مجلة هيرودوت للعلوم الإنسانية والاجتماعية | المجلد 7 / العدد: 25 (2023)، ص 237-257

تأمين الخطر السيبراني

Insurance Cyber Risk

بغدادي شامبي*
جامعة الجزائر 1 –كلية الحقوق سعيد حمدين
b.chambi@univ-alger.dz

تاريخ الاستلام: 2022/03/08 تاريخ القبول: 2023/02/16

الملخص:

يعالج الموضوع التأمين كآلية جديدة قانونية وتقنية علاجية للحد من ظاهرة الخطر السيبراني أو بما يعرف بالجريمة الإلكترونية التي أصبحت تشكل تهديد حقيقي لأمن الدول والأشخاص. هذا الخطر يصيب المعلومات المتمثلة في الشيء غير المادي ذو القيمة الاقتصادية ذات الخصائص الشخصية، السرية، الاستراتيجية. حيث تم التوصل إلى أن المعلومات كقاعدة عامة صعبة التأمين نظرا لخصائصها غير الملموسة وخصائص الخطر السيبراني غير المرئي وتصنيف هذا الخطر من الأخطار الكبرى. استثناءا، يمكن التأمين عليها وفقا شروط مذكورة في الموضوع. كما يمكن للأشخاص الطبيعية والمعنوية خاصة إبرام عقد تأمين سيبراني مع شركات التأمين لتعويض الأضرار التي تصيبها جراء الكارثة السيبرانية. تقدم شركات التأمين ضمانات عينية للمؤمن له المتضرر بإرسال فريق خبراء إعلام آلي عند وقوع الكارثة لجبر الضرر والسيطرة على الوضع، كما تقدم ضمانات نقدية لإعادة إقلاع نشاط المؤمن له المتضرر، استرجاع معلوماته، تعويض مسؤوليته المدنية جراء عدم حماية نظام معلوماته ورجوع الغير ضده بدعوى جماعية.

الكلمات المفتاحية : تأمين الخطر السيبراني ، الجريمة الإلكترونية ، تأمين المعلومات ، تأمين أخطار الإعلام الآلي ، إدارة الخطر السيبران.

Abstract:

This topic treats insurance as a new legal and technical protective mechanism to face cyber risk known as electronic-crime which has become a real menace for the security of the states and persons over the world. Informations which has an economic value, and can be personal, secrets or strategics as a characteristics are the dematerialized things cibled by the risk. It was concluded that informations and the cyber risk in itself are difficult to insure as general rule due to their special characteristics but it can be insured as an exception with some conditions cited. Physical and legal persons can conclude a cyber insurance contract with insurance companies to compensate the cyber sinister. Many guarantees are offered by the insurer. Primary, indemnity in kind, by sending a cyber security team to resolve the situation. Secondly, in cash to compensate business loss, data recovery and cyber-liability due to class action by others.

Keywords
Cyber Insurance contract, Cyber risk management, Pegasus, Cyber Crime, Working at distance

* بغدادي شامبي

● مقدمة:

الأخطار منذ خلق الأرض وهي في تطور مستمر ولهذا التأمين كان دائما آلية علاجية للتقليل من أضرارها. هناك ما يسمى بالأخطار التقليدية القابلة للتأمين كالحريق، أضرار المياه، السرقة، المسؤولية المدنية لصاحب السيارة إلخ.. فهي أخطار مقننة في قانون التأمين الجزائري[1] ومدرجة في مرسوم عمليات التأمين[2]. هذا من جهة، من جهة أخرى هناك أخطار نامية، يرتبط وجود هذه الأخطار مع التطور التكنولوجي، تغير الظروف المناخية الراجع إلى زيادة عدد المصانع في العالم، تعدد العملة، البورصة... إلخ، لهذه الأخطار للإنسان يد في حدوثها.قامت الفيديرالية الفرنسية لشركات التأمين بنشر تقرير على موقعها الرسمي على هذا النوع من الأخطار[3]. حيث خصصت بارومتر تتكلم فيه عن الأخطار النامية في العام 2018 إلى 2022. من بين هذه الأخطار: أخطار الأوبئة، الخطر السيبراني، الانهيار المالي، التغير المناخي، السياسة الدولية، الانهيار التنظيمي. الخطر الذي احتل المرتبة الأولى من حيث درجة الخطورة هو الخطر السيبراني والذي هو موضوع هذه الدراسة. كلمة سيبراني تعريب وليس ترجمة للكلمة الحديثة **Cyber**. سيبراني تضاف إلى كلمة أخرى معروفة لتكوين (مصطلح مضاف ومضاف إليه) يتعلق بأجهزة وشبكات الحاسب. فالأخطار السيبرانية من منظور قانون التأمين أو الجريمة الإلكترونية من منظور قانون العقوبات، مصطلحين مترادفين ونعني بهم الهجمات الإلكترونية على أنظمة معالجة المعلومات ومن تم التعدي على المعلومات. كما يذكر أن هذه الأنواع من الأخطار غير محينة و مدرجة في قانون التأمينات الجزائري و هذا راجع لحداثتها .

أخيرا، قد قامت الجزائر بتشريع القانون 09-04[4] وأنشئت لجنة للوقاية منها ولمحاربة هذه الجريمة الإلكترونية، هذا من الجانب العقابي، لكن دون جدوى فالخطر يزداد يوما بعد يوم.تشهد الجزائر تضخم قانوني في هذا المجال، لكن الخطر السيبراني هو خطر تقني قبل كل شيء ويستوجب التعامل معه بآليات تقنية جديدة للتقليل من أضراره ولهذا يعالج الموضوع آلية جديدة تقنية وقانونية ومنتوج جديد هو التأمين على هذا النوع من الأخطار وذلك بنقل هذا الخطر السيبراني إلى محترفي التأمين لتلقي تعويضات في حالة الكارثة السيبرانية. لكن الأمر ليس بالسهل، فالتأمين على هذا النوع من الأخطار الكبرى عادة ما يرفض من المؤمنين لصعوبة التأمين عليه.

الإشكالية:

---

[1] أمر رقم 95-07 ممضي في 25 يناير 1995، يتعلق بالتأمينات، الجريدة الرسمية عدد 13 مؤرخة في 08 مارس 1995، الصفحة 3.

[2] مرسوم تنفيذي رقم 02-293 ممضي في 10 سبتمبر 2002، يعدل ويتمم المرسوم التنفيذي رقم 95-338 المؤرخ في 6 جمادى الثانية عام 1416 الموافق 30 أكتوبر سنة 1995 والمتعلق بإعداد قائمة عمليات التأمين وحصرها، الجريدة الرسمية عدد 61 المؤرخة في 11 سبتمبر 2002، الصفحة 10.

[3] *Planetecsca.Fr*,2022,https://www.planetecsca.fr/content/uploads/sites/4/2019/07/FFA2018_02_07_premier_barometre_des_risques_emergents_pour_lassurance.pdf. Accessed 15 Dec 2022.

[4] قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ممضي في 05 غشت 2009، الجريدة الرسمية عدد 47 مؤرخة في 16 غشت 2009، الصفحة 5.

تشير الدراسات التي عالجت هذا النوع من المواضيع أن معالجة الأنظمة المعلوماتية تتضمن جانب مادي وآخر غير مادي، حيث يشمل التأمين هذين العنصرين: المادي منه سهل المنال، بينما غير المادي يتميز بالتعقيد والصعوبة. تأمين الأخطار السيبرانية له مشكلات خاصة من أهمها أن المؤمن له لا يستطيع كشف الخطر الذي يستطيع أن يقع بدون ان يراه، إلا أن القرصان يستطيع اختراق النظام بدون أن يشعر المؤمن له بالخطر المحدق به كون أن هذه الأخيرة لا يمكن رؤيتها في مجال التأمينات بل يتم كشفها مع الوقت. وهذا المشكل يستطيع ان تزيد في درجة حدوثه عوامل أخرى كتداخل أنظمة المعلومات التي تحدث أخطار في جهات جغرافية مختلفة وقد ترفع من درجة الخلل يدفع باتجاه زيادة حدوث الخطر السيبراني الذي يقترن مع مشاكل أخرى في التأمين منها: عدم العلم بدرجة احتمالية حدوث هذه الأخطار، عدم العلم بكيفية الكشف عن هذه الأخطار، الوقاية منهم والحماية، صعوبة تقييم الخسائر، صوبة تحديد كمية الخسائر وصعوبة تسعيرة هذه الأخطار لعدم وجود قاعدة بيانات أخطار مصرح بها من قبل.

ضمن هذه الرؤية جاءت إشكالية بحثنا التي تتضمن السؤال الجوهري التالي:

السؤال الرئيسي: هل يمكن التأمين على المعلومات التي تعتبر شيء غير ملموس ذو قيمة اقتصادية وكذلك التأمين على آثار الأخطار السيبرانية التي لها خصائص خاصة؟

الفرضيتين :

-يمكن التأمين على المعلومات بما أن المعلومات تعتبر أشياء معنوية ذات قيمة اقتصادية .

-يمكن التأمين على الخطر السيبراني رغم أنه غير مرئي، لأنه يوافي كل شروط الخطر الفنية التي تسمح له أن يكون قابل للتأمين من مشروعية ، خارج عن إرادة الأطراف و تواتر الأخطار.

المنهج المستخدم:

1. المنهج الوصفي التحليلي لأننا بصدد دراسة ظاهرة ألا وهي الخطر النامي، الخطر السيبراني في التأمينات (الجانب التعويضي).
2. المنهج المقارن (مقارنة بين إنتهاج سياسة إدارة الخطر السيبراني داخل المؤسسة، وسياسية نقل الخطر إلى شركة التأمين. تمت المقارنة بين العقود التقليدية لتأمين الإعلام الآلي والجديدة (العقد السيبراني للتأمين) مع عمل مقارنة بين مختلف الشروط العامة والضمانات التي تقترحها شركات التأمين، في الأخير مقارنة بين فرنسا والجزائر في مجال السوق السيبراني للتأمين.

1. الخطر السيبراني:

تم التطرق في هذا المبحث الأول من الدراسة في مطلب أول إلى ما هو الخطر السيبراني : تعريفه، خصائصه، أنواعه، ثم في مطلب ثاني من المبحث إلى إدارة الخطر السيبراني، بمعنى الأمن السيبراني الداخلي لحماية المؤسسة ضد الهجمات الإلكترونية.

1.1 الإطار المفاهمي للخطر السيبراني

يتم شرح في هذا المطلب الأول من المبحث الأول تعريف الخطر السيبراني، خصائصه، أنواعه.

1.1.1 تعريف الخطر السيبراني وأسبابه وخصائصه : سيبراني تعريب وليس ترجمة للكلمة الحديثة **Cyber**. سيبراني تضاف إلى كلمة أخرى معروفة لتكوين (مصطلح مضاف ومضاف إليه) يتعلق بأجهزة وشبكات الحاسب[5].تمت ترجمة هذا المصطلح (الخطر السيبراني) نسبة للمصطلح في المراجع الفرنسية المتداولة في مجال التأمينات.

اصطلاحا تتعدد التعاريف المتعلقة بالخطر السيبراني، إلا أنها تتفق في تعريفها للأخطار السيبرانية بأنها: « أولا آثار انتهاك البيانات بدون الهجوم على نظام المعلومات، أو ثانيا آثار الهجوم على نظام المعلومات أي الدخول غير المشروع لنظام المعلومات. [6] » .

من بين آثار الهجمة على البيانات:[7]سرقة البيانات المالية والاستراتيجية للزبائن والموردين، إتلاف البيانات، حذف البيانات، انتهاك سمعة المؤسسة، اما آثار الهجمة على نظام المعلومات فتتمثل في الدخول غير المشروع إلى نظام المعلومات، إيقاف نظام المعلومات، تشييل أو فيرسة نظام المعلومات (العمل على تعبئته بالفيروسات)، الاستعمال غير المشروع لنظام المعلومات[8] وإلحاق إضرار بالسمعة.

لم يعتمد المشرع الجزائري مصطلح "الخطر السيبراني" لا في قانون التأمينات أو قانون آخر، لكن تبنى تعريفه بمصطلح الجريمة الإلكترونية وذلك في قانون العقوبات، حيث تبنى للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات ، معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ، ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي، فلا يكون هناك مجال لهذا البحث. لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات[9] التي وضعت تعريفا لنظام المعلومات، حيث أنه عرف في المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تحت مصطلح "المنظومة المعلوماتية "، وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين.

2.1.1 الخصائص التي يتميز بها الخطر السيبراني : (الخصائص التي تبين أن الخطر السيبراني لا يقبل التأمين في الأصل) [10] الخطر السيبراني بمقارنته بالأخطار الأخرى التي يمكن التأمين عليها. هو في الأصل خطر لا يمكن التأمين عليه نظرا للخصائص التي يتميز

---

[5] **المهندس محمد بن سعود الخطيب**، إستشاري الأنظمة، 10 محرم 1435 هجري، http://tangentlink.com/wp-content/uploads/2013/11/4.-Relation-Between-Cyber-and-EW-Colonel-REng-Mohammed-Saud-Al-Khatib.pdf Accessed 15 Dec 2022.

[6] *Samia Tibah*, Présentation Cyber risques, 2018, https://www.ccr.dz/images/pdf/cyber-risks-ccr.pdf. Accessed 15 Dec 2022.

[7] Samia Tibah, Ibid, 12 Mars 2018.

[8] Voir Aussi : ÉRIC A. CAPRIOLI, Banque et Assurance Digitales, Droit et Pratiques, RB Éditions, 2017, p 205.

[9] كتاب قيم صدر في 2018 يتكلم على تكنولوجيا المعلومات وعلاقتها بكل القوانين (التجارية، العقابية).. إلخ حتى الخطر السيبراني وعلاقته بكل القوانين.

[10] **Comission Cyber Risk :** Rapport : Assurer le risque Cyber, Tome 1, Club des Juristes, 2018, Page 21.

بها، فلا يمكن التحكم فيه 100% كباقي الأخطار، لأنه يتميز بخصائص أو أسس فنية تختلف عن باقي الأخطار الأخرى. [11]هناك 6 خصائص حسب اللجنة الفرنسية لتأمين الخطر السيبراني ويمكن إضافة خصائص عدة أخرى، إذن نذكر أهمها:

1- الكوارث السيبرانية خسائر يمكن أن تزيد بشكل ملحوظ في المستقبل:[12] تعرض مزود خدمة لحوسبة سحابية **Prestataires de Cloud** لخطر سيبراني حسب إحصائيات اللويدز، يمكن أن تصل حتى 53 مليار دولار كمتوسط خسارة بمعنى مبلغ مساوي لمبلغ خسارة الكوارث الطبيعية التي لا يؤمنها المؤمنون إلا بعمليات إعادة التأمين عادة. في الوقت الحاضر يمكن التأمين على الأخطار السيبرانية لأن تكلفتها لم تصل الأخطار الكبرى كالكوارث الطبيعية، لكن في المستقبل هناك تخوف على أن تفوق هذه الأخطار قدرة السوق ومن تم عدم التأمين عليها، فكل شيء مرتبط بعامل الوقت والتطور التكنولوجي والإحصائيات.

2 -المخاطر السيبرانية أخطار جد مترابطة:[13] ترابط الأجهزة وأنظمة الإعلام الآلي مع ترابط المستخدمين، يستطيع أن يكون مصدر غموض للمؤمن (ترابط الأنظمة يزيد من ترابط الأخطار السيبرانية نسبيا). ولا يستطيع ضمان الخطر السيبراني عندما تكون الكارثة تفوق قدرته وتهدد ملاءة شركة التأمين، إلا إن وجدت إعادة تأمين.

3 -عدم وجود قاعدة بيانات إحصائية موثوقة بخصوص التصريح بالكوارث السيبرانية[14] : غياب قاعدة بيانات إحصائية دقيقة تحرم المؤمنين من أداة عمل أساسية لنمذجة المخاطر السيبرانية ومنها تحديد قسط التأمين المتناسب مع الخطر السيبراني، وتحرم جميع الجهات الفاعلة الاقتصادية في مصدر المعلومات التي من شأنها أن تساهم في زيادة الوعي بالخطر السيبراني.

4 -خسائر كبيرة غير ملموسة، يصعب تقييمها[15] : الكوارث السيبرانية تحقق ضرر فعال ومن تم خسارة مالية كبيرة، لكن الأهم لنا هو خاصية الخطر غير الملموس، فالأخطار الأخرى القابلة للتأمين جلها ملموسة ويمكن رؤيتها بسرعة أو اكتشافها، (كالحريق، أضرار المياه، الصواعق..). لكن الكارثة السيبرانية تكتشف إلا بعد مدة من حدوثها، وبعض الأحيان لا تكتشف أصلا. والمؤمن له يستطيع أن يكتشف الكارثة بعد مدة من حدوثها وهنا تدخل مسألة هل يعتد المؤمن بتاريخ اكتشاف الخطر أو حدوثه في مدة سريان العقد هذا ما سنرى في التزامات المؤمن له (الإخطار بالكارثة) .

5 -خطر جد صعب التأمين عند تحليله، بسبب تقنية وحساسية المعلومات المتبادلة[16] : عدم تقييم الخطر جيدا بسبب عدم شفافية المعلومات المتبادلة بين المؤمن والمؤمن له.الكثير من المؤمن لهم لا تصرح للمؤمن بالمعلومات (الأشياء المعنوية غير الملموسة ذات القيمة الاقتصادية). هذه البيانات، التي تهم جوهر نشاطها وقيمتها (المشاريع الحالية، براءات الاختراع... إلخ)، هي استراتيجية

---

[11]نادي الحقوقيون في فرنسا أنشأ لجنة حقوقيين في 2018 مختصة في تأمين الخطر السيبراني وكل ما يحيطه به. وهي لجنة تتكون من حقوقيين وتقنيين في المجال جد معروفين في فرنسا من بينهم رئيس الاتحاد الفرنسي للتأمين كرئيس اللجنة والأمينة العامة فاليري لافارج سازكوزي. وباقي الأعضاء نجدهم في الصفحة 4 من الكتاب (تأمين الخطر السيبراني في 2018) وقامت اللجنة بنشر دراسة على موقع نادي الحقوقيين الفرنسي، دراسة عبارة عن كتاب 2018، تأمين الخطر السيبراني تقرير جانفي يحتوي على 100 صفحة 2018.

[12] Comission Cyber Risk : Rapport : Assurer le risque Cyber, Op Cit, p 22.

[13] Comission Cyber Risk : Rapport : Assurer le risque Cyber, Ibid, p 25.

[14] Comission Cyber Risk : Rapport : Assurer le risque Cyber, Ibid, p 28.

[15] Comission Cyber Risk : Rapport : Assurer le risque Cyber, Ibid, p 30.

[16] Comission Cyber Risk : Rapport : Assurer le risque Cyber, Ibid., p 32.

وسرية. فهذا إشكال، فلا يمكن تقييم المعلومات بهذه الطريقة، ولا يتمكن المؤمن معرفة القيمة الحقيقية للشيء المؤمن عليه، عكس التأمينات الأخرى أين يتم التعرف على قيمة الشيء المؤمن عند اكتتاب العقد.

6 – خطر ديناميكي للغاية[17] : **90**% من الكوارث السيبرانية تنتج بسببين: السبب الأول خطأ الإنسان، والثاني سلوك الإنسان. عدم القدرة على التنبؤ بسلوك الإنسان، العمدي (الجريمة) وغير العمدي (الخطأ)، التي تكون سبب وقوع وخطورة العديد من الحوادث السيبرانية (احتمال سرقة أو أخطاء معالجة البيانات، اختيار الضحية في حالة هجمة.. إلخ) يجعل الأخطار السيبرانية بطبيعتها أكثر تنوعًا وصعوبة في التنبؤ والتحكم، والنمذجة مقارنة بالأخطار الأخرى.

3.1.1 أنواع الأخطار التي تتعرض لها المؤسسات : الأخطار المتعلقة بأمن تكنولوجيا المعلومات ترتبط بوقوع أحداث تؤثر على سلامة، إتاحة، سرية المعلومات، البنية التحتية ونظم المعلومات للشركة.

الخطر الداخلي (الأخطار السيبرانية من داخل المؤسسة): 60% من الهجمات تأتي من داخل المؤسسة (العاملين، الزوار، الزبائن، المجهزين (الموردين)، مزودي الخدمة، المتدربين أو المقيمين، خادمي الصيانة الذين ليسوا في كل الأحوال أبرياء. بإمكانهم الاطلاع على أسرار تكنولوجية، تجارية، مالية.. إلخ، ويستطيعوا تسريبها أيضا. هناك كم هائل من المعلومات يمكن الحصول عليها من سلة المحذوفات (القمامة) لأن هذه المعلومات لم تحذف بصفة نهائية، والسلة عبارة عن مجلد يمكن استرجاع المعلومات منه، فيمكن الحصول منها على (مشاريع عقود، مشاريع إعادة الهيكلة، بيانات سوق الأوراق المالية (البورصة)، عناصر مالية أو عناصر محاسبة إلخ...) لهذا يجب التفطن لمثل هذه الأشياء.

أخطار خارجية (الأخطار السيبرانية من خارج المؤسسة): أهم الأخطار تكمن في هجمات أنظمة الإعلام الآلي بكل أنواعها:

هجمات حجب الخدمةDDOS: يرمز الاختصار **DDOS** لهجوم حجب الخدمة أو الحرمان من الخدمة وهو أسلوب منتشر وشائع يستخدمه القراصنة عن طريق إغراق المواقع بسيل من البيانات غير اللازمة يتم إرسالها عن بعد.[18]

البرمجيات الخبيثة: هي برمجية يتم تضمينها أو إدراجها عمدا، في نظام الحاسوب لأغراض ضارة، بدون رضا المالك. فقد تستخدم لعرقلة تشغيل الحاسوب، جمع معلومات حساسة، أو الوصول إلى أنظمة الكمبيوتر الخاصة.[19]من الأمثلة على البرمجيات الخبيثة هي الفيروسات **Viruses**، أحصنة طروادة **Trojans**، القنابل الموقوتة **Bomb Logic**، باب المصيدة **Backdoor**، الديدان **Computer worms**...إلخ

حصان طروادة Trojan: بكل بساطة حصان طروادة عبارة عن برنامج خبيث، يقوم بالتحكم عن بعد بجهاز أو كمبيوتر شخص قام بفتح هذا البرنامج في حاسوبه.

---

[17] Comission Cyber Risk : Rapport : Assurer le risque Cyber, Ibid., p 32.

[18] ***CNN Arabic*, 2016, "DDOS ما هي هجمات حجب الخدمة وكيف تؤدي إلى خسارة مئات ملايين الدولارات؟".** https://arabic.cnn.com/scitech/2016/12/08/sc-081216-what-ddos-attack. Accessed 15 Dec 2022.

[19] **"برمجيات خبيثة – ويكيبيديا".** *Ar.Wikipedia.Org*, 2022, https://ar.wikipedia.org/wiki/برمجيات_خبيثة/. Accessed 15 Dec 2022.

برامج التجسس (keylogger): تسجل برامج التجسس جميع المعلومات، مثلا كل ما تقوم الضحية بكتابته، يسجله الفيروس هذا **Keyloggers**. فإن كتبت على الساعة 12:15 كلمة: السلام عليكم، يسجلها البرنامج ويرسلها إلى المخترق.

برامج نزع الفدية (RANSOMEWARE): نوع من البرمجيات الخبيثة، يقوم من خلالها الهاكر، تشفير ملفات المؤسسة او الشخص الضحية الذي يقوم بفتح البرنامج في حاسوبه ومن تم يطلب منه مبلغ معتبر من المال لكي يقوم الهاكر بفك تشفير ملفاته.وفي هذا الصدد، الفدية كانت محل جدال في موضوع ضمانها من المؤمنين. من أكبر المؤسسات التي كانت ضحية هذا الفيروس **Renault**الفرنسية[20].تشير المعطيات أن40 % من حواسيب المراقبة الصناعية المستعملة لكاسبارسكي ، كانت ضحية اختراق في سنة 2017. نهيك عن الأخطار الأخرى التي تصيب أنظمة المعلومات الجزائرية في شتى المجالات (إدارات ومؤسسات تجارية وصناعية) في ظل غياب منتوج تأميني سيبراني يغطي هذه الأخطار.[21]

فيروسات جديدة الجيل الأخير:

بيغاسوس « **Pegasus**»من آخر الفيروسات أو برامج التجسس الذي أنشئه **NSO Group** هو برنامج سري[22]. برنامج تم إنشائه لبيعه للحكومات ، لأغراض أمنية و هذا ما صرحت به الشركة . لكن مؤخرا تم إستعامله لإختراق إطارات في دول مجاورة ، الشركة باعت البرنامج و لها لوحة تحكم لعمل تسجيل خروج **Disconnect** من نظام حصان طروادة (الفيروس بيغاسوس) لأي مستعمل للبرنامج لأغراض غير تلك المحددة في البرنامج . و هل نفهم من هذا أن الشركة تتجسس أيضا على ماذا يفعل مستعمل البرنامج ؟ . هناك سؤال تم طرحه أيضا لو تتمكن عناصر إرهابية أو إجرامية من التحكم في البرنامج . اجاب صانعو البرنامج أن هذا غير ممكن لأن البرنامج يباع في شكل جهاز مادي «**HARDWARE** »و غير مادي «**SOFTWARE**». ملآين الدولارات دفعتها الدول لإقتناء هذا النوع من البرامج التي تسمح لها بالتحكم في اجهزة الهاتف بمجرد ضغطة زرعبر ثغرات من نوع «**Remote code execution**» **RCE**.

أنواع أخرى :اختراق خطوط اتصال PHREAKING Voip: قيام جماعة من المخترقين باختراق سيرفر يقدم خدمات اتصال، ومن بعد تملكه لرقم الهاتف (لهاتف الخادم أو السيرفر)، يقوم بالاتصال إلى خطوط اتصالاته التي تأخذ أموال مقابل المكالمة (أرقام الهاكر التي تأخذ أرصدة عند الاتصال بها). ومن تم يضخم فاتورة المؤسسة التي تمتلك سيرفر الاتصال الذي تم اختراقه.

الصفحات المزورة للمواقع، لسرقة بيانات تسجيل الدخول للضحايا Phishing :بعد أن يستنسخ المخترق الموقع المراد استنساخه، يقوم بإرسال رابط مزور للضحايا، فتقوم بإدخال معلوماتها ومن تم يلتقطها المخترق.

---

[20] LIBERATION, avec AFP, Ransomware Renault parmi les cibles d'une cyberattaque mondiale , publié le 12 mai 2017 , http://www.liberation.fr/planete/2017/05/12/renault-parmi-les-cibles-d-une-cyberattaque-mondiale_1569124 . Accessed 15 Dec 2022.

[21] *Imene.A* , 2018,L'industrie énergétique en Algérie espionnée , **https://www.algerie360.com/letude-de-kaspersky-revele-662-ordinateurs-touches-cyberattaques-lindustrie-energetique-algerie-espionnee/** . Accessed 15 Dec 2022.

[22] Ronen Bergman, "Weaving A Cyber Web ", 01 Nov2019,https://www.ynetnews.com/articles/0,7340,L-5444998,00.html. Accessed 15 Dec 2022.

2.1إدارة الأخطار السيبرانية داخل المؤسسة :

تم التطرق في هذا المطلب الثاني من المبحث الأول إلى سياسية إدارة المخاطر السيبرانية بمرحلتيها ، مرحلة التحضير للهجمة السيبرانية و مرحلة ثانية ، مرحلة التدخل لحل الكارثة السيبرانية أو بما يعرف بمرحلة التنفيذ .

1.2.1 تسيير الخطر السيبراني قبل حدوثه :

تعريف: إدارة المخاطر السيبرانية:" عملية تحديد وقياس وضبط ومراقبة المخاطر السيبرانية ". [23] هناك مرحلتين عند اتخاذ القرار: أولا، مرحلة الوقاية من الخطر السيبراني والكشف عن الكارثة.ثانيا، مرحلة علاج الخطر السيبرانية (التدخل عند حدوث الكارثة السيبرانية للتحكم فيها).

مرحلة التحضير للكارثة السيبرانية[24] :

التنظيم والوعي، الأمن السيبراني مسألة الجميع: بخصوص الأمن السيبراني أو أمن الإعلام الآلي، سلوك أي فرد جد مهم في المؤسسة، كل العمال والمدراء يجب أن يكونوا واعيين بالأمر. مع حملهم رسالة واحدة: الأمن مسألة الجميع.

إعداد خطة استجابة للحوادث السيبرانية[25] إعداد خطة استجابة للحوادث السيبرانية هو عمل جماعي بأدوار محددة لكل شخص وعمل تجارب للتعامل مع الوضعية. هناك مراحل عديدة في هذه المرحلة، نقوم بها لكي يمكن التصدي للخطر السيبراني يوم وقوعه.

1 تشكيل فريق الاستجابة للحوادث :

قرار وضع خطة الإستجابة للكارثة السيبرانية يجب أن توافق عليها المديرية العامة للمؤسسة وإعطاء الوسائل للشخص الرئيس لفريق الإستجابة لكي ينسق الأعمال بين أفراد الفريق.

2 مرحلة كشف الكارثة السيبرانية[26]

الاستعداد لمواجهة الخطر السيبراني يتطلب الاستعداد لكشف الكارثة السيبرانية إن حدثت لأن هذا الخطر ليس كالأخطار الأخرى يكشف عنها يوم وقوعها. الآن السؤال، ما حجم آثار الكارثة السيبرانية على حياة المؤسسة؟ تقنيات عديدة يمكن أن تدخل في الحسبان للكشف عن الكارثة السيبرانية وليس فقط، بل التقليل من آثارها كتشفير المعلومات.

[27] تنصيب نظام معالجة الحوادث السيبرانية والكشف عن الكارثة السيبرانية:

---

[23] **البنك المركزي الأردني**، تعليمات التكيف مع المخاطر السيبرانية، https://www.cbj.gov.jo/DetailsPage/CBJAR/NewsDetails.aspx?ID=213 . **Accessed 15 Dec 2022.**

[24] Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Les Essentiels de la banque et de la finance, RB Editions, 2017, p 75.

[25] Laure Zicry, Ibid, p 78.

[26] Laure Zicry, Ibid, p 79.

[27] Laure Zicry, Ibid, p 80.

SOC, CERT, SIEM هذه الأنظمة تساعد إن حدثت الكارثة السيبرانية (الاختراق) بدون نسيان إجراء تجارب الاختراق **Test Intrusions**.

اختيار وانتقاء مزودي الخدمة الخارجيين المناسبة: الاستعداد للكارثة السيبرانية، تدخل فيها عملية اختيار مزود الخدمة **Prestataire externe** المناسب الذي ستستدعيه المؤسسة إن حدث الخطر السيبراني. العديد من مزودي الخدمة يمكن الاعتماد عليها بخصوص الخطر السيبراني.

- 1 –خبراء العلوم الجنائية المتعلقة بالحاسب الآلي.
- 2 –شركة اتصالات متخصصة في العلاقات العامة.
- 3 –شركة إدارة الأزمات الإلكترونية (السيبرانية).
- 4 –شركة التأمين كمزود خدمة.

الإعلام والمراقبة: [28]أمن الإعلام الآلي هو مسألة الجميع داخل المؤسسة، ليس فقط مختصي الإعلام الآلي التي تتعامل معهم المؤسسة داخليا وخارجيا. كل شخص في المؤسسة يجب أن يعلم بأن المؤسسة تستطيع أن تكون عرضة كارثة سيبرانية.

تجريب خطة الاستجابة للأزمة السيبرانية: بعد وضع الخطة (الجانب النظري)، يجب تطبيقها كمرحلة ثانية. للتمرن والتحضير ليوم حدوث الكارثة والتجهيز الجيد لها.

2.2.1 تسيير الخطر السيبراني عند حدوثه :

يتم شرح الإجراء ات التي يتم اتخاذها عند حدوث الكارثة السيبرانية :[29]

1 تنفيذ الخطة التي تم وضعها لحل الأزمة السيبرانية:

عندما يحدث الخطر (الكارثة)، يجب كشفه أولا، وعند كشفه نجد آثاره على نظام معلومات المؤسسة (سرقة البيانات، فساد البيانات.. إلخ) وأثاره على نشاط المؤسسة (وقف النشاط، حذف البيانات.. إلخ). أول خطوة هي: تنفيذ خطة التحكم في الأزمة التي تم عدها قبل وقوع الخطر السيبراني وإخطار جميع أعضاء فرقة الاستجابة أو مواجهة الأزمة وحلها. [30]

2 المرحلة الثانية في مواجهة الكارثة السيبرانية : الإجراء ات الأولية التي يتم اتخاذها : مهمات متزامنة تبدأ مباشرة بعد الأزمة :

1–المهمات ذات الطابع التقني : يتكفل بها خبراء العلوم الجنائية المتعلقة بالحاسب الآلي **Forensics**. يجب توقيف الكارثة السيبرانية إن كانت لا تزال واقعة (كاختراق موقع مثلا والتحكم فيه لمدة معينة من الهاكر، يجب وقف الاختراق هذا). أيضا يجب

[28] Laure Zicry, Ibid, p 83.
[29] Laure Zicry, Ibid, p 86.
[30] Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Op-cit, p 89.

معرفة نوع هذه الهجمة السيبرانية (فيروس، برنامج نزع فدية أم ماذا؟ حجب خدمة؟) .مزود الخدمة **Forensics**يقوم بكل هاته العمليات على أحسن وجه (وقف الهجمة وفهمها وسدها ومعرفة من المسؤول عنها.

2-المهمات ذات الطابع القانوني: يجب اتخاذها من طرف الخلية القانونية للمؤسسة، أو من طرف مكتب محامين، مختصين في المجال السيبراني. عند معرفة المؤسسة لنوع الكارثة السيبرانية التي حلت بها، المحامون ورجال القانون سيحددون الإجراء ات التي يجب اتخاذها (الإخطار لسلطة الرقابة والزبائن) وحتى كيفية إدارة دعاوى الزبائن الموجهة ضد مؤسستهم التي لم تحمي جيدا نظام قانونها.

3 مهمات التواصل داخليا وخارجيا التي يجب القيام بها من طرف المؤسسة: للتواصل قبل الصحافة أو المجرمين (المخترقين الذين نفذوا الهجمة السيبرانية لأن في أغلب الأحيان يتم التصريح بها من طرفهم لأنهم قاموا بالتغلب على نظام حماية لكي يبرزون عضلاتهم).

المرحلة 3: الإخطار لسلطات الرقابة: [31]الإخطار عن الكارثة السيبرانية يتنوع على حسب نوع الكارثة السيبرانية وهنا جدول يوضح من يجب أن يخطر بالكارثة السيبرانية. (في فرنسا) لأخذ فكرة عن الأنظمة.

OIVالمؤسسات العبارة عن المشتغلين الحيويين	سرقت البيانات بالإضرار بنظام المعلومات.	سرقت البيانات بدون الإضرار بنظام المعلومات	الإخطار
ANSSI	**CNIL et ANSSI**	**CNIL**	لمن؟ سلطة الرقابة
بدون آجال	في غضون 72سا من اكتشاف الكارثة**CNIL** **ANSSI** : بدون آجال	في غضون 72سا من اكتشاف الكارثة.	الوقت الذي يجب احترامه للإخطار.

Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Les Essentiels de la banque et de la finance, RB Éditions, 2017, p 88.

2. تأمين الخطر السيبراني:

[31] Laure Zicry, Ibidem, p 88.

بعد تبيان ما هو الخطر السيبراني، وكيف يمكن عمل حماية داخلية ضد هذا النوع من الأخطار بسياسية إدارة المخاطر. يتم شرح في هذا المبحث قرار نقل الخطر السيبراني لشركات التأمين وذلك في مطلبين، مطلب أول يضم مفهوم عقد التأمين السيبراني بأركانه وآثاره ومطلب ثاني تم التطرق فيه إلى واقع السوق السيبراني في الدول الغربية والعربية كمقارنة.

1.2 عقد التأمين السيبراني :

من خلال هذا المطلب الأول نحاول فهم تطور عقود تأمين الإعلام الآلي إلى غاية العقد السيبراني للتأمين، وكذلك التعريف بهذا العقد وهذا ما تم تسمتيه بالإطار المفاهمي للعقد السيبراني للتأمين. ثانيا تم التطرق في هذا المطلب إلى الإطار القانوني للعقد السيبراني : أركان العقد السيبراني للتأمين و آثاره (إلتزامات المؤمن له و المؤمن).

1.1.2 الإطار المفاهمي للعقد السيبراني للتأمين :

يتم شرح في هذا الفرع تطور تأمين أخطار الإعلام الآلي، تعريف العقد السيبراني للتأمين..

تطور التأمين[32]: التأمين بدأ بضمان الأجهزة بوثائق تأمين من نوع كسر الماكينات، وهذا الجانب المادي من الإعلام الآلي (ضمان الأجهزة الوظيفية للإعلام الآلي من الأخطار). مع مرور الزمن تعقدت المسألة مع ضمان المعلومات نفسها. وهو الجانب الثاني في التعريف السابق للإعلام الآلي (المعلومات نفسها). من المجال المادي الملموس انتقلنا إلى المجال غير المادي، غير الملموس (العقد السيبراني للتأمين)[33].**تنوع عقود التأمين**[34]: هناك نوعين من العقود الخاصة حسب الأستاذ بيقو [35]، و4 عقود بالنسبة للمحامية والأستاذة الفرنسية **Laure Zicry**. الأستاذ بيقو: عقود كل مخاطر الإعلام الآلي[36]، **Tous risques**

---

[32] Jean Bigot, Traité de droit des Assurances, Assurance Dommages, Chapitre 3 L'Assurance des risques informatiques, Op cit, p 390.

[34] حسب تقديرنا هناك أكثر من 6 عقود في تأمين الإعلام الآلي (تأمين الأخطار السيبرانية الذي هو الجديد الذي يصيب المعلومات وغير ملموس كخطر وهو موضوع دراستنا، وهو عبارة عن تأمين هجمات إلكترونية من الداخل والخارج (الجريمة الإلكترونية). تأمين أخطار الإعلام الآلي التقليدية التي تصيب الأجهزة الذي هو ملموس كخطر هو عقد يغطي أضرار الأجهزة (الجانب المادي أولا) ، الأخطار التقليدية من حريق ، صواعق ، سرقة .والمعلومات كجانب ثاني في العقد (عند إصابة الجهاز تصاب المعلومات أيضا) و المسؤولية المدنية. ، تأمين الغش المعلوماتي خطر يشبه الخطر السيبراني إلى درجة كبيرة (سرقة و اختلاس المعلومات و الأموال من داخل المؤسسة (العمال) و خارجها .تأمين التهديد بالابتزاز عبر الأنترنت ، تأمين مسؤولية مستعملي الأنترنت ، تأمين مسؤولية المحترف في الإعلام الآلي.

[35] Jean Bigot, Traité de droit des assurances, Assurance Dommages, Op Cit, p 394.

[36] ليلة 10 مارس 2021 تم نشوب حريق في سيرفرات موقع استضافة كبير في فرنسا OVH ما تسبب في تعطل ملايين المواقع والبرامج الخاصة التي كانت تعمل على خوادم الشركة، في المقر بمدينة ستراسبورغ الفرنسية. و منه خسائر بملايين الدولارات لكثير من المواقع الإلكترونية على مستوى العالم (فقد الإستغلال) .وشركة OVH الفرنسية هي مؤسسة حوسبة سحابية فرنسية، تمتلك أكبر مركز بيانات في العالم في المنطقة السطحية، وأكبر مزوّد استضافة سيرفرات في أوروبا، وثالث أكبر مزوّد في العالم. نشب حريق بمركز البيانات OVH الذي يقع بمدينة ستراسبورغ شرق فرنسا، حيث تعطل نحو 3.6 ملايين موقع إلكتروني عبر الإنترنت. وقالت السلطات إنه من غير المحتمل أن يتم استرداد البيانات لهذه المواقع. وأتى الحريق على أجزاء مهمة من الوحدات، مما أدى إلى توقف العديد من المواقع الإلكترونية التي تستضيفها خوادم الشركة الفرنسية. السبب الأول من كل هذا الذي أدى إلى تعطيل المواقع الإلكترونية ، فقد الإستغلال و فقد البيانات هو الحريق الذي أصاب الشركة و ليس هجمات سيبرانية أو إلكترونية (كعقد التأمين السيبراني) على مركز بياناتها . فهنا نحن بصدد عقد تأمين الماكينات أو عقد تأمين العتاد الإلكتروني ، عقد تأمين أخطار الإعلام الآلي كلاسيكي يختلف عن عقد تأمين الأخطار السيبرانية ، لكن عنده نقاط تشابه مع هذا الأخير و منها إختفاء أو فقد المعلومات ، فقد الإستغلال .حسب موقع argus de l'assurance مبنى شركة OVH و العتاد مؤمن بعقد تأمين الأشياء عند AXA . وهناك عقد آخر للمسؤولية المدنية للشركة إتجاه زبائنها (أصحاب المواقع) الذين فقدوا بياناتهم الخاصة بالمواقع و كذلك فقد الأرباح (فقد الإستغلال) لم ترد الشركة التصريح حسب المقال ذاته أي شركة تأمين إكتتبت معها العقد .

SBG-1 مركز بيانات الشركة تضرر جزئيا جراء الحريق ، 4 بنيات تحتية على 12 تضررت و لهذا العديد من المواقع الالكترونية التي كانت معلقة بهذا المركز لم تكن في الخدمة.

informatiques TRI وتغطي الأجهزة، البرامج، وكل المصاريف اللازمة لإعادة إقلاع نشاط المؤسسة بعد أن تصيبها الكارثة. والعقد الثاني هو عقود امتداد أو ملحقة بأخطار الإعلام الآلي **informatiques ERI Extension des risques** وتغطي آثار أخطار احتيال الإعلام الآلي. أو تأمين الغش المعلوماتي وهو عقد يشبه العقد السيبراني للتأمين ويكون مضمون به أحيانا. **Tout comme le contrat Fraude Informatique** هاذين العقدين نستطيع جمعهم في عقد واحد و هو العقد الشامل للإعلام الآلي **Globale informatique**.

العقد السيبراني للتأمين (عقد موضوع الدراسة): Contrat Cyber–Risque[37]

تعريف العقد السيبراني للتأمين:نحاول وضع تعريف شامل بإسقاط التعريف القانوني للتأمين على تأمين الخطر السيبراني فنقول :« التأمين السيبراني عقد تأمين أضرار يكتتب بين المؤمن له و المؤمن ، يدفع الأول قسط تأمين (مبلغ من المال) ، و يدفع الثاني (شركة التأمين) في حال تحقق الخطر المبين في وثيقة التأمين مبلغ تأمين للمؤمن له (مكتتب العقد) أو المستفيد المبين في العقد و ذلك في ضمان الأضرار و المسؤولية المدنية عند رجوع الغير على المؤسسة أو الشخص الطبيعي (المؤمن له) (تعويض مالي) ، و مساعدة عينية لحل الأزمة السيبرانية (تعويض عيني) و ذلك بإرسال فريق خبراء في الإعلام الآلي عند حدوث الكارثة السيبرانية. نضيف للتعريف القانوني التعريف الفني: التأمين السيبراني هو عملية تأمينية يقوم بها المؤمن لتعويض أضرار الكارثة السيبرانية (جانب قانوني وجانب فني).» نستطيع القول إن هذا التعريف شامل.

2.1.2 الإطار القانوني للعقد السيبراني للتأمين

يشمل هذا الفرع من الدراسة شرح: أركان عقد التأمين السيبراني من رضا، محل وسبب وكذلك آثار العقد: إلتزامات المؤمن له والمؤمن.

أركان العقد السيبراني للتأمين:

1 إنعقاد العقد السيبراني للتأمين (التراضي) [38]

SBG–2 تضرر كليا و لهذا كل المواقع التي كانت على متن هذه الغرفة أو الطابق تعطلت و تضررت كليا. أما SBG–3 , SBG–4 لم تتضرر لكن تم إعادة إطلاق الخدمة بعد 24 ساعة من الحريق .

هنا نحن بصدد خطر كلاسيكي هو الحريق الذي أضر مبنى الشركة المستضيفة للعديد من المواقع عبر العالم ، و منه أضر الحريق عتاد الإعلام الآلي (أنظمة المعلومات) من سيرفيرات و مركز البيانات الإلكتروني ، و منه تضرر المعلومات التي كانت محمولة في هذا العتاد ، معلومات رقمية خاصة بأصحاب المواقع و منه تضرر المواقع و منه تضرر زبائن هذه المواقع و مدراء المواقع .. عبارة عن سلسلة أضرار غير مباشرة و مباشرة .

[38] Voir Aussi : Jean Bigot, Traité de droit des assurances, Le contrat d'assurance, 2e Edition, Tome 3, L.G.D.J, 2014, p7.
Voir aussi :
Laurence de Percin, L'Assurance pour les nuls, First, 2010, p 45.

ينعقد العقد السيبراني للتأمين ككل عقد تأمين الأشياء، من تلاقي الإيجاب والقبول، أهلية التعاقد، عدم وجود عيوب الرضا، الشكلية للإثبات فقط وليس شرطا للانعقاد. يمكن الرجوع لكتاب الأستاذ عبد الرزاق بن خروف بخصوص شرح هذه الأحكام العامة.[39]

2محل عقد التأمين السيبراني : عقد التأمين السيبراني ، ككل عقد أشياء محله هو الخطر. الخطر هو القصد الجنائي أو الخطأ الواقع على المعلومات ومنه تسبيب أضرار عدة للمؤمن له، فهذا هو محل عقد التأمين السيبراني. أما محل الشيء المؤمن هو المعلومات. ويجب شرح هذا الشيء المؤمن المميز عن باقي الأشياء المؤمنة.

المعلومات الشيء محل التأمين: ما هي أنواع المعلومات التي هي محل التأمين ضد الخطر السيبراني؟ [40]

1- المعلومات ذات الطابع الشخصي: كل المؤسسات تمتلك هذا النوع من المعلومات، وهي معنية بحمايتهم. ماذا نعني بالمعلومات ذات الطابع الشخصي؟ **المادة 2** من قانون الإعلام الآلي و الحريات ل 6 جانفي 1978 بفرنسا الفصل 2، الباب 1: تنص على التعريف التالي: « **البيانة ذات الطابع الشخصي هي كل معلومة ترتبط بكل شخص محدد (معروف الهوية) ، أو الذي نستطيع تحديد هويته ، مباشرة أو بطريقة غير مباشرة بالرجوع إلى رقم يحدد هويته أو بالرجوع إلى عناصر عدة ترتبط به. لكي يعرف أن شخص ما يمكن تحديده، يجب الإحاطة بجل وسائل تحديد الهوية، كالمعلومات الشخصية لهذا الشخص التي يمتلكها مسؤول معالجة البيانات.**» التعريف هذا واسع، ومجال البيانات ذات الطابع الشخصي ما لانهاية. إذن البيانات ذات الطابع الشخصي تتلخص في: اللقب، الاسم، عنوان المنزل، عنوان الإيمل، رقم الهاتف، الصور، الفيديوهات، بصمة الأصابع الرقمية، بطاقة التعريف، جوازات السفر، عنوان الإيبي ... إلخ

2- نوع المعلومات الثانية في المؤسسة : البيانات الاستراتيجية للمؤسسة [41]

أولا: المعلومات المرتبطة بالمؤسسة: معلومات عن صناديق الاستثمار هي محل استهداف من طرف القراصنة أيضا. بمناسبة العناية الواجبة أو التدقيق الإلزامي في المعطيات **Due Diligence**، المؤسسات المستهدفة، لها معطيات عن الشركات التي تريد شراءها أو بيعها.

نوع آخر من البيانات الاستراتيجية التي تكن محل استهداف: **بيانات البحث و التطوير Les données Recherche et développement , Research and Development R&D**.

أخيرا ... بيانات أخرى هي استراتيجية للمؤسسة ومنها:

- **1-**العقود المكتتبة مع الشركاء **Partenaires** لإطلاق خدمة جديدة أو عرض جديد.

---

[39] عبد الرزاق بن خروف، التأمينات الخاصة في التشريع الجزائري، دار الخلدونية، القبة القديمة، الجزائر، التأمينات البرية الجزء الأول، 2017 ص 109 وما يليها.
Voir aussi : Bernard Beignier, Sonia Ben Hadj Yahia, Droit des assurances, 2e édition, L.G.D.J, 2015, p 34.

[40] Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Op Cit, P23.

[41] Laure Zicry, Ibid, P26.

- **2–**العقود المكتتبة مع مزودي الخدمة **Prestataires**.
- **3–**الخطة الاستراتيجية أو خطة العمل**Business Plan** لتطوير المؤسسة.
- 4–الاستجابة لنداءات المناقصة **Réponse aux appels d'offres**.

الخطر والأضرار (محل العقد) يمكن إقتباسهم من ضمانات عقد أكسا السيبراني:

1الضمانات الأساسية:

خرق البيانات (المعلومات) أو الإضرار بها، سرقة البيانات الشخصية، فقد الإستغلال، ضمان المسؤولية المدنية للمؤمن له (المؤسسة) عندما يرجع عليها الزبائن التي سرقت معلوماتهم زعما أن المؤسسة لم تحمي نظام معلوماتها.

2 الضمانات الإضافية :

محاولة إبتزاز سيبراني (محاولة تهديد)، الاختلاس السيبراني، التجسس السيبراني الصناعي والاقتصادي، الإضرار بسمعة المؤسسة إلكترونيا، إنتحال شخصية المؤسسة والتكلم باسمها، نزاع مع زبون في الأنترنيت، مزود الخدمة.

الملاحظة والتعقيب:

كل هذه الضمانات (تعويض الأضرار التالية) لها إستثناءات عامة في العقد.و هناك إستثناءات خاصة بكل ضمانة[42] . عقد أكسا السيبراني يضمن هذه الأضرار، عندما يكون الخطر (السبب الأول) هو القصد الجنائي، أو الخطأ.

3 السبب في عقد التأمين السيبراني: ككل عقد تأمين أشياء ، تنطبق عليه الأحكام العامة المتعلقة بالسبب. وهو المصلحة المشروعة (الاقتصادية).[43]

[42] AXA Assurance. Piratage informatique, https://www.yesassurances.fr/cyber-secure-axa/, Accessed 2022.

[43]**دوافع نقل الخطر السيبراني إلى شركة التأمين:**

- هي إستراتيجية المؤسسة لكي تؤمن على نفسها من هذا الخطر وعدم ترك الأخطار التي يمكن نقلها إلى شركات التأمين على عاتقها.
- الميزة التنافسية: شهادة تأمين الخطر السيبراني مطلوبة للاستجابة إلى بعض دعاوى تقديم العطاء ات، فبدون هذه الشهادة المؤسسة لا يمكنها المنافسة.
- حماية كبيرة لميزانية المؤسسة، فبدون التأمين السيبراني، تتحمل المؤسسة جميع النفقات التي تنجر من آثار الخطر السيبراني أو الهجمات الإلكترونية. فالربح مضمون للشركة التي تكتتب هذا النوع من العقود إن حصل الخطر فعلا، فكل ما عليها هو دفع الأقساط ونسبة الاقتطاع، فكل المصاريف والنفقات التي يخلفها هذا النوع من الخطر النامي تتكبدها شركة التأمين.
- ضمان المؤمن له (المؤسسة) تسيير الكارثة من طرف الأشخاص ذات الكفاءة التي تعينهم شركة التأمين للمؤسسة: خبراء، مختصين، محاورين. بسرعة مثلا إخطار سلطة المراقبة 72 ساعة.

آثار عقد التأمين السيبراني :نرى في هذا الفرع الالتزامات التي تقع على المؤمن له والمؤمن بعد اكتتاب العقد، فهذه المرحلة تسمى تنفيذ العقد. **التزامات المؤمن له** تنص على التزامات المؤمن له المادة **15** من الأمر المتعلق بالتأمينات الجزائري. ومنها نستنتج أن الالتزامات[44]التي يرتبها عقد التأمين على عاتق المؤمن له هي:

- **1–**التصريح عند اكتتاب العقد بجميع البيانات و الظروف.
- **2–**التصريح بتغير الخطر أو تفاقمه.
- **3–**دفع الأقساط في مواعيدها.
- **4–**احترام الالتزامات و قواعد النظافة و الأمن.
- **5–**إخطار المؤمن بوقوع الخطر بتحققه.

بعجالة نشرح الالتزام الأول والرابع من التزامات المؤمن له لأن باقي الالتزامات هي نفسها كباقي عقود التأمين العامة.

1–التصريح عند اكتتاب العقد بجميع البيانات و الظروف (مبدأ الإعلام) :

التزام التصريح بالبيانات للمؤمن عقود أخطار الإعلام الآلي (التقليدية):[45]

يطرح المؤمن أسئلة عدة على المؤمن له (المؤسسة) (الخصائص، نوع النشاط، رقم حجم الأعمال.. إلخ)، وحتى الأشياء التي يراد تأمينها (وصفها، تصنيفها، الأقدمية، شروط الاستعمال) وحتى الإجراء ات المتخذة لحمايتها وأمنها المادي. موقعها، عزل المباني التي تحتوي الوحدة المركزية (السيرفرات) يعني مركز البيانات **Data Center**، والنسخ المحفوظة الحماية من الحرائق وسقوط الصواعق والمياه، الحماية من الكهرباء الساكنة التي تتكون نتيجة الاحتكاك وتناقل الشحنات بين جسمين مختلفين.

التزام التصريح بالبيانات للمؤمن في العقد التأمين السيبراني: المعلومات لا يمكن التصريح بها للمؤمن لسريتها، لكن هذه العقود تشترك مع العقود التقليدية في التصريح بالبرامج المستعملة و الأجهزة و حتى مفاتيح البرامج الخ...تضمن عقود الإعلام الآلي التقليدية استرجاع المعلومات بعد فقدها و هذا قاسم مشترك أكبر مع العقود الحديثة السيبرانية (فقد المعلومات و مشكلة استرجاعها).

–احترام الالتزامات و قواعد النظافة و الأمن[46]

هذا الالتزام مشدد في هذا النوع من التأمينات سواء في العقود التقليدية للإعلام الآلي أو العقد السيبراني للتأمين (العقد الجديد) مقارنة بالتأمينات الأخرى.

---

[44]عبد الرزاق بن خروف، التأمينات الخاصة في التشريع الجزائري، دار الخلدونية، القبة القديمة، الجزائر، التأمينات البرية الجزء الأول، 2017 ص 135.

[45] Jean Bigot, Traité de droit des assurances, Assurance Dommages, Chapitre 3 L'Assurance des risques informatiques, Tome5, LGDJ, 2017, p 395.

[46]عبد الرزاق بن خروف، مرجع سابق، 2017 ص165.

1 **الالتزام بالوقاية والأمن في العقود التقليدية لتأمين الإعلام الآلي (الجانب المادي)**: بخصوص التنصيبات المهمة الكبرى لأجهزة وبرامج الإعلام الآلي في المؤسسات، يستطيع المؤمن أن يقوم بالتحري في المؤسسة بواسطة خبراء لمعاينة محل المؤسسة وهذا لتقييم الخطر والنصح بمقاييس الوقاية والحماية. الصيانة إبقاء المعدة أو الجهاز أو الآلة تعمل في حالة جيدة عبر الفحص والإصلاح. تعرف الصيانة على أنها اكتشاف الأعطال وتشخيصها ثم إصلاحها أو استبدال الأجزاء العاطلة ثم التأكد من تمام الإصلاح بكل الوسائل المتاحة لتأكيد جودة الإصلاح والمعايرة على مقاييس الجودة المتوفرة إن أمكن.

2 **الالتزام بالوقاية والأمن في العقد السيبراني للتأمين** : لن يتم منح الضمانات إلا في حالة احترام الإجراء ات الوقائية التالية : وهذه إجراء ات وقائية حسب عقد **Verspieren**:[47]

1–يكون تسجيل الدخول بشبكة الكمبيوتر عبر كلمة مرور تحتوي على 8 أحرف على الأقل.

2–يتم تحديث البرامج والتطبيقات المستخدمة وفقًا لما يوصي به الناشر (لا يكون التحديث من موقع غير الموقع الرسمي للبرنامج).

3–يتم تثبيت برنامج مكافحة الفيروسات وجدار حماية على نظام المعلومات وتحديثها تلقائيا.

4–يتم إجراء نسخ احتياطي أسبوعي **backup** كحد أدنى من بيانات الكمبيوتر على وسائط خارجية وتخزينها في خارج المؤسسة.

5– يتم إحاطة و توعية موظفي مكتب المحاسبة بالمخاطر والتهديدات المرتبطة بالهجمات السيبرانية.

التزامات المؤمن (شركة التأمين في العقد السيبراني للتأمين) :ثلاث أنواع كبرى من التغطيات ألا وهي: [48]

1. ضمانات المساعدة وتسيير الكارثة (تعويض عيني):

تكاليف المساعد والمستشار في تسيير الكارثة: [49]

عندما يكتشف المؤمن له (المؤسسة) الكارثة السيبرانية التي حلت به، في غالب الأحوال يقع في حالة هيستيريا لا يستطيع التحكم في الكارثة، فلن يجد سريعا الأشخاص ذات الكفاءة التي تستطيع التحكم في الكارثة. ولن يعرف الالتزامات التي تقع على عاتقه عند حدوث كارثة سيبرانية. لهذا يجب اكتتاب عقد تأمين سيبراني، لأن من بين الضمانات التي يقترحها هي ضمانات المساعدة، حيث لشركة التأمين خبراء و مختصين في تسيير الكارثة معترف بهم .فتغطي له شركة التأمين مختلف تكاليف هذه الخبراء. أول شيء، مباشرة ترسل له هذه الخبراء للتحكم في الأزمة السيبرانية.

---

[47] VERSPIEREN, CONTRAT D'ASSURANCE COLLECTIVE CYBER RISQUES, Conditions générales, 2022, https://reassurez-moi.fr/guide/wp-content/uploads/2021/01/assurance_cyber_risques_mma_cg.pdf .Accessed 15 Dec 2022.

[48] Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Les Essentiels de la banque et de la finance, RB Editions, 2017, p 109.

[49] Laure Zicry, Ibid, p 110.

2ضمانات المسؤولية المدنية : [50] مسؤولية المؤسسة تستطيع أن تقوم :

1. انتهاك سرية معلومات زبائن وعمال المؤسسة (موقع مثلا) من طرف الهاكر وذلك بإغفال المؤسسة جانب الحماية على نظام معلوماتها.
2. عدم احترام التزامات السرية من طرف المؤسسة، التي اكتتبتها بموجب عقد أو مفروضة بالقانون.
3. في فرنسا وأوربا، عدم احترام التزامات التنظيم العام لحماية المعلومات**GRPD** 25 ماي 2018 مثلا: التزام الإخطار عند حصول الكارثة السيبرانية من طرف المؤسسة.

هذا بخصوص مفهوم مسؤولية المؤسسة، لكن فيما يخص تأمين مسؤولية الشركة عن الكارثة السيبرانية، يغطي المؤمن أتعاب ومصاريف المحامي ويعوض ضحايا المؤمن له التي طالبته بالتعويض عن الضرر المعنوي والمالي الذي أصابها.

3 تأمين الأضرار: [51] المؤسسة التي حلت بها الكارثة، يجب عليها ليس فقط التحكم في الهجمة الكارثة بل حتى تبرير مسؤوليتها عند رجوع الزبائن التي سرقت معلوماتهم عليها، ويجب عليها تغطية الأضرار التي أصابتها، لأنها مسؤولة وضحية في نفس الوقت. تستطيع فقد الاستغلال أي نشاطها يتأثر و تخسر أموال كبيرة في فترة الكارثة السيبرانية لأن نشاطها توقف، و تستطيع أن تخسر أموال أيضا عندما تكون ضحية ابتزاز سيبراني بهجمة لحجب خدمتها أو فيروس نزع الفدية **Cyber Extorsion** (..**Ransomeware , Attack DDOS**)شركة التأمين تغطي كل الخسائر المالية التي تتكبدها المؤسسة المؤمنة لها في فترة الكارثة السيبرانية وتساعدها على إعادة إقلاع نشاطها في أسرع وقت ممكن فتغطي التكاليف الإضافية للاستغلال، وتتحمل أيضا فقد الاستغلال (خسارة هامش الربح).

2.2 سوق التأمين السيبراني :

للثقافة التأمينية، يتم التطرق إلى واقع سوق التأمين السيبراني في العالم الغربي في فرع أول والعربي في فرع ثاني من خلال هذا المطلب.

1.2.2 السوق السيبراني للتأمين في الدول الغربية :

ظهر هذا المنتوج التأميني في الولايات المتحدة الأمريكية أول مرة. أين سوق المعلوماتية كان معروف من قديم.[52]

سريعا كان يجب إضفاء الحماية على معلومات المستهلكين لأنظمة المعلومات. فشرعت قوانين لحماية المعلومات في أمريكا، تحدد هذه القوانين مختلف الالتزامات التي تقع على المؤسسات التي تملك في أنظمة معلوماتها لمعلومات ذات الطابع الشخصي والسري عندما لا تحمي هذه المعلومات والتي سمحت بتسريبها. على غرار عقود تأمين مسؤولية مديري أو رؤساء المؤسسة، عقد التأمين السيبراني في أمريكا، تم عمل نسخ لصق له في أوربا. كان أول بلد محتضن لهذا السوق التأميني هو إنجلترا، لأن لهم نفس اللغة

---

[50] Laure Zicry, Ibid, p 116.
[51] Laure Zicry, Ibid., p 118.
[52] Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Op.cit., p 107.

(الإنجليزية) مع أمريكا، دول الكومنولث، خصص هذا السوق مع الأول للأمريكيين العاملين في إنجلترا، ولم يجدوا أين يؤمنوا أنفسهم ضد هذا الخطر عند مجيئهم. سنوات فيما بعد، عقود التأمين السيبراني وصلت إلى فرنسا. السوق بدأ إقلاعه حوالي نهاية سنة 2010، بداية 2011.. لكن لم يقلع جيدا حتى سنة 2013، لأن المؤسسات لم تقدم على هذا المنتوج، والقليل منها كان واعيا بعواقب الأخطار السيبرانية وآثارها، ظنا منهم أن خلية إدارة الأخطار السيبرانية داخل المؤسسة ستوقف جميع الآثار، بما في ذلك ضمان فقد الاستغلال بعد كارثة سيبرانية. ضنا منهم أيضا أنهم لن يتعرضون إلى كارثة سيبرانية.. وبدون التشاور مع مسؤولي حماية نظام المعلومات داخل المؤسسة. توسع انتشار بيع عقود التأمين السيبرانية، بعد الكوارث السيبرانية التي صارت في أوربا، خاصة بعد ظهور برنامج نزع الفدية **Ransomeware** الذي أفلس الكثير من المؤسسات. حيث الضمانات التي أصبحت مقترحة في عقود التأمين السيبرانية تتماشى كثيرا مع آثار الأخطار السيبرانية وتشملها مع فرق طفيف في الضمانات من مؤمن إلى آخر في قائمة الضمانات. أكثر من 10 مؤمنين في فرنسا[53]، يقترحون هذا المنتوج بمبلغ يفوق 500 مليون أورو بالنسبة إلى الضمانات.[54] هناك من الزبائن (المؤسسات خاصة والقليل من الأشخاص الطبيعية) من يشترون قيمة ضمانات ضعيفة بعض الشيء بالنسبة إلى البعض الآخر (2 مليون، 5 مليون يورو)، وهناك من يشتري حتى 100 مليون يورو (المؤسسات الكبرى)، وحتى المؤسسات الكبرى والصغيرة تشتري هذه الضمانات.

2.2.2.السوق السيبراني في الجزائر (مشروع قيد الإنجاز) : سوق تأمين أخطار الإعلام الآلي التقليدية (الأجهزة واسترجاع المعلومات) في الجزائر موجود منذ مدة. ومع هذا كانت الشركة الوطنية للتأمين وإعادة التأمين **CAAR** [55] السباقة لإدخال هذا النوع من التأمينات في التسعينات 90 [56] ويضمن حماية أجهزة المؤسسات وأجهزة الأشخاص الطبيعيين، وحتى استرجاع معلوماتهم ومفاتيح البرامج إلخ ... هذا بخصوص الأخطار التقليدية التي تضر بالأجهزة (الحريق، السرقة، أضرار المياه، الصواعق ... إلخ)، كلها أخطار ملموسة ويمكن رؤيتها. أما بخصوص موضوعنا، تأمين الخطر السيبراني هو قطاع مستقبلي في سوق التأمين الجزائري، يكون كحل وتهيئة لأرضية رقمنه القطاعات في الجزائر، فالرقمنة لا تخلو من الآثار السلبية. ليس هناك في الجزائر شركة تؤمن ضد الخطر السيبراني لكن هو مشروع جديد لأن هناك فراغ كبير في هذا القطاع يجب سده، فهناك الكثير من العوائق التي تعيق هذا القطاع حتى في أوربا. كما تم سن قوانين ومراسيم جديدة تكلمت عن حماية المعطيات ذات الطابع الشخصي، وحماية معلومات الركاب، والمعلومات الإدارية

---

[53] AGCS, AIG Europe, AXA Corporate Solutions, AXA France, Beazley, CHUBB, CNA Hardy, Hiscox, Mitsui, MRCIP, Tokio Marine HCC, QBE, XL Catlin, Swiss Re International Zurich.

[54] Laure Zicry, Ibid, p 108.

[55] Voir aussi : **Nebbache Melkheir NORIA,** Assurance des risques informatiques, Voir : Partie : Experience de la CAAR Dans le domaine, Institution de parrainage : Compagnie Algérienne d'Assurance et de réaussurance (CAAR), Institut de financement du développement du Maghreb Arabe, 1992.
Aussi : **Benmicia Youcef,** Assurance des risques informatiques, Institution de parrainage : Compagnie Algérienne d'Assurance et de réaussurance (CAAR), Institut de financement du développement du Maghreb arabe, 1992.

[56] Voir : CAAR,"**Tous Risques Informatiques - CAAR", 2022, https://caar.dz/tous-risques-informatiques/.** Accessed 15 Dec 2022.

Voir aussi :*Caar.Dz, Conditions générales, ASSURANCE PETITS SYSTEMES INFORMATIQUES*, **https://caar.dz/wp-content/uploads/2017/03/petits_systemes_informatiques.pdf. Accessed** 15 Dec 2022.

وأنشئت لجنة لحماية الأنظمة المعلوماتية في الجزائر[57] وهناك الكثير من التطور الحاصل في الموضوع. نظمت الشركة المركزية لإعادة التأمين يوم دراسي أو أيام دراسية تتكلم فيها عن الأخطار النامية. والخطر السيبراني بالخصوص، قال رئيس مجلس إدارة الشركة إنه من المهم معرفة نتائج التجارب الأجنبية والسويسرية والفرنسية والألمانية في إدارة المخاطر الجديدة (الأخطار النامية).[58]

3.2.2.دول العالم العربي : هناك القليل جدا من الشركات التي تقوم بهذا النوع من التأمينات، بالخصوص في دول الخليج.[59]

دور الاتحاد المصري للتأمين[60]سيقوم الاتحاد المصري للتأمين بدراسة هذا النوع من التأمين من خلال الحصول من الأسواق العالمية على العديد من وثائق تأمين الجرائم الالكترونية ودراستها باللجان المختصة بالاتحاد لإعداد منتج جديد يتناسب مع السوق المصري. تعد أكبر مشكله لترويج هذا النوع من التأمين هي إقناع العملاء في مصر بهذا النوع من التأمين وعلى الجانب الآخر تقع المسئولية على أطراف العملية التأمينية (شركات التأمين والوسطاء والهيئة) كل في دوره لنشر الوعي بين الفئات المستهدفة للتعريف بهذا النوع من التأمين وأهميته في التخفيض من مواجهة هذه المخاطر.

الخاتمة:

الخطر السيبراني خطر نامي يتمثل في الهجمات الإلكترونية التي تصيب المعلومات ويتميز على الأخطار الأخرى القابلة للتأمين بخصائص خاصة منها: أنه خطر غير مادي، غير ملموس، وغير مرئي ويتم اكتشافه بعد مدة من حدوثه

هذا ما يبين صعوبة تأمين هذا الخطر وأن شركات التأمين قبلت بهذا الخطر تدريجيا ولم تقترب منه إلا بحذر. محل الأشياء المؤمنة التي تقع عليها الأخطار هاته هي المعلومات وتم تبيان تصنيفاتها وتقسيماتها وأنها ذات قيمة اقتصادية. كما أنها تقيم بقيمة استرجاعها وهذا حسب الأستاذ الفرنسي **Jean Bigot** المعروف في مجال التأمينات.

عقد التأمين السيبراني هو عقد تأمين أشياء تطبق عليه أحكام تأمينات الأضرار، فهو عقد تأمين أضرار (أشياء ومسؤولية)، وهو منتوج مستقبلي في الجزائر والوطن العربي كما أن من بين الضمانات التي يمنحها هذا العقد، أولا ضمانات عينية تتمثل في إرسال شركات التأمين لخبراء حماية الإعلام الآلي للمؤمن له المتضرر يوم وقوع الكارثة السيبرانية للتحكم فيها. وثانيا ضمانات نقدية يدفعها المؤمن مثل

---

[57]مرسوم رئاسي رقم 20-05 ممضي في 20 جانفي 2020 وزارة الدفاع الوطني، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية عدد 4 مؤرخة في 26 جانفي 2020، الصفحة 5.

[58] Voir : *Hiscox*, Novembre 2016 Séminaire de la CCR – Alger, https://www.ccr.dz/images/pdf/seminaire1.pdf. Accessed 15 Dec 2022. *Voir aussi : Ccr*, "La Protection Des Entreprises Contre Les Risques Émergents - Compagnie Centrale De Réassurance (CCR)". *Ccr.Dz*, 13 Janvier 2018, https://www.ccr.dz/fr/component/k2/item/39-assurances-un-seminaire-fait-le-point-sur-la-protection-des-entreprises-contre-les-risques-emergents. Accessed 15 Dec 2022.

[59] Voir : *Insurancemarket.Ae*, 2022, "Cyber Security Insurance", https://insurancemarket.ae/cyber-security-insurance/. Accessed 15 Dec 2022.

[60] Mr. Alexander Blom, موقع الإتحاد المصري للتأمين,التأمين ضد الجرائم الإلكترونية , https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1251. Accessed 15 Dec 2022.

مصاريف إعادة إقلاع النشاط، استرجاع المعلومات وإدارة الدعاوى الناشئة عن رجوع الغير بدعوى جماعية ضد المؤمن له لعدم حماية معلوماتهم. **تم التوصل في هذه الدراسة للنتائج التالية :**

–أن المعلومات أشياء معنوية ذات القيمة الاقتصادية صعبة التأمين عليها نظرا لخصائصها غير الملموسة، والصعبة التصريح بها نظرا لسريتها في الكثير من الأحيان واستثناءا يمكن وفقا لشروط تم ذكرها أعلاه. كما أنها تقيم بقيمة استرجاعها.

–يقع الخلط في الكثير من الأحيان بين مختلف عقود تأمين أخطار المعلوماتية، فهناك عقود كلاسيكية منها تأمين أخطار الإعلام الآلي المتعلق بالأخطار التي تصيب الأجهزة والمعلومات بطريقة غير مباشرة وهناك عقود جديدة منها عقد التأمين السيبراني التي تصيب مباشرة المعلومات، فيجب على الطرف الضعيف في التأمين فهم مضمون العقود جيدا قبل اكتتابها.

–منتوج تأمين الخطر السيبراني لا يزال منتوج جديد في الدول الغربية، أما في الدول العربية فهو شبه منعدم الاكتتاب نظرا لغياب الثقافة التأمينية. **ومنه نقدم بعض الاقتراحات:**[61]

- تسريع تطوير الثقافة المتعلقة بالخطر السيبراني.
- قراءة جيدا محتوى عقود التأمين السيبراني قبل إبرامها (الضمانات والاستثناءات...).
- التحضير لأرضية دخول نظام الدفع العالمي بالجزائر (بالمعايير الدولية) خاصة من جانب أمن هذا النظام قبل تنصيبه، فالتأمين على المعلومات هو وسيلة لأمن أنظمة معلومات البنوك.
- الحث على الأخذ بآليات جديدة تتواكب مع هذه الجرائم الحديثة وليس فقط سن قوانين وعدم تطبيقها.
- تجميع البيانات الناتجة عن الحوادث السيبرانية (جمع قاعدة بيانات إحصائية للكوارث السيبرانية).

[61] بغدادي شامبي، تأمين وإدارة الأخطار السيبرانية، مذكرة لنيل شهادة الماستر في قانون التأمينات، جامعة الجزائر 1، 2018، ص 173.