10
هولندا	0.676	6	قبرص	0.294	19
			اليونان	0.206	22

Source : International Telecommunication Union (ITU), Op.cit, p.p 1-3.

الجدول 3: معايير مؤشر الأمن السيبراني في دول مختارة

الدول	تدابير قانونية	تدابير تقنية	تدابير تنظيمية	تدابير بناء القدرات	تدابير تعاونية
الولايات المتحدة	1.0000	0.8333	0.8750	1.0000	0.5000
كندا	0.7500	1.0000	0.8750	0.8750	0.5000
البرازيل	0.7500	0.6670	0.870	0.7500	0.5000
استونيا	1.0000	0.6670	1.0000	0.5000	0.5000
ألمانيا	1.0000	1.0000	0.6250	0.6250	0.5000
المملكة المتحدة	1.0000	0.6670	0.7500	0.7500	0.5000
إسرائيل	1.0000	0.6670	0.6250	0.7500	0.5000
السويد	0.7500	0.6670	0.6250	0.6250	0.6250
تركيا	0.5000	0.6670	0.7500	0.7500	0.5000
الدانمارك	1.0000	0.6670	0.5000	0.5000	0.5000
فرنسا	1.0000	0.1667	0.5000	0.7500	0.6250
اسبانيا	1.0000	0.6670	0.6250	0.6250	0.2500
ايطاليا	0.7500	0.3333	0.6250	0.6250	0.5000

بولندا	1.0000	0.3333	0.6250	0.6250	0.2500
سويسرا	0.5000	0.3333	0.2500	0.2500	0.5000
قبرص	0.7500	0.1667	0.3750	0.1250	0.2500
البرتغال	0.7500	0.5000	0.1250	0.1250	0.2500
ألبانيا	0.7500	0.3333	0.1250	0.1250	0.0000
اليونان	0.5000	0.3333	0.1250	0.1250	0.1250

Source : International Telecommunication Union (ITU), Op.cit, p.p 9-15.

من خلال الجدول رقم 3 وعند دراسة مكونات مؤشر الأمن السيبراني العالمي على نطاق واسع يبدو التعاون طموحًا بحيث يتحقق بنسبة 100٪ لجميع البلدان. على سبيل المثال تم الكشف عن أعلى مؤشر لتدابير بناء القدرات بين كل من الولايات المتحدة الأمريكية (1.0000)، وكندا (0.8750)، والبرازيل (0.7500)، والمملكة المتحدة (0.7500)، وإسرائيل (0.7500). أما ما تعلق بالتدابير التنظيمية فإن أعلى مؤشر واضح في إستونيا (1.0000). وفيما يتعلق بالتدابير الفنية فإن المركز الأول في القائمة الإجمالية لكل من كندا (1.0000) وألمانيا (1.0000). وأخيرًا هناك مستويات عالية من مؤشر التدابير القانونية (حوالي 1.0000) تدعم الولايات المتحدة الأمريكية وإستونيا وألمانيا والمملكة المتحدة وإسرائيل والدنمارك وفرنسا وإسبانيا. أما اليونان في وضع معتدل فيما يتعلق بالتدابير القانونية (0.5000) والتقنية (0.3333)، وبذلك ينبغي بذل الجهود لتحسين التدابير التنظيمية (0.1250)، وبناء القدرات (0.1250)، وتدابير التعاون (0.1250).

2. تطوير المنتجات والخدمات في سوق الأمن السيبراني

تؤثر الزيادة في الطلب على السلع والخدمات في مجال الأمن السيبراني على شركات إنتاج الأسلحة والخدمات العسكرية وتؤدي إلى ظهور ما يعرف بسوق الأمن السيبراني.

يتضمن سوق الأمن السيبراني تطوير المنتجات والخدمات للتطبيقات الهجومية والدفاعية، حيث تركز هذه التطبيقات على النشاط الحكومي والعسكري، ويشار إليها أيضًا باسم الأسلحة الإلكترونية. كما يتكون

قطاع الأمن السيبراني من الشركات التي توفر المنتجات والخدمات للاستخدام الهجومي والدفاعي عبر تكنولوجيا المعلومات والاتصالات والمجال الصناعي.

ومع الأخذ في الاعتبار الأهمية المتزايدة للأمن السيبراني تعمل صناعة الأسلحة والخدمات في سوق الأمن السيبراني بهدف تغطية هذه الاحتياجات، وتبرز في هذا الإطار مجموعة من النماذج على غرار: Airbus Defense & Space وBEA Systems وLockheed Martin وSaab وThales والتي تنوعت في مجال الأمن السيبراني من أجل توسيع نطاق إنتاجها وقاعدة عملائها في القطاع المدني وتطوير الكفاءات التقنية للسوق العسكرية.

قدمت تقريبا نصف شركات الأسلحة والخدمات التابعة لمعهد ستوكهولم الدولي لبحوث السلام SIPRI أفضل 100 حلول للأمن السيبراني[18]، وأصبحت شركات مثل Symantec و Intel Corporation وIBM من أهم مزودي خدمات الأمن السيبراني في وقت كانت فيه تخفيضات مهمة في النفقات العامة، وقد أثرت هذه التخفيضات أيضا على أسواق الأسلحة التقليدية، إذ يغطي الأمن السيبراني لصناعة الأسلحة أربع (4) مجالات رئيسية: برامج وخدمات حماية البيانات والشبكات، خدمات الاختبار والمحاكاة، خدمات التدريب والاستشارات، والدعم التشغيلي.

تجدر الإشارة إلى أنهم طوروا استراتيجيات مختلفة، وقد شملت إستراتيجية التنويع الخاصة بهم التعاون مع الشركات غير العسكرية. فمن جهة تتعاون شركة BAE مع شركة Vodafone لتحسين الأمن في مجال الاتصالات، كما أقامت شركة Lockheed Martin تحالفات إستراتيجية مع شركات تكنولوجيا المعلومات وأمن الإنترنت (Microsoft، Hewlett Packard)، وكان هناك تعاون بين العديد من الشركات المصنعة للحلول الأمنية السيبرانية في الولايات المتحدة مثل Lockheed Martin وIBM من أجل تعزيز بوابات الإنترنت الخاصة بهم ضد الهجمات الإلكترونية. وعلى الجانب الآخر أنشأت إيرباص للدفاع والفضاء قطاعًا متخصصًا في مجال الأمن السيبراني شارك فيه أكثر من 600 خبير في أوروبا (فرنسا، المملكة المتحدة، ألمانيا)، كما يخصص قطاع الأمن السيبراني الأوروبي عائدات سنوية معتبرة للاستثمار في البحث والتطوير.

علاوة على ذلك يمكن أن يسهم الأمن السيبراني من منظور اقتصادي في استخدام أدوات تحليل التكلفة في اتخاذ القرارات في سياق إدارة المخاطر، والتي تهدف إلى تحديد حجم الاستثمار في الأمن السيبراني حسب التكلفة المتوقعة[19].

3. احتمالات فشل سوق الأمن السيبراني

تتبلور الجوانب الاقتصادية للأمن السيبراني من خلال نمذجة الهجوم والدفاع، فالنظر إلى الأمن السيبراني من منظور اقتصادي يمكن أن يقدم رؤية مهمة في تحديد الفرص المهمة المتاحة في مجال السياسة العامة. علاوة على ذلك يمكن تطبيق الأدوات القياسية للاقتصاد الجزئي على تحليل نتائج تقييم السياسات لتحقيق قدر أكبر من الأمن السيبراني. في هذا السياق تثار أسئلة من قبيل معرفة مقدار ما ينبغي للمجتمع أن ينفقه على الأمن السيبراني، وما إذا كانت القرارات التي يتخذها المنتجون والمستهلكون من القطاع الخاص ستؤدي على الأرجح إلى الحد الأمثل اجتماعيًا للأمن السيبراني، لكن بعض صانعي السياسة يشككون في قدرة السوق السيبراني على توفير ما يكفي من الأمن السيبراني.

تشير الأدبيات المستفيضة في الاقتصاد العام إلى الحالات التي ستفشل فيها الفوائد والتكاليف في الأسواق الخاصة في حساب جميع الفوائد والتكاليف الاجتماعية، وقد ينشأ هذا الموقف في سوق الأمن السيبراني، ففي مجال الاقتصاد العام غالبًا ما يُعتبر الأمن السيبراني بمثابة منفعة عامة، لأنه يقدم بعض الخصائص المحددة مثل خاصية عدم الاستبعاد وعدم التنافس في الاستهلاك. هذه الخصائص يمكن أن تخلق بدورها حوافز للمستفيدين المحتملين من هذه السلع للعمل كمنتفعين متطفلين بالمجان، وهذا الأمر يعكس فشل السوق الكلاسيكي الذي يدعو إلى تدخل الحكومة والتنظيم الحكومي. بمعنى آخر توجد حواجز اقتصادية أمام تحسين الأمن السيبراني، ففي حالة ما إذا كانت الاستثمارات الخاصة في الأمن السيبراني أقل من الفوائد الاجتماعية، مما يؤدي إلى ترك الأمن السيبراني إلى السوق، وبالتالي سيفضي ذلك إلى انخفاض الاستثمار في الأمن السيبراني.

يتعامل الفشل المحتمل للسوق في مجال الأمن السيبراني مع العوامل الخارجية للشبكات، وعدم تناسق المعلومات، وحوافز الانتفاع المجاني، وجوانب السلع العامة للاستثمار الأمني الخاص، وفشل التنسيق.

فإذا كان مستخدم الإنترنت محميًا بدرجة كافية ضد الهجمات السيبرانية، فمن غير المرجح أن يتم اختراق جهاز الكمبيوتر الخاص به. وبالتالي يمكننا استنتاج أن هذا له تأثير إيجابي على المستخدمين الآخرين، وكذلك يقلل من احتمال انتقال الفيروسات وغيرها من المخاطر السيبرانية، وبالتالي فالموقف السابق يتوافق مع شبكة خارجية إيجابية ويمكن أن يؤدي إلى مشكلة الانتفاع المجاني. وتجدر الإشارة أنه يتم اكتشاف

مشكلة الانتفاع المجاني عندما يمكن للمرء الاستفادة من سلعة أو خدمة دون دفع ثمنها، وعلى العكس من ذلك فإن انعدام الأمن يخلق عوامل خارجية سلبية. وبالتالي يتأثر الأمن السيبراني بتدابير الأمان المستخدمة من قبل جميع مستخدمي الإنترنت، وهذا هو حال السلع العامة نظرًا لأن العوامل الخارجية أو الاستثمار في الحماية أو الأمن السيبراني يقلل من خطر الهجوم السيبراني[20].

زيادة على ذلك يتميز سوق الأمن السيبراني بعدم اتساق المعلومات التي تمنع اتخاذ القرار الأمثل، ومثل هذه الحالات تخلق مشاكل محتملة[21]. باعتبارها تنتج حواجز ضد تحسين الأمن السيبراني، فيمكن القول أنه توجد معلومات غير متماثلة عندما يكون لدى أحد أطراف الصفقة معلومات أفضل من الناحية النوعية مقارنة بالطرف الآخر. بمعنى آخر، يكون أحد أطراف المعاملة أكثر إطلاعًا من الطرف الآخر. وفي هذه الحالة تكون المعلومات المتعلقة بالجودة غير مكتملة، ويتم توزيعها بشكل غير متماثل. فمن ناحية يتردد المشترون في دفع ثمن شيء لا يمكنهم قياسه، لأنه من الصعب على المشتري معرفة حقيقة جودة المنتج، ومن ناحية أخرى يمتنع المنتجون أو البائعون عن الاستثمار في الأمن السيبراني، لكنهم يقولون دائمًا أن منتجاتهم آمنة، وهذا الوضع يمكن أن يؤدي إلى نقص الاستثمار في الأمن السيبراني، ومع ذلك يتم إنشاء المعايير من أجل التصديق على جودة المنتج، ولكن مرة أخرى في الممارسة العملية سيتعين على البائعين تحمل هذا التقييم وهذا يمكن أن يدفع بالحوافز ذات الآثار السلبية.

ونظرًا لأن التعرف على مستخدمي الإنترنت أمر مستحيل، فعند حدوث هجوم عبر الإنترنت، لا يمكن تحدي الجهة المسؤولة قانونيًا عن هذا الهجوم في الواقع. لذلك من الصعب جدًا وصف الهجمات السيبرانية، ومن الصعب قياس آثارها. فبسبب العوائق التي تعترض عملية الإسناد، يرى أي شخص أنه ليس لديه مصلحة شخصية أو حوافز كافية لحماية الكمبيوتر، ويتجاهل الحماية ويتجنب تكلفة هذا الإجراء، وفي المقابل يشكل حوافز للانتفاع المجاني. كما يتم فرض ضغوط كبيرة على الأمن السيبراني نظرًا لوجود نقص في اللوائح والتشريعات الدولية التي يمكن أن تتحكم في استخدام القوة في الفضاء السيبراني فضلاً عن ردع وإسناد الهجمات السيبرانية[22].

تشكل إخفاقات التنسيق مشكلة في الاقتصاد يمكن نمذجتها وفق نظرية اللعب، إذ يمكن صياغة الحوافز التي تواجه المستخدم الفردي مثلما هو الحال مع معضلة السجين، فالأسباب السلوكية المتوقعة التي من خلالها قد لا يفترض من فواعل السوق أن تستثمر في مستويات الأمان المثلى اجتماعيًا من شأنها إبراز

سبب فشل السوق في توفير الأمن السيبراني. فتحليل عائدات الاستثمار في الأمن السيبراني تشبه معضلة السجين، التي تعتبر مثالا بسيطا ينطبق على العديد من المواقف التي تتصارع فيها قوتان، حيث يمكنهما الاختيار بين التصادم والتعاون[23]. فالتفاعل الاستراتيجي بين شركتين في وضع يحتوي على قواعد ونتائج مُنمذجة يُظهر مصفوفة العوائد لنتائج اللعبة الخاصة بكل مجموعة من الاستراتيجيات والتي يمكن اعتبارها فوائد مستحقة.

ففي مصفوفة العوائد التالية يتم منح الفوائد التي تتمتع بها كل من الشركتين باستخدام الإنترنت (نظام الشبكة)، مع مراعاة عوامل الفائدة والتكلفة اعتمادًا على استراتيجيات الشركات أو اللاعبين. حيث تمنح كل خانة من المصفوفة العوائد لكل من الشركتين بالنسبة لكل مجموعة من الإجراءات، إذ تم عرض أربعة استراتيجيات لمجموعة الشركات، حيث أن استراتيجيات شركتين تعتبر معقولة. ففي الحالة الأولى تستثمر الشركة في الأمن السيبراني من أجل الحصول على شبكة آمنة، وفي الحالة الثانية لا تستثمر الشركة في الأمن السيبراني ولا تكون شبكتها آمنة.

الجدول 4: مصفوفة العوائد

		الشركة ب	
		شبكة مؤمّنة	شبكة غير مؤمّنة
الشركة أ	شبكة مؤمّنة	(20،20)	(30،10)
	شبكة غير مؤمّنة	(10،30)	(15،15)

Source : Benjamin Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry", **Journal of Law, Economics and policy**, Vol.1, No.2, Winter 2005, p 499.

تظهر أرباح الشركة "أ" باعتبارها الرقم الأول من كل زوج، أما الشركة "ب" فهي الرقم الثاني. لذلك إذا استثمرت كلتا الشركتين في الأمن السيبراني بالقدر نفسه وبالطريقة نفسها من أجل الحصول على شبكة آمنة يحصل كل منهما على عائد قدره 20 من حيث المنفعة أو الفائدة، ويظهر هذا في الخانة العلوية اليمنى، فقد اتبعوا إستراتيجية تعاونية من أجل تقاسم نفس التكلفة والفائدة. وبالتالي تعتبر هذه الاستراتيجيات هي الأمثل اجتماعيا.

أما إذا استثمرت الشركة "أ" في الأمن السيبراني من أجل الحصول على شبكة آمنة ولم تفعل الشركة "ب" فإن الشركة "أ" تحصل على مكافأة قدرها 10 بينما تحصل الشركة "ب" على مكافأة قدرها 30. ويظهر هذا في الخانة العلوية اليسرى. ففي هذه الحالة يتم فرض التكلفة الإجمالية على الشركة "أ"، في حين تتمتع الشركة "ب" بالفوائد القصوى بتكلفة صفرية وهذا بسبب إستراتيجية الشركة "أ"، وستحصل الشركة "ب" على 30 لأنها ستظل تحصل على المنفعة المقدمة من الشركة "أ" بضمان شبكة الاتصال. في هذه الحالة تتم معاقبة الشركة "أ" مقابل الشركة "ب" حيث يزداد احتمال التعرض للهجوم بسبب الإهمال ويظهر الموقف العكسي في الخانة السفلية اليمنى حيث تستثمر الشركة "ب" في الأمن السيبراني من أجل الحصول على شبكة آمنة وترفض الشركة "أ" ذلك.[24]

وإذا لم يستثمر أي منهما في الأمن السيبراني من أجل الحصول على شبكة آمنة، فسيحصل كل منهما على مكافأة قدرها 15، وهذا ما تظهره الخانة السفلية اليسرى. ففي هذه الحالة يتم إعفاء كل من الشركتين من تكلفة التأمين لكنهما يتعرضان لخطر متزايد ضد الهجمات السيبرانية المحتملة. ونتيجة لذلك تكون الفوائد الإجمالية أقل من تلك الناتجة عن الوضع الأمثل اجتماعيًا.[25]

على العموم لا تنزعج الشركات المستثمرة في الأمن السيبراني عندما تعلم أن الشركات الأخرى لن تستثمر مما يجعلها عرضة للخطر على أي حال، وهو يتوافق مع توازن ناش حيث تتخذ كل شركة أفضل قرار بالنظر إلى السلوك الأكثر احتمالًا للخصم (العائد (15،15))، ويبرز النموذج سبب إخفاق السوق في توفير الأمن السيبراني[26]. حيث يجب أن تكون المزايا الخاصة كبيرة بما يكفي لجعل الشركات تستثمر في الأمن السيبراني.

في هذا السياق فإن أي حكومة كمشتري للأسلحة السيبرانية أو خدمات الشبكات التي تؤثر على الأمن القومي تسعى لامتلاك معلومات كاملة عن سوق الأمن السيبراني، لأنه في حالة عدم وجود معلومات كاملة من جانب الحكومات، من الصعب التمييز بين المتعاملين ذوي الأداء القوي أو الضعيف في أمن الشبكات وتأمين البرامج الثابتة وتطوير البرمجيات. فمن أجل لتطوير سياسة اقتصادية يثار سؤال من قبيل معرفة ما إذا كانت المبادرة الخاصة يمكن أن توفر ما يكفي من الأمن السيبراني، أو أن هناك شكلًا ما من أشكال المشاركة الحكومية له ما يبرره، وبشكل عام يفشل السوق في توفير المقدار المناسب من الأمن السيبراني.

خاتمـــة

من خلال العرض السابق يمكن القول أن الاعتماد المتبادل بين شبكات البنى التحتية الحيوية قد أفرز شكلا جديدا للحرب والصراع في المجال السيبراني وتنامي التهديدات والمخاطر السيبرانية أين أصبح العدو ليس عدوا تقليديا، فباعتبار الحرب السيبرانية هي نوع جديد من الحرب غير المتماثلة وغير المرئية ونظرًا لطبيعتها غير الخطية يمكن أن تؤدي إلى تعطيل المجتمع بأقل تكلفة استثمارية في ظل تنامي الهجمات غير التماثلية. وبالتالي يصبح الأمن السيبراني أحد أخطر تحديات الأمن الاقتصادي والوطني الذي يتعين على أي دولة مواجهته والتعامل معه. وقد توصل البحث إلى النتائج التالية:

-يعبر مؤشر الأمن السيبراني العالمي عن مستوى الاستعداد لدى الدول في عدة مجالات (التدابير القانونية والتدابير التقنية والتدابير التنظيمية وبناء القدرات والتعاون الدولي). علاوة على ذلك فإن زيادة الطلب على السلع والخدمات في مجال الأمن السيبراني لها تأثير على شركات إنتاج الأسلحة والخدمات السيبرانية العسكرية، ومع تزايد أهمية أمن المعلومات السيبرانية تعمل صناعة الأسلحة والخدمات في سوق الأمن السيبراني بهدف تغطية هذه الاحتياجات.

-يمكن أن يسهم الأمن السيبراني من منظور اقتصادي وباستخدام أدوات تحليل التكلفة-العائد في اتخاذ القرارات في سياق إدارة المخاطر، كما يهدف إلى تحديد حجم الاستثمار في الأمن السيبراني حسب التكلفة المتوقعة. علاوة على ذلك يستخدم الأمن السيبراني كمشكلة اقتصادية أدوات الاقتصاد الجزئي ونمذجة السلوك الهجومي والدفاعي من أجل تحليل ما إذا كانت القرارات المتخذة على المستويات الفردية من المرجح أن تؤدي إلى قدر اجتماعي أمثل من الأمن السيبراني.

-يسلط النهج الحديث للاقتصاد العام الضوء على بعض الحالات التي تفشل فيها المنافع والتكاليف الخاصة في حساب جميع الفوائد والتكاليف الاجتماعية، لأن اقتصاد السوق يتميز بسلوكيات فردية لا تكون دائمًا مثالية اجتماعيًا لضمان الرفاه الاجتماعي والقدر المطلوب من الأمن السيبراني، ولا سيما الحالات التي يمكن أن تظهر فيها هذه القضايا على غرار: العوامل الخارجية للشبكة، ومعضلة السجين، وعدم تناسق المعلومات وجوانب السلع العامة للاستثمار الأمني الخاص.

-الفشل المحتمل للسوق السيبراني في تبادل المعلومات هو نتيجة للحافز على الانتفاع المجاني. وبالتالي فإن الحواجز الاقتصادية التي تحول دون تحسين أمننة الفضاء السيبراني تستدعي إشراك الحكومة ووضع القواعد التنظيمية. فالحكومة تحتاج إلى دراسة اقتصاديات الأمن السيبراني بشكل أفضل من أجل تحقيق المستوى الاجتماعي الأمثل وفحص ما إذا كان السوق قد فشل حقًا في توفير القدر اللازم من الأمن السيبراني.

-من المتوقع أن يرتفع الطلب على الأمن السيبراني في السنوات القادمة حيث ترتبط استدامة هذا الطلب بالأهمية الإستراتيجية والسياسية والاقتصادية للأمن السيبراني. والهدف من ذلك وفق وجهة النظر الاقتصادية هو حماية مصالح الشركات والبنية التحتية، ومن وجهة النظر الإستراتيجية تثار المسائل المرتبطة بإدارة الفضاء السيبراني والسيادة الرقمية، كما يتيح وضع الاستراتيجيات الإلكترونية تنظيم العلاقات بين الأفراد والمنظمات والشركات والدول. لهذه الأسباب من الضروري أن يصبح الأمن السيبراني رصيدًا قوميًا استراتيجيًا.

التهميش :

[1] - statista, "Number of internet users worldwide from 2005 to 2018, Statista 2019, (Retrieved on 4/12/2019),see : https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[2] - Rory Michael Hermann, "Cyber War In Asmall War Environment", ProQuest LLC, April 2017, p 11, (Retrieved on 16/03/2020),see : https://pqdtopen.proquest.com/doc/1892789852.html?FMT=AI&pubnum=10271200

[3] - Paul Cornish and others, "On Cyber Warfare", A Chatham House Report, London, The Royal Institute of International Affairs, November 2010, p.p 6-7.

[4]- Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It, (New York, HarperCollins Publishers Inc, 2010), p 11.

[5]- Sean Collins and Stephen McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications", Journal of Policing, Intelligence and Counter Terrorism, Vol.7, No.1, (April 2012), p 80.

[6] - RAND Corporation, "Asymmetric warfare", 2016, (Retrieved on 08/12/2019),see : https://www.rand.org/topics/asymmetric-warfare.html

[7] - Jim Q. Chen and Alan Dinerman : "Cyber Capabilities in Modern Warfare", in : Martti Lehto and Pekka Neittaanmäki (Edits) : Cyber Security: Power and

Technology, (Cham (Switzerland) : Springer International Publishing AG, 2018), p 27.

[8] - National Research Council, Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy, (Washington, The National Academies Press, DC, 2010), p 43.

[9] -أنظر كل من:

- Thomas Rid And Ben Buchanan, "Attributing cyber attacks", Journal of Strategic Studies, Vol.38, N.1-2 (2015), p 20.

- Mohamed Chawki, "Anonymity in Cyberspace: Finding the Balance between Privacy and Security", Droit-Tic, Juill. 2006, p.p 13-14, (Retrieved on 08/12/2019), see : http://www.droit-tic.com/pdf/Anonymity_Cyberspace.pdf

[10] - Angelyn Flowers and Sherali Zeadally, "Cyberwar: The What, When, Why, and How", Commentary, IEEE Technology And Society Magazine, (Fall 2014), p 16.

[11] - Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", Journal of Strategic Security, Vol.4, N.2 (Summer 2011), p 50.

[12] - Ibid, p 51.

[13] - Robert Kaiser, "The birth of cyberwar", Political Geography, Vol. 46 (May 2015), p.p 11-12.

[14] - Paulo Shakarian, "The 2008 Russian Cyber-Campaign Against Georgia", Military Review, (November-December 2011), p.p 63-64.

[15] - Marios-Panagiotis Efthymiopoulos, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Vol.8, N.12 (2019), p8.

[16] - European Commission, "Cyber-Security", Scoping paper, Scientific Advice Mechanism, (29 January, 2016), p 2.

[17] - International Telecommunication Union (ITU), "Global Cyber-Security index & cyberwellness profiles", Report, Geneve, ABI research Telecommunication Development Sector, 2015, p 29.

* فريق مواجهة الطوارئ الحاسوبية (CERT) هو فريق خبراء يتعامل مع حوادث أمان الكمبيوتر. استخدم لأول مرة في عام 1988 من قبل مركز تنسيق CERT (CERT-CC) في جامعة كارنيجي ميلون (CMU). تم اختيار

اختصار CERT للاسم التاريخي من قبل فرق أخرى في جميع أنحاء العالم. أخذت بعض الفرق اسم CSIRT الأكثر تحديدًا للإشارة إلى مهمة التعامل مع حوادث أمان الكمبيوتر بدلاً من أعمال الدعم الفني الأخرى.

[18]- Stockholm International Peace Research Institute (SIPRI), Armaments, Disarmament and International Security, (Stockholm : SIPRI Yearbook, 2016), p 19.

[19] - Lawrence A. Gordon And Martin P. Loeb, "The Economics of Information Security Investment", ACM Transactions on Information and System Security, Vol. 5, No.4 (November 2002), p.p 443-446.

[20] - Ross Anderson, "why information security is hard : an economic perspective", 2001, (Retrieved on 09/12/2019), see : https://www.acsac.org/2001/papers/110.pdf

[21] -Ibid.

[22] - Andrew Liaropoulos, "Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?", Journal of Information Warfare, Vol. 12, No. 2 (2013), pp. 22-23.

[23]- Cuong T. Do and others, "Game Theory for Cyber Security and Privacy", ACM Computing Surveys, Vol. 50, No. 2, Article 30 (May 2017), p.p 4-5.

[24] - Benjamin Powell, Op.cit, p 499.

[25] - Ibid, 499-500.

[26] -Ibid, p 2.