Articles in Press

Clarifying War-Related Cyber Risk Exclusions in Cyber Insurance: A Comparative Legal Analysis of Contractual Validity and Societal Implications

Loay Alosh, Ashraf Aladwan

PII: 1376.2025

DOI: https://doi.org/10.35192/jjoas-h.1376.2025

Reference: JJOAS-H 1376.2025

To appear in: Jordan Journal of Applied Science-Humanities Science Series

Received Date: 24 Jun 2025

Revised Date: 22 Aug 2025

Accepted Date: 28 Aug 2025

Please cite this article as: Alosh, L. M. & Aladwan. A. I. (in press Clarifying War-Related Cyber Risk Exclusions in Cyber Insurance: A Comparative Legal Analysis of Contractual Validity and Societal Implications. *Jordan Journal of Applied Science – Humanities Series*. Advance online publication. https://doi.org/10.35192/jjoas-h.1376.2025

This is a PDF of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability. This version will undergo additional copyediting, typesetting and review before it is published in its final form. As such, this version is no longer the Accepted Manuscript, but it is not yet the definitive Version of Record; we are providing this early version to give early visibility of the article.

Please also note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Articles in Pre

Clarifying War-Related Cyber Risk Exclusions in Cyber Insurance: A Comparative Legal Analysis of Contractual Validity and Societal Implications

خصوصية أحكام الاستبعاد الاتفاقي للمخاطر الإلكترونية الناشئة عن الحروب من تغطية عقد التأمين السيبراني: دراسة تحليلية مقارنه

Loay Mustafa Alosh[1*], Ashraf Ismail Aladwan[1]

[1]The University of Jordan, Amman, Jordan

Loayalosh40@gmail.com[*]

Abstract

This study examines the legal validity of contractually agreed exclusions of war-related cyber risks from cyber insurance coverage, in light of the rising frequency of state-sponsored cyber-attacks and the contractual, legal, and societal challenges they pose. It evaluates the extent to which such exclusion clauses align with general principles of contract law, particularly good faith and contractual balance, and assesses their implications for the protection of insured parties and the stability of digital economic activity.The study highlights the conceptual ambiguity surrounding key terms commonly used in cyber insurance policies, such as “cyber warfare” and “hostile cyber operations,” and analyzes how this ambiguity affects the allocation of rights and obligations between insurers and insureds. Methodologically, the research adopts a descriptive-analytical approach to relevant legal texts and insurance contracts, combined with a comparative analysis of regulatory models and leading international case law, notably Mondelez v. Zurich and Merck v. ACE, in order to ground the discussion in practical disputes. The findings show that current exclusion clauses suffer from significant vagueness, which results in inconsistent judicial interpretations and enables insurers to avoid liability on uncertain or contested grounds, especially when attribution of cyber-attacks to sovereign actors is inconclusive. Judicial precedents tend to interpret such clauses narrowly where policy wording is unclear or where state responsibility is not firmly established. The study recommends: (1) enacting clear legislative definitions of “cyber warfare” and related concepts; (2) adopting standardized cyber insurance contracts with precise exclusion language; (3) requiring reliance on neutral, expert technical reports rather than political judgments in attributing cyber incidents; and (4) enhancing regulatory oversight to ensure transparency and fairness in the digital risk market. By doing so, the research contributes to the applied humanities and legal studies literature on how law, technology, and insurance practices can be aligned to better manage cyber risks and protect economic and social interests in an increasingly digitized world.

Keywords: Applied Legal Studies, Cyber Insurance, Cyber War, Cyber-Attacks.

الملخص

هدف هذا البحث إلى تحليل مدى مشروعية الاستبعاد الاتفاقي للمخاطر الإلكترونية ذات الطابع الحربي من تغطية عقد التأمين السيبراني، في ظل تصاعد الهجمات السيبرانية المدعومة من دول، وما تثيره من إشكاليات تعاقدية وقانونية. وقد ركّز البحث على تقييم مدى توافق هذه البنود مع المبادئ العامة للعقود، لا سيما مبدأي

Articles in Press

حسن النية والتوازن العقدي، مع تسليط الضوء على غموض المفاهيم المستخدمة في عقود التأمين، مثل "الحرب السيبرانية" و"العملية العدائية الإلكترونية"، وأثر هذا الغموض على حقوق المؤمن لهم. اعتمد البحث المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية والعقود التأمينية ذات الصلة، مدعومًا بمنهج مقارن استعرض نماذج تنظيمية وسوابق قضائية دولية، أبرزها قضيتي *Mondelez v. Zurich* و*Merck v. ACE*، مما أضفى بعدًا تطبيقيًا عمليًا على الدراسة. وقد توصّل البحث إلى عدة نتائج، أبرزها أن بنود الاستثناء الحالية تعاني من غموض مفاهيمي واسع، يؤدي إلى تباين في التفسير القضائي، ويتيح لشركات التأمين التنصل من التغطية بغير وجه مشروع. كما أظهرت السوابق القضائية ميلاً لتقييد تطبيق هذه البنود في حال غياب الصياغة الدقيقة أو الإسناد القاطع للهجوم إلى جهة سيادية. وأوصى البحث بضرورة سنّ تشريع يعرّف "الحرب السيبرانية" بشكل دقيق ويُحدّد شروط الإسناد القانوني المرتبط بها، بما يضمن وضوح نطاق استثناء التغطية. كما تدعو إلى اعتماد نماذج عقدية موحّدة تتضمّن استثناءات مصاغة بدقة تراعي خصوصية الهجمات السيبرانية، وإلزام شركات التأمين بالاعتماد على تقارير فنية محايدة عند التذرّع بالاستثناء، بعيدًا عن التقديرات السياسية غير الملزمة. وتشدد على أهمية تدخل الجهات الرقابية لفرض شفافية أكبر في صياغة حدود التغطية بلغة واضحة ومباشرة، إلى جانب دعم البحث القانوني المتخصص لتطوير قواعد تفسير حديثة تتماشى مع طبيعة الأخطار الرقمية المتجددة.

الكلمات المفتاحية: الدراسات القانونية التطبيقية، القانون، التأمين السيبراني، الحرب السيبرانية، الهجمات الإلكترونية.

المقدمة

في ظلّ التحوّل الرقمي المتسارع الذي يشهده العالم، غدت الفضاءات السيبرانية ميدانًا جديدًا للصراعات، حيث لم تعد الهجمات الإلكترونية مجرّد تهديدات معزولة، بل أصبحت أدوات استراتيجية ضمن منظومات الحرب الحديثة. ومع تصاعد الهجمات ذات الطابع العدائي، ولا سيّما تلك التي تُنسب أو يُشتبه في ارتباطها بدول ذات سيادة، برزت تحديات قانونية أمام قطاع التأمين، خصوصًا فيما يتعلق بمدى التزام شركات التأمين السيبراني بتغطية الأضرار المترتبة على مثل هذه المخاطر.

وقد اتجهت معظم عقود التأمين السيبراني إلى استبعاد التغطية في حالات "الحرب" أو "الأعمال العدائية"، استنادًا إلى بنود تقليدية صيغت أساسًا للنزاعات المسلحة الكلاسيكية. غير أنّ تطبيق هذه البنود على الهجمات السيبرانية يثير إشكاليات مفاهيمية؛ إذ تفتقر الظواهر السيبرانية الحديثة لتعريفات دقيقة في الإطارين القانوني والتعاقدي، مثل مفهوم "الحرب السيبرانية" أو "الهجوم العدائي الإلكتروني". وتزيد الطبيعة العابرة للحدود لهذه الهجمات وصعوبة تحديد مرتكبيها بدقة من تعقيد المسألة، ما يدفع شركات التأمين إلى التحفّظ أو فرض شروط مالية مشدّدة (Rovetto, 2022).

وقد مثّلت قضايا بارزة، مثل قضية *Mondelez International v. Zurich Insurance*[1]، نموذجًا حيًا لهذا الإشكال؛ إذ رفضت شركة التأمين التعويض عن هجوم سيبراني بحجة كونه عملاً حربيًا مدبّرًا من قبل دولة، ما أثار نزاعًا قانونيًا حول مدى مشروعية هذا الاستبعاد وإمكانية نسب الفعل العدائي إلى جهة سيادية، فضلًا عن الجدل حول مدى تكييفه قانونًا ضمن مفهوم "الحرب" (Shackelford, 2024).

ومن هنا يسعى هذا البحث إلى تحليل خصوصية الاستبعاد الاتفاقي للمخاطر الإلكترونية الناشئة عن الحروب، عبر تناول ماهية التأمين السيبراني كأساس مفاهيمي يوضح الإطار العام للعقود المبرمة في هذا المجال، ثم التعمق في دراسة تحليلية لقضية *Mondelez v. Zurich* بوصفها نموذجًا قضائيًا بارزًا يعكس التحديات العملية لتطبيق استثناء الحرب في السياق السيبراني، وصولًا إلى بحث التوجهات الحديثة التي تبنّاها القضاء وشركات التأمين في معالجة مسألة استبعاد مخاطر الحرب السيبرانية في ضوء المتغيرات التقنية والقانونية المستجدة.

١,١ الدراسات السابقة

شهدت السنوات الأخيرة تزايدًا ملحوظًا في الاهتمام الأكاديمي بتنظيم التأمين السيبراني، خاصة فيما يتعلق بالاستثناءات المتعلقة بالحرب السيبرانية، وفي هذا السياق، تأتي دراسة إسماعيل (٢٠٢١) لتتناول الإطار القانوني المنظم للتأمين الإلكتروني ضد المخاطر السيبرانية، مع التركيز على المشكلات القانونية التي تعيق فاعلية هذا النوع من التأمين في ظل غياب تشريعات عربية واضحة، وعلى رأسها قطر. اعتمدت الدراسة المنهج التحليلي المقارن، حيث قامت بتحليل النصوص القانونية ذات الصلة في القانون القطري وبعض القوانين الأجنبية، واستعرضت

نماذج العقود التأمينية المتداولة عالميًا. وقد كشفت نتائجها عن قصور تشريعي واضح، خاصة فيما يتعلق بغياب تعريف دقيق للمخاطر السيبرانية، وأوصت بإعداد نماذج عقدية موحدة تتضمن استثناءات الحرب بصياغات دقيقة، وسنّ تشريع خاص للتأمين السيبراني.

تُظهر الدراسة أهمية الضبط التشريعي لبنود الاستثناء، غير أن تركيزها ظلّ مقصورًا على الجانب المعياري دون التعمق في الأبعاد القضائية التطبيقية. وتتمثل قيمتها في إبراز الحاجة إلى تعريفات دقيقة وصياغات واضحة، وهو ما يشكّل أساسًا للبحث الحالي.

وفي إطار متصل، هدفت دراسة (Albalawi, 2025) إلى تقييم فاعلية القواعد القانونية التقليدية في التعامل مع تحديات المخاطر السيبرانية، خاصة لدى الشركات الصغيرة والمتوسطة. اتبعت الدراسة المنهج التحليلي المقارن، من خلال تحليل التشريعات الأجنبية والعربية ومضامين وثائق التأمين السيبراني، مع التركيز على صعوبة تحديد المسؤولية القانونية للهجمات الإلكترونية. وانتهت الدراسة إلى أن التشريعات القائمة تعاني من فجوات واضحة في التعامل مع خصوصية الحرب السيبرانية.

ركّزت الدراسة على أثر المخاطر السيبرانية على الـSMEs من منظور تشريعي، لكنها لم تتناول بعمق إشكاليات التفسير القضائي لبنود الاستثناء، كما تكمن أهميتها في بيان أثر الغموض على الفاعلين الأضعف تفاوضيًا، وهو ما يعزز ضرورة التوازن العقدي.

أما دراسة (He et al., 2025) فقد ركزت على الإشكاليات التي تثيرها البنود الاستبعادية للمخاطر الإلكترونية ذات الطابع الحربي، ودرست مدى توافقها مع المبادئ القانونية كحسن النية والتوازن العقدي. اعتمدت الدراسة على تحليل بنود الاستثناء في العقود، مع دراسة الاجتهادات القضائية، خصوصًا قضية Mondelez ضد Zurich. وقد أظهرت النتائج أن الصياغات التقليدية لبنود الاستثناء لا تستوعب طبيعة الهجمات السيبرانية الحديثة، كما كشفت عن غموض قانوني وتفاوت في التفسير القضائي. وأوصت بإعادة صياغة تلك البنود بشكل دقيق يعكس الواقع السيبراني الجديد.

عالجت الدراسة أوجه القصور في الصياغات التقليدية بجدارة وربطتها بالاجتهادات القضائية، ما يجعلها مرجعًا مهمًا، غير أن اعتمادها على نماذج أنجلو-أمريكية يحدّ من تعميم نتائجها، الأمر الذي يستدعي مراعاة خصوصية النظم العربية.

وتأتي دراسة (Cremer et al., 2024) لتسلط الضوء على سوق التأمين السيبراني الألماني، خاصة فيما يتعلق بتأثير بند استثناء الحرب على الشركات الصغيرة والمتوسطة خلال الحرب الروسية الأوكرانية. استخدمت الدراسة نهجًا متعدد الأدوات، جمع بين تحليل ٤٤ وثيقة تأمين ومقابلات مع ٢٦ خبيرًا في المجال. وتوصلت إلى أن بنود الاستثناء تُصاغ بشكل غامض، ولا تأخذ بعين الاعتبار تطور مفهوم الحرب ليشمل العمليات الهجينة والسيبرانية.

قدّمت الدراسة قيمة للواقع الألماني بأدوات ميدانية ووثائقية، وأظهرت أثر الغموض على السوق، غير أن خصوصية السياق تحدّ من التعميم، لكنها تبقى مفيدة في إبراز الحاجة إلى معايير أوضح.

من جانب آخر، ركزت دراسة (Shackelford, 2020) على مدى وضوح هذه البنود وتماشيها مع مبدأ الشفافية. اتبعت الدراسة المنهج التحليلي المقارن، من خلال تحليل وثائق تأمينية واجتهادات قضائية من الولايات المتحدة والمملكة المتحدة، مع مقارنة بالممارسات المعتمدة في سوق لويدز والأنظمة العربية. وأظهرت الدراسة وجود غموض في تعريف الهجوم الحربي، مما يترك مجالاً واسعًا للتأويل، ويدفع إلى نزاعات قضائية غير متجانسة. وأوصت بصياغة نماذج معيارية موحدة، ووضع معايير دقيقة لتحديد الطبيعة الحربية للهجمات الإلكترونية.

شكّلت الدراسة مدخلًا مبكرًا لبحث حدود استثناء الحرب في البيئة السيبرانية، مع التركيز على مبدأ الشفافية. إلا أن حداثة التطورات اللاحقة تجعل نتائجها بحاجة إلى تحديث، ومع ذلك تظلّ مرجعًا أساسًا في النقاش.

يُلاحظ أن العديد من تلك الدراسات قد أظهرت اهتمامًا متزايدًا بإشكالية التأمين السيبراني، إلا أنها قد عالجت الموضوع من منظور عام أو في إطار تأميني تقليدي لا يعكس خصوصية السياق السيبراني بالكامل، كما أن بعضها انحصر في المعالجة النظرية أو التشريعية دون استحضارٍ كافٍ للتطبيقات القضائية التي تمثل مسرحًا حقيقيًا لتفسير هذه البنود محل النزاع. بالإضافة إلى ذلك، لم تولِ معظم هذه الدراسات اهتمامًا كافيًا للبعد العقدي

Articles in Press

التفصيلي، لاسيّما ما يتعلق بمبدأ حسن النية والتوازن العقدي، ومدى انعكاس غموض بنود الاستبعاد على حقوق المؤمن لهم.

في هذا السياق، يتميّز البحث الحالي بأنه لا يكتفي بتوصيف الإشكاليات العامة، بل ينطلق من تحليل دقيق للبنية القانونية لعقود التأمين السيبراني، وتفكّك الطبيعة الخاصة للاستثناءات المرتبطة بالحرب، ويبرز أثرها على التوازن بين الأطراف، كما يستند إلى تحليل واقعي معمّق لحالات قضائية معاصرة مثل قضية Mondelez v. Zurich، مما يضفي على نتائجه طابعًا عمليًا مباشرًا، وتمتد المساهمة الأصلية للبحث أيضًا إلى تناول التباينات في الفقه القضائي المقارن بشأن مدى انطباق استثناء الحرب على الهجمات السيبرانية، ويناقش بإمعان حدود التأويل ومبادئ الإثبات القانوني في هذه السياقات. بذلك، يضيف البحث الحالي لبنة جديدة إلى الأدبيات القانونية في موضوع ناشئ وحساس، ويشكّل مرجعًا تأصيليًا وتحليليًا لمن يسعى إلى فهم الإطار العقدي والفقهي لاستثناء الحرب السيبرانية من التغطية التأمينية.

مشكلة البحث وأسئلته

تشهد عقود التأمين السيبراني استبعادًا متكررًا للمخاطر المرتبطة بالحرب السيبرانية من نطاق التغطية، استنادًا إلى بنود تقليدية لا تراعِي الخصوصية التقنية لهذا النوع من المخاطر، ويُثير هذا الاستبعاد إشكالية قانونية تتمثل في مدى مشروعيته التعاقدية في ضوء غموض المفاهيم المستخدمة، وغياب معايير قانونية دقيقة لتكييف هذه الأفعال أو إسنادها، مما يؤدي إلى تضارب في التطبيقات القضائية والتعاقدية، ويهدد مبدأي حسن النية والتوازن العقدي. وتزداد هذه الإشكالية تعقيدًا بالنظر إلى الطبيعة المزدوجة للموضوع، التي تستدعي معالجة قانونية تتكامل فيها الأبعاد التقنية والتأمينية، في ضوء الاجتهادات المقارنة والاتجاهات الحديثة في العقود السيبرانية.

أسئلة البحث

وللوقوف على أبعاد هذه الإشكالية وتحليل جوانبها القانونية والتأمينية المختلفة، يسعى هذا البحث إلى الإجابة عن السؤال التالي:

إلى أي مدى يُعدّ الاستبعاد الاتفاقي للمخاطر السيبرانية ذات الطابع الحربي في عقود التأمين السيبراني مشروعًا من الناحية القانونية، في ضوء الغموض المفاهيمي وتباين الاجتهادات القضائية والتطبيقات التعاقدية؟ ومن هذا السؤال الرئيس، تنبثق الأسئلة الفرعية التالية:

١. ما الأساس القانوني الذي تستند إليه شركات التأمين في استبعاد المخاطر الإلكترونية المرتبطة بالحروب من نطاق التغطية التأمينية؟
٢. ما الإشكالات المفاهيمية والقانونية المرتبطة بتعريف "الحرب السيبرانية" و"الأعمال العدائية الإلكترونية" في سياق عقود التأمين؟
٣. كيف تعاملت السوابق القضائية مثل قضية Mondelez ضد Zurich مع تفسير هذه البنود في حالات النزاع المتعلق بهجمات إلكترونية منسوبة لدول؟
٤. ما السُبل الممكنة لتحقيق توازن بين مصالح شركات التأمين وحماية حقوق المؤمن لهم في ظل الطبيعة المتطورة والمعقّدة للمخاطر السيبرانية؟

أهداف وأهمية البحث

أهداف البحث

يهدف هذا البحث إلى تحقيق الأهداف التالية:

١. تحديد الأساس القانوني الذي تستند إليه شركات التأمين في تضمين بنود استبعاد تغطية المخاطر الإلكترونية ذات الطابع الحربي ضمن عقود التأمين السيبراني.
٢. بيان الإشكالات المفاهيمية والقانونية المرتبطة بتعريف مصطلحات مثل "الحرب السيبرانية" و"الأعمال العدائية الإلكترونية"، واستكشاف أثر غياب التعريفات الدقيقة على الممارسات التأمينية.

Articles in Press

٣. دراسة التوجهات القضائية المقارنة في تفسير بنود الاستبعاد، من خلال تحليل نماذج قضائية بارزة، وعلى رأسها قضية Mondelez International v. Zurich Insurance، لفهم كيفية تعاطي القضاء مع حالات النزاع ذات الصلة.

٤. ٤.اقتراح سبل عملية وقانونية لتحقيق التوازن بين مصالح شركات التأمين وحقوق المؤمن لهم، بما يعزز من فعالية التأمين السيبراني في مواجهة المخاطر الإلكترونية المعقدة.

أهمية البحث

١. **الأهمية النظرية:** تنبع الأهمية النظرية لهذا البحث من تركيزه على أحد الموضوعات القانونية المستحدثة والمعقّدة، وهو الاستبعاد الاتفاقي للمخاطر السيبرانية الناشئة عن الحروب ضمن عقود التأمين السيبراني، وهو شرط يُدرج ضمن عقد التأمين بالاتفاق بين المؤمن والمؤمَّن له، ينص على عدم شمول تغطية بعض الأخطار، مثل الهجمات السيبرانية الناشئة عن الحروب أو النزاعات المسلحة أو الأعمال العدائية بين الدول. حيث يسعى البحث الحالي إلى الإسهام في تطوير البناء النظري للنصوص التأمينية وتحليلها في ضوء مبادئ القانون المدني والتجاري، ولا سيّما مبادئ حسن النية، وتوازن الالتزامات، وحماية الطرف الأضعف في العلاقة التعاقدية، كما تكتسب أهميتها من معالجتها المفاهيم القانونية غير المستقرة مثل "الحرب السيبرانية" و"الأعمال العدائية الإلكترونية"، ومحاولة تفكيك هذه المفاهيم وفق رؤية قانونية منهجية تسهم في إثراء الأدبيات الفقهية العربية في مجال التأمين السيبراني، الذي ما زال محدود التناول في الإنتاج الأكاديمي القانوني.

٢. **الأهمية العملية:** أما من الناحية العملية، فتكمن أهمية البحث الحالي في سعيه إلى تقديم قراءة تحليلية لأثر بنود الاستبعاد الاتفاقي في عقود التأمين السيبراني، وتبيان انعكاساتها الواقعية على حقوق المؤمن لهم في ظل التهديدات الإلكترونية المتزايدة، وتبرز أهمية ذلك في ضوء الحاجة الملحّة لدى شركات التأمين، والمشرّعين، والجهات الرقابية، إلى أدوات قانونية أكثر تماسكًا ووضوحًا في التعامل مع النزاعات المتعلقة بتغطية الهجمات السيبرانية ذات الطابع الحربي، كما يمكن أن تسهم نتائج البحث في توجيه السياسات التعاقدية المستقبلية، وتعزيز الوعي القانوني لدى المستفيدين من التأمين السيبراني، بما يحدّ من حالات الغموض أو النزاع عند وقوع المخاطر.

حدود ومحددات البحث

- **الحدود الموضوعية والزمنية**: يتناول هذا البحث موضوع الاستبعاد الاتفاقي للمخاطر الإلكترونية الناشئة عن الحروب من تغطية عقد التأمين السيبراني، من منظور قانوني تأميني، وتركّز على تحليل مدى مشروعية هذه البنود، وتفسيرها في ضوء المبادئ العامة للعقود. مع الإشارة إلى أبرز السوابق القضائية أو الوثائق التي ظهرت خلال العقدين الأخيرين، لا سيما بعد عام ٢٠١٠، وهو تاريخ تصاعد التهديدات السيبرانية المعقدة على مستوى دولي.
- **محددات البحث:** يعتمد البحث الحالي مجموعة من المحددات التي تم إقرارها بقصد تركيز الجهد البحثي ضمن نطاق منضبط يخدم أهدافها بشكل منهجي، ومن أبرزها:

٣. اقتصار البحث على الجانب القانوني للعقود التأمينية السيبرانية، دون التطرق المفصّل للجوانب التقنية البحتة المرتبطة بآليات الاختراق الإلكتروني، أو أنظمة الأمن السيبراني ذات الطبيعة الهندسية أو المعلوماتية.

٤. تركيز التحليل على العقود التأمينية التي تتضمن بنود استبعاد للمخاطر ذات الطابع الحربي أو العدائي، واستبعاد أنواع التأمين الأخرى التي لا تشمل هذا النوع من البنود (مثل التأمين الصحي، أو تأمين المركبات...).

٥. الاعتماد على السوابق القضائية والنماذج التعاقدية المنشورة أو المتاحة للاطّلاع القانوني، دون التوسع في عقود غير منشورة أو اتفاقات خاصة يصعب الوصول إلى مضامينها التفصيلية.

المنهجية

يعتمد هذا البحث على المنهج التحليلي التطبيقي المقارن، من خلال تحليل النصوص القانونية المنظمة لعقود التأمين، لا سيما تلك المتعلقة بأحكام الاستبعاد الاتفاقي للمخاطر، مع الاستناد إلى العقود النموذجية

Articles in Press

والأحكام القضائية ذات الصلة، وذلك بغرض الوقوف على الإطار القانوني الناظم لتغطية المخاطر السيبرانية ذات الطابع الحربي. كما تم توظيف المنهج المقارن عبر مضاهاة النظم القانونية العربية والأجنبية، بما يُتيح الكشف عن أوجه القصور والاختلاف في تنظيم استثناء الحرب السيبرانية. وقد جرى كذلك الرجوع إلى المصادر الفقهية والأدبيات القانونية المتخصصة في مجال التأمين السيبراني، دعمًا للتحليل النظري. ويعزز البحث جانبه التطبيقي من خلال دراسة حالة واقعية تمثّلت في هجوم NotPetya السيبراني عام ٢٠١٧، لما أثاره من جدل قانوني بشأن تكييف الهجمات الإلكترونية بوصفها أعمالًا حربية، وانعكاس ذلك على مدى التزام شركات التأمين بالتغطية.

خطة الدراسة

للإجابة على أسئلة الدراسة تم تقسيم هذا البحث الى ثلاث مباحث، خصص الأول لماهية التأمين السيبراني والثاني للتحليل القانوني لقضية Mondelez v. Zurich، والثالث للتوجهات الحديثة لاستبعاد أخطار الحرب

- المبحث الأول: ماهية التأمين السيبراني
- المبحث الثاني: تحليل قانوني لقضية *Mondelez v. Zurich*
- المطلب الثاني: استثناء الحرب في عقود التأمين السيبراني: بين الحرب التقليدية والحرب السيبرانية
- المبحث الثاني: تحليل قانوني لقضية *Mondelez v. Zurich*
- المطلب الأول: مبدأ حسن النية والتوازن العقدي في تفسير بنود الاستبعاد
- المطلب الثاني: قضية (Mondelez v. Zurich) الوقائع، الإشكاليات القانونية، وآثارها على عقود التأمين السيبراني.
- المبحث الثالث: التوجهات الحديثة لاستبعاد أخطار الحرب السيبرانية
- المطلب الأول: متطلبات لويدز لاستبعاد الحرب السيبرانية
- المطلب الثاني: بدائل لاستثناء الكوارث السيبرانية

المبحث الأول: ماهية التأمين السيبراني

أدى التطور التكنولوجي السريع إلى ظهور أخطار جديدة لم تغطّها العقود التأمينية التقليدية، فبرز التأمين السيبراني لحماية الأفراد والكيانات من الهجمات الإلكترونية. وتُعرّف هذه المخاطر بأنها تهديدات قد تؤدي إلى خرق البيانات أو تعطيل العمليات، في حين تُعد الهجمات السيبرانية اعتداءات رقمية خبيثة غالبًا ما تكون من مصدر مجهول. ولتحديد الإطار المفاهيمي والتنظيمي لهذا التأمين، يُقسم هذا المبحث إلى مطلبين.

المطلب الأول: التأمين السيبراني: بين المفهوم والتطورات والتحديات التي يثيرها

يُعد التأمين السيبراني من أكثر أشكال التأمين حداثة وتطورًا، وقد نشأ استجابة لحاجة الأسواق إلى تغطية الأخطار غير المسبوقة المرتبطة بالأنظمة الرقمية، غير أن تحديد ماهية هذا النوع من التأمين وتمييزه عن التأمين التقليدي يتطلب الوقوف على تعريفه، وأشكاله، ونطاق تغطيته، بالإضافة إلى تتبّع مسار تطوره في السوق العالمي، ومدى تنامي الحاجة إليه. وعليه، يتناول هذا المطلب الجوانب التالية:

ويُعرَّف التأمين السيبراني بأنه نوع من التأمين يهدف إلى حماية الأفراد والمؤسسات من الأضرار الناتجة عن الهجمات الإلكترونية والمخاطر التقنية، مثل اختراق البيانات، والقرصنة، وهجمات الفدية، والأعطال التقنية. ويُعدّ أداة أساسية في إدارة المخاطر الحديثة، خاصة مع تصاعد وتنوع الهجمات السيبرانية في بيئات العمل الرقمية (شامبي، ٢٠٢٣).

وتتخذ وثائق التأمين السيبراني عدة أشكال، من أبرزها (Romanosky et al., 2019):

- تأمين الطرف الأول: يغطي الخسائر المباشرة التي تتعرض لها الشركة نتيجة حادث سيبراني (مثل تعطل الأنظمة، فقدان البيانات، التوقف عن العمل).
- تأمين الطرف الثالث: يتعلّق بالمسؤوليات القانونية تجاه أطراف خارجية متضررة بفعل خرق معلومات أو تسرب بيانات.

Articles in Press

- التأمين الصامت أو الضمني: هو إدراج التغطية ضد الهجمات السيبرانية ضمن وثائق التأمين التقليدي دون نص صريح، مما يثير غموضًا قد يُفسر لصالح المؤمن له. وقد دفع هذا الغموض "رابطة سوق لويدز" إلى إلزام أعضائها باستبعاد هذه التغطية، في حين ظهر التأمين السيبراني الإيجابي الذي يحدد بوضوح حدود التغطية والاستثناءات.

وقد شهد سوق التأمين السيبراني تطورًا منذ أواخر التسعينيات، إذ أطلقت AIG أول بوليصة متخصصة عام ١٩٩٧، ثم توسعت التغطيات مع مطلع الألفية لتشمل مختلف القطاعات، فغدت تغطي خسائر الطرف الأول ومسؤوليات الأطراف الثالثة (Herr, 2021).

وأسهمت حوادث مثل اختراق بيانات وهجمات الفدية العالمية في دفع شركات التأمين إلى إعادة تقييم نماذجها ورفع الأقساط (Smith& Mulrain, 2017). وتشير التقديرات إلى أن حجم السوق قد يبلغ ٣٠ مليار دولار بحلول ٢٠٣٠ (Jones, 2022)، وتُعد أمريكا الشمالية السوق الأضخم، إذ تستحوذ على ما بين ٦٠٪ إلى ٧٠٪ من إجمالي الأقساط، وقد شهدت أقساط التأمين الأمريكية ارتفاعًا من ٦,٥ مليار دولار عام ٢٠٢١ إلى ٩,٧ مليار دولار عام ٢٠٢٢، رغم تباطؤ النمو النسبي خلال ٢٠٢٣ بسبب تراجع الأسعار واشتداد المنافسة (NAIC Staff, 2024).

على الصعيد التشريعي، ساهمت قوانين حماية البيانات مثل اللائحة الأوروبية العامة والتشريعات الأمريكية في تعزيز هذا النوع من التأمين، كما بدأت بعض الدول العربية (مثل الإمارات والسعودية) بسن قوانين لحماية البيانات والمعاملات الإلكترونية. ففي الإمارات نص القانون الاتحادي رقم (٥) لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات على إلزامية حماية البنية الرقمية، وهو ما دفع شركات التأمين إلى إدخال منتجات متخصصة. وفي الأردن، تناول القانون المدني الأردني (المواد ٩٢٠ وما بعدها) الأحكام العامة لعقد التأمين، مؤكدًا على بطلان الشروط التعسفية المخالفة للنظام العام. وفي مصر، نصت المادة (٧٤٧) من القانون المدني المصري على أن شرط الإعفاء أو التقييد الباطل إذا أخل بجوهر التزام المؤمن (السنهوري، ١٩٦٤). هذه النصوص تبرز أن الأساس التشريعي العربي مهيأ لتطبيق مبادئ العدالة في عقود التأمين السيبراني.

وبالرغم من النمو المتسارع الذي يشهده سوق التأمين السيبراني، إلا أن هذا القطاع لا يزال يواجه عدة تحديات تعيق من استقراره وانتشاره بالشكل المأمول، ومن أبرز هذه التحديات (Markopoulou, 2021):

- صعوبة تقدير حجم الخطر بدقة: نظرًا لتطور طبيعة التهديدات السيبرانية واتساع نطاقها، تصبح النماذج التقليدية لقياس المخاطر غير كافية لتقييم التعرض الفعلي.
- غموض خطوط التغطية: إذ لا تزال الكثير من الوثائق التأمينية تعاني من غموض في صياغة الاستثناءات أو حدود التغطية، خصوصًا فيما يتعلق بالأعمال الرقمية المعقدة.
- غياب المعايير الموحدة: تختلف الوثائق من شركة لأخرى من حيث تعريف المصطلحات وتحديد طبيعة الأخطار المغطاة أو المستبعدة.
- إشكالية الهجمات المدعومة من دول: تثير الهجمات ذات الطابع السيادي تساؤلات حول اعتبارها "أعمالًا حربية" مستثناة من التغطية، مما يستلزم أطرًا تنظيمية أوضح لمعالجتها.

المطلب الثاني: استثناء الحرب في عقود التأمين السيبراني: بين الحرب التقليدية والحرب السيبرانية

شكّل استثناء الحرب بندًا ثابتًا في وثائق التأمين التقليدية لعدة عقود، استنادًا إلى نماذج موحدة، أبرزها نموذج NMA 464 المستخدم على نطاق واسع في سوق "لويدز"، والذي يستبعد الأضرار الناجمة عن الحرب، سواء كانت معلنة أو غير معلنة، أو عن أعمال عدائية ذات طابع سيادي (Nagurney et al.,2025).

غير أنّ انتقال النزاعات إلى الفضاء الرقمي أثار جدلًا حول مدى انطباق استثناء الحرب على الهجمات السيبرانية، إذ إن الفضاء الإلكتروني بيئة غير مادية بلا حدود جغرافية أو سيادة تقليدية، مما يثير التساؤل: هل يعد الهجوم السيبراني "حربًا" بالمعنى التأميني أو الدولي؟ وقد انقسم الفقه في تفسير المادة (٤/٢) من ميثاق الأمم المتحدة بين اتجاه يقصر القوة على الأضرار المادية الجسيمة (United Nations, 1945)، وآخر يوسّعها لتشمل الأضرار الاقتصادية وتعطيل البنى التحتية الحيوية (Alhamdan, 2023). وحاول Michael Schmittالتوفيق بين الاتجاهين عبر "دليل تالين"، فاعتبر أن بعض الهجمات الإلكترونية ترقى إلى "هجوم مسلح" حتى وإن لم تكن عسكرية تقليدية(Schmitt, 2017).

ويُستدل على الإشكالية العملية لتطبيق هذا الاستثناء من قضية شركة Merck[٢] ضد ACE، حيث رفضت شركة التأمين تغطية أضرار هجوم (NotPetya) استنادًا إلى استثناء الحرب، إلا أن محكمة نيوجيرسي العليا رأت أن الهجوم لا يدخل ضمن "الحرب التقليدية"، مؤكدة أن الاستثناءات تُفسَّر وفق صياغتها الدقيقة وسياقها، لاسيما مع غياب نص صريح يستبعد الهجمات السيبرانية، وقد انتهت القضية عام ٢٠٢٤ بتسوية سرية(Chopra, 2021).

أما في الفقه العربي، فقد استقر الرأي على ضرورة أن يكون الاستبعاد محددًا بدقة، وإلا وقع باطلًا لكونه شرطًا تعسفيًا يفرغ التأمين من مضمونه (الجابر والرشيد، ٢٠٢٥؛ الزعبي، ٢٠٢١). وقد أكدت محكمة التمييز الأردنية في اجتهاداتها أن عقود التأمين تُعدّ من عقود الإذعان، وأن البنود الغامضة تُفسَّر ضد مصلحة المؤمن (Battah, 2020؛ الجابر والرشيد، ٢٠٢٥)، استنادًا إلى حكم المادة (٢/٢٤٠) من القانون المدني الأردني التي تقضي بعدم جواز تفسير الشروط الغامضة بما يضرّ مصلحة الطرف المذعن (القانون المدني الأردني، المادة ٢/٢٤٠). وقد كرّست ذلك أحكامها في عدة قرارات، منها قرار تمييز حقوق رقم (٢٠٠٥/١٨٠٥) تاريخ ٢٠٠٥/١٠/١١ الذي فسّر غموض شرط التغطية في وثيقة التأمين لصالح المؤمن له (قرار تمييز حقوق رقم ٢٠٠٥/١٨٠٥، منشور في قاعدة قسطاس)، وقرار تمييز حقوق رقم (٢٠٠٣/٤٤٩٥) تاريخ ٢٠٠٤/٤/١٢ الذي أكّد التزام شركة التأمين بالتغطية ضمن الحدود الواردة في الوثيقة (قرار تمييز حقوق رقم ٢٠٠٣/٤٤٩٥).

وفي مصر، قضت محكمة النقض في الطعن المدني رقم ١٩٥٢ لسنة ٥٨ ق، بجلسة ١١ ديسمبر ١٩٩٠، ببطلان الشروط التعسفية التي تُخل بالتوازن العقدي، حيث نص مبدأها "إذا ورد في عقد التأمين شرط تعسفي من شأنه أن يُخل بتوازن العقد أو يُعفي شركة التأمين من التزامها الرئيسي، فإن هذا الشرط يقع باطلاً". هذه الأحكام تبرهن أن القضاء العربي متسق مع القاعدة اللاتينية (أبو السعود، ٢٠١١).

ومن الناحية المفاهيمية، يعمّق غياب تعريف موحّد لـ "الحرب السيبرانية" من الأزمة؛ فالحرب السيبرانية تُفهم عادة كهجمات منظمة تشنّها دولة أو جهة تدعمها ضد بنى تحتية حيوية كالكهرباء والمياه والمصارف باستخدام أدوات رقمية متقدمة مثل البرمجيات الخبيثة أو الفيروسات (شويرب ومراد، ٢٠٢٣؛ محمود وكيطان، ٢٠٢١؛ عبد العال وآخرون، ٢٠٢٢). وتمثل هذه الهجمات امتدادًا لـ"حرب المعلومات"، حيث تُستخدم البيانات كسلاح استراتيجي لزعزعة الثقة وتحقيق أهداف سياسية، ما يميزها عن الهجمات الجنائية ذات الطابع المالي أو التخريبي (الرعاش، ٢٠٢٤؛ شنوف، ٢٠٢٠).

يشير عبد الرضا (٢٠٢٣) إلى أن بعض الدول تعتمد استراتيجيات هجومية في الفضاء السيبراني تُوازي العمليات العسكرية في خطورتها، مما دفعها إلى توسيع مفهوم "الدفاع الوطني" ليشمل الحرب السيبرانية. ومع ذلك، يثير إسقاط مفاهيم الحرب السيبرانية على عقود التأمين إشكاليات تفسيرية؛ إذ غالبًا ما تكون طبيعة الهجوم والجهة المنفذة غير واضحة، وقد تُنسب بعض الهجمات إلى دول من دون أدلة قاطعة، مما يضعف كفاية هذا الإسناد لتفعيل استثناء الحرب (Cremer et al., 2024).

كما أن بعض الأفعال، كالتجسس الرقمي أو الاختراقات ذات الطابع الاستخباراتي أو التنافسي، قد تُلحق أضرارًا اقتصادية جسيمة دون أن تُصنّف أعمالًا حربية، مما يخلق تداخلًا مفاهيميًا وتباينًا في التأويل القانوني، ويجعل إدراجها ضمن الاستثناء الاتفاقي محل جدل بين شركات التأمين والمؤمَّن لهم والهيئات القضائية (Rovetto, 2022).

يشير (Woods & Weinkle, 2019) إلى أن استخدام مفاهيم مثل "الحرب السيبرانية" و"الإرهاب الإلكتروني" يزداد تعقيدًا حين تُحمّل أبعادًا سياسية أو إعلامية، مما يصعّب توحيد المعايير ويجعل تحديد النية والسياق وطبيعة الهدف عوامل حاسمة في تفسير شروط الاستبعاد.

وعليه، تكشف هذه التطورات عن مأزق قانوني مزدوج؛ فمن ناحية، يفتقر النظام القانوني الدولي والتشريعات الوطنية إلى تعريفات ومعايير دقيقة تضبط نطاق الحرب السيبرانية. ومن ناحية أخرى، فإن الإبقاء على صياغات عامة في عقود التأمين يُخلّ بمبدأ اليقين والتوازن العقدي، ويجعل المؤمن له عرضة لفراغ حمائي يناقض الغاية الجوهرية من التأمين.

المبحث الثاني: تحليل قانوني لقضية *Mondelez v. Zurich*

تُعد قضية Mondelez v. Zurich من أبرز السوابق القضائية التي أثارت جدلًا واسعًا في الأوساط القانونية والتأمينية بشأن تفسير بنود الاستبعاد المرتبطة بالحرب في سياق التأمين السيبراني؛ فقد مثلت هذه القضية نموذجًا واقعيًا لتقاطع المخاطر السيبرانية مع المفاهيم التقليدية في وثائق التأمين، لا سيما في ظل الغموض

المفاهيمي المتعلق بالحرب السيبرانية، والإسناد القانوني للهجمات الإلكترونية المدعومة من دول. وتبرز أهمية هذه القضية فيما أثارته من تساؤلات قانونية حول كيفية التكييف القانوني للهجمات الإلكترونية، ومدى مشروعية لجوء شركات التأمين إلى تفعيل بنود الاستثناء في مثل هذه الحالات، فضلاً عن أثر ذلك على مراكز المؤمن لهم وحقوقهم التعاقدية. وعليه، يتناول هذا المبحث الموضوع من خلال مطلبين رئيسين، على النحو الآتي:

المطلب الأول: مبدأ حسن النية والتوازن العقدي في تفسير بنود الاستبعاد

يُعد مبدأ حسن النية أحد الركائز الأساسية في تفسير العقود. وقد نصت المادة (١/٢٠٢) من القانون المدني الأردني على أن: "يجب تنفيذ العقد طبقًا لما اشتمل عليه وبطريقة تتفق مع ما يوجبه حسن النية"، وهو ما ينطبق على عقود التأمين (الذيابات، ٢٠٠٥). ويُلزم هذا المبدأ الطرف الأقوى . شركة التأمين . بعدم استغلال صياغة الشروط بما يضر تعسفًا بالمؤمن له، خاصة وأن هذا الأخير غالبًا ما يكون الطرف الأضعف. وقد أكدت محكمة التمييز الأردنية في قرارها رقم ٢٠١٦/٢٥٣٩ أن شروط عقود الإذعان إذا اتسمت بالغموض تُفسَّر لمصلحة الطرف المذعن، ويملك القاضي تعديل أو إلغاء البنود التعسفية حمايةً للعدالة (شويات، ٢٠١٩).

وفي السياق ذاته، شددت محكمة التمييز الأردنية في قرارها رقم ٢٠١٦/٢٣٠٧ على أن الشروط التي تؤدي إلى اختلال واضح في مراكز الأطراف يمكن أن تُعد باطلة أو تفسر تفسيرًا ضيقًا (الصمادي، ٢٠١٠). يجد هذا المبدأ سندًا إضافيًا في الفقه العربي، الذي أجمع على أن شرط الاستبعاد إذا صيغ بعبارات عامة وفضفاضة فإنه يعد شرطًا تعسفيًا يؤدي إلى بطلانه (التميمي، ٢٠١٠؛ الزعبي، ٢٠٢١؛ أبو الهيجاء، ٢٠١٨)، لكونه يفرغ التأمين من مضمونه ويخل بمبدأ المشروعية التعاقدية (الجابر والرشيد،٢٠٢٥).

وفي التشريع المصري، نصت المادة (٧٤٧) من القانون المدني على أن التزام المؤمن يظل قائمًا ما لم يثبت أن المؤمن له تعمد إخفاء بيانات جوهرية أو ارتكب غشًا، بما يعني أن أي شرط إعفاء واسع النطاق يُعد مخالفًا للنظام العام، وقد أكدت محكمة النقض المصرية (الطعن المدني رقم ٢٥٩٢ لسنة ٦٨ ق) أن الشروط التي تنال من جوهر التزام المؤمن تُعتبر باطلة لتعارضها مع العدالة العقدية. وهو ما يتسق مع الفقه اللاتيني الذي يرفض الشروط التعسفية في عقود الاستهلاك والإذعان (Gordley, 2006).

وفي القانون العام، يُكرَّس هذا الاتجاه من خلال قاعدة تفسير العقود ضد الجهة الصاغة – قاعدة contra proferentem– والتي تقضي بأن أي شرط غامض يُفسَّر ضد الطرف الذي صاغه (Unegenova et al., 2024)، وقد طبّقت هذه القاعدة في قضية Canada Steamship Lines Ltd v. The King [1952] AC 192، حيث اشترطت المحكمة أن تكون شروط الإعفاء أو الاستثناء واضحة وصريحة وغير قابلة للتأويل، وأن يُفترض رفضها إن كانت تحتمل أكثر من معنى (Gordon, 2023). ويُضاف إلى ذلك ما قررته محكمة ولاية إلينوي في قضية Mondelez v. Zurich، التي ناقشت مدى قانونية تطبيق استثناء الحرب على هجوم سيبراني، وأكّدت أن عدم وضوح بند الاستثناء، وعدم ذكره صراحة للمخاطر السيبرانية، يجعل تفسيره موضع شك، ويحول دون تحميل المؤمن له تبعات غير متوقعة (Chopra, 2021).

وبالتالي، فإن الاستبعاد الاتفاقي للمخاطر السيبرانية ذات الطابع الحربي، إذا لم يُصَغ بلغة دقيقة ومباشرة، يكون مخالفًا لهذين المبدأين، إذ يُخِلّ بالتوازن بين مصلحة شركة التأمين وحقوق المؤمن له، ويُعرّض الأخير لحرمان غير مبرر من التغطية، مما يهدد عدالة العلاقة التعاقدية ويُضعف الثقة بالنظام التأميني ككل.

المطلب الثاني: قضية Mondelez v. Zurich – الوقائع، الإشكاليات القانونية، وآثارها على عقود التأمين السيبراني.

تُعدّ قضية *Mondelez International v. Zurich Insurance* من أبرز القضايا المعاصرة التي أثارت نقاشًا واسعًا حول مدى إمكانية تطبيق بنود استثناء الحرب التقليدية على الأضرار الناجمة عن الهجمات السيبرانية، وتعود القضية إلى عام ٢٠١٨، حين رفعت شركة Mondelez الأمريكية، وهي إحدى كبرى شركات الصناعات الغذائية في العالم، دعوى قضائية ضد شركة Zurich السويسرية للتأمين، مطالبة بتعويضات تتجاوز ١٠٠ مليون دولار، نتيجة الأضرار التي لحقت بها إثر هجوم إلكتروني من نوع NotPetya، الذي وقع في يونيو ٢٠١٧ وتسبب في تعطيل واسع للبنية التحتية الرقمية للشركة على مستوى عالمي (Ferland, 2019).

وقد رفضت Zurich المطالبة، مستندة إلى بند استثناء ضمن وثيقة التأمين ينص على استبعاد التغطية عن "الخسائر المباشرة أو غير المباشرة الناجمة عن أي فعل عدائي أو حربي، سواء في وقت السلم أو الحرب، صادر عن أي حكومة أو سلطة عسكرية أو جهة ذات طابع سيادي"، واعتبرت Zurich أن الهجوم منسوب إلى جهات

حكومية روسية في سياق حملة سيبرانية ضد أوكرانيا، ما يندرج -برأيها- ضمن مفهوم "العمل الحربي" وفقًا للبند المذكور (Chopra, 2021).

في المقابل، رفضت Mondelez هذا التوصيف، مؤكدة أن الهجوم لا يرقى إلى مستوى "عمل حربي" بالمعنى القانوني أو التقليدي، وأن الوثيقة التأمينية التي تملكها هي من نوع "تأمين شامل ضد جميع الأخطار" (All-risk property insurance)، وتغطي صراحة الأضرار الناتجة عن فشل مفاجئ في الأنظمة الإلكترونية، وأشارت الشركة إلى أن بند استثناء الحرب لم يشر صراحة إلى الهجمات السيبرانية أو الأعمال العدائية الرقمية، ما يجعل تطبيقه على هذه الحادثة غير مبرر تفسيرًا وقانونًا (Rovetto, 2022).

وقد أثارت هذه القضية جملة من الإشكاليات القانونية، لعل أبرزها يتمثل في تفسير بنود الاستثناء، ومدى وجوب وضوحها ودقتها عند الصياغة؛ فقد أكدت Mondelez أن صياغة البند كانت غامضة وعامة، ولم تتضمن إشارات صريحة إلى الأخطار السيبرانية، مما يفتح الباب لتفسيرات متعددة. وأشارت إلى أن عبء الدقة في الصياغة يقع على عاتق شركة التأمين، لا سيما فيما يخص البنود الاستثنائية، التي قد تُفسّر عند الغموض لصالح المؤمن له (Brunner, 2022).

ومن بين الجوانب القانونية المعقدة التي ناقشتها القضية مسألة نسبة الهجوم إلى جهة سيادية؛ فبينما اعتمدت Zurich على تقارير حكومية تفيد بتورط روسيا، جادلت Mondelez بأن NotPetya لم يكن موجّهًا ضدها مباشرة، بل تضررت منه كأثر جانبي، وهو ما لا ينطبق على شرط "الاستهداف العدائي المباشر" الذي تستند إليه استثناءات الحرب في وثائق التأمين الكلاسيكية (Wolff, 2021).

ورغم استمرار النزاع لعدة سنوات، فإن القضية انتهت بتسوية خارج المحكمة في نوفمبر ٢٠٢٢، دون صدور حكم قضائي حاسم، ما أبقى الإشكالات القانونية التي طرحتها مفتوحة أمام الاجتهاد المستقبلي، إلا أن القضية كان لها تأثير عملي وتنظيمي واسع؛ إذ دفعت العديد من شركات التأمين، ولا سيما في أسواق كبرى مثل "لويدز" في لندن، إلى مراجعة وإعادة صياغة بنود الاستثناء في وثائق التأمين السيبراني، مع إدراج تعريفات أدق لمفاهيم مثل "الهجمات السيبرانية ذات الطابع الحربي" و"العمليات العدائية الرقمية المدعومة من دول" (Wolff, 2021).

وفي الفقه العربي، تمثل هذه القضية مرجعًا مهمًا للتأكيد على أن عقود التأمين السيبراني يجب أن تُعامل كعقود إذعان أو استهلاك، وبالتالي فإن الشروط الغامضة تُفسَّر ضد مصلحة شركة التأمين (أبو الهيجاء، ٢٠١٨؛ الزعبي، ٢٠٢١؛ الجابروالرشيد، ٢٠٢٥). وقد كرّست محكمة التمييز الأردنية هذا الاتجاه مرارًا (قرار تمييز حقوق رقم ٢٠٠٥/١٨٠٥؛ ٢٠١٦/٢٣٠٧)، وأكدت محكمة النقض المصرية في أحكامها على بطلان أي شرط يُخلّ بالتوازن العقدي. وبهذا يتضح أن النظام القانوني العربي يتفق في جوهره مع المبادئ المقارنة وإن اختلفت أدوات التعبير عنها (Battah, 2020).

وقد أبرزت القضية الحاجة الملحّة إلى وجود أطر معيارية دولية تنظم توصيف الهجمات السيبرانية، وتحدد متى يُمكن اعتبارها "أعمالًا حربية"، خاصة في ظل اعتماد التوصيف على تقارير حكومية أو استخباراتية قد تكون منحازة، وأعرب عدد من الخبراء عن تخوفهم من أن التوسع في استخدام توصيف "الحرب" قد يضر بمنظومة التأمين، ويمنح الشركات ذريعة واسعة لرفض التعويضات، حتى دون وجود دليل قانوني قاطع (Chopra, 2021).

كما بيّنت القضية أيضًا قصور النظام القانوني التقليدي في التعامل مع النزاعات الناشئة عن "الحروب الرمادية" أو "التهديدات المركبة"، وهي ظواهر تقع في منطقة وسطى بين الحرب والجريمة (Rovetto, 2022). ومن هنا، يمكن القول إن قضية Mondelez تمثل نقطة تحوّل مركزية في فهم وتطبيق بنود الاستبعاد الاتفاقي، في ظل التحولات المتسارعة في البيئة التقنية والأمنية العالمية.

المبحث الثالث: التوجهات الحديثة لاستبعاد أخطار الحرب السيبرانية

أعاد الواقع السيبراني تشكيل مفهوم المخاطر التقليدي، بحيث باتت الفضاءات الرقمية تمثل مناطق غير منظمة ذات طبيعة جيوسياسية معقدة، تستدعي أنماطاً جديدة من إدارة المخاطر. وعلى غرار نشوء شركة "لويدز أوف لندن" في إطار مواجهة أخطار بحرية جديدة، برزت الحاجة إلى مقاربات تأمينية متقدمة تتعامل مع تعقيدات الحرب السيبرانية.

ورغم مركزية التأمين كوسيلة لإدارة المخاطر ذات الطابع الجغرافي السياسي، إلا أن الحرب السيبرانية كشفت عن قصور في تغطيات السوق التأميني، لا سيما في ظل صعوبة تحديد الفاعل، وتعقيد الإسناد، وتداخل

الأضرار بين الجسيم والعرضي. ولهذا، تم تطوير أدوات جديدة في سوق التأمين، وفي مقدمتها ما أصدرته "رابطة سوق لويدز" من متطلبات لاستبعاد أخطار الحرب السيبرانية، إلى جانب مقترحات بديلة للتعامل مع الكوارث الإلكترونية.

المطلب الأول: متطلبات لويدز لاستبعاد الحرب السيبرانية

أصدرت لويدز نشرة رقم٧٥٣٨١ بخصوص إلزام الشركات الأعضاء بصياغة وثائق التأمين السيبراني بحيث تستثني صراحة الهجمات السيبرانية المدعومة من دول، وأكدت على ضرورة وجود تعريفات واضحة وشروط إسناد دقيقة، مع منع تغطية المخاطر السيبرانية التي تشكل تهديداً لأمن الدولة أو بنيتها التحتية الأساسية، ما لم يتم الاتفاق المسبق، وقد تضمنت البنود النموذجية الأربعة التي اقترحتها لويدز تعريفات محددة للحرب (كصراع مسلح بين دول أو عمليات إلكترونية تشكل جزءاً من الحرب)، والعملية السيبرانية (كممارسات إلكترونية تؤثر بشكل كبير على قدرة الدولة على العمل)، وأسس الإسناد للدول وليس للأفراد، كما وضعت حداً معيناً لتفعيل الاستثناء، كحدوث "ضرر كبير" على المستوى الوطني (Lloyd's, 2022). ويهدف هذا التنظيم إلى تقليص الغموض في التغطية، وتعزيز القدرة على التنبؤ القانوني عند التعامل مع المطالبات الناشئة عن حوادث سيبرانية ذات طابع سيادي (Brunner, 2022).

وفي الفقه العربي، يُنتقد هذا الاتجاه لكونه يعيد إنتاج الاستبعاد الفضفاض بعبارات تقنية جديدة (الزعبي، ٢٠٢١). فقد أكّد الفقهاء على أن أي شرط استبعاد لا يُصاغ بدقة ووضوح يعد شرطًا تعسفيًا باطلًا، استنادًا إلى أن عقود التأمين عقود إذعان بطبيعتها (الجابر والرشيد، ٢٠٢٥)، وهو ما أقرته محكمة التمييز الأردنية في قراراتها (٢٠١٦/٢٥٣٩ و٢٠١٦/٢٣٠٧ - قواعد بيانات قسطاس والقضاء الأردني الرسمي)، وكذلك محكمة النقض المصرية التي قضت ببطلان أي شرط يخل بالتوازن العقدي (طعن مدني ٢٥٩٢ لسنة ٦٨ ق - هيئة قضايا الدولة المصرية، ٢٠٠٠).

وبذلك، فإن إلزام شركات التأمين بصياغة استثناءات دقيقة خطوة إيجابية من زاوية التوقع القانوني، لكنها لا تعفي من الخطر إذا لم تُراعَ معايير العدالة العقدية التي تحمي المؤمن لهم من التعسف.

المطلب الثاني: بدائل لاستثناء الكوارث السيبرانية

سواء تعلّق الأمر بهجمات سيبرانية ترعاها الدول أو بتهديدات أخرى، ينبغي على شركات التأمين والجهات التنظيمية إدراك أن استثناءات الحرب، رغم اتساعها، لا تكفي لحماية السوق من الكوارث السيبرانية واسعة النطاق، خصوصًا تلك التي قد تنجم عن جهات غير حكومية أو أخطاء عرضية أو كوارث طبيعية؛ فهذه الاستثناءات لا تغطي سوى الهجمات المدعومة من دول، ولا تصلح لمعالجة كافة محفزات الخطر. ومن ثمّ، يتعين تطوير أدوات تأمينية مخصصة لإدارة هذا النوع من الكوارث بفعالية (حميد، ٢٠١٨).

أولاً: استثناء مصمم خصيصاً للكوارث السيبرانية

يسهم الاستثناء المصمم خصيصًا للكوارث السيبرانية في تمكين شركات التأمين من إدارة هذه المخاطر بفعالية أكبر من استثناءات الحرب التقليدية، خاصة في حال كانت ناتجة عن محفزات غير تقليدية أو مادية، ويتمثل التحدي في صعوبة التنبؤ بأنواع المحفزات الإلكترونية المستقبلية، نظرًا لتغير مشهد المخاطر باستمرار وتطور استخدام التكنولوجيا، كما أظهرت جائحة كوفيد-١٩. وعليه، يصعب وضع صياغة دقيقة تستوعب جميع السيناريوهات المحتملة، مما يجعل هذا التحدي أكثر تعقيدًا في البيئة الرقمية المتسارعة (Lahmann, 2023).

ثانياً: دعم حكومي مباشر

يثار في الفقه التأميني تساؤل حول جدوى استحداث برامج حكومية متخصصة للتأمين ضد الكوارث السيبرانية، على غرار النموذج الأمريكي المتمثل في قانون TRIA، وهو تشريع اتحادي يهدف إلى توفير شبكة أمان لشركات التأمين في مواجهة الخسائر الناجمة عن الهجمات الإرهابية واسعة النطاق، حيث يوفر هذا القانون تعويضاً مالياً لشركات التأمين التي تواجهه خسائر كبيرة بسبب هذه الهجمات ، لما له من فوائد في تحسين تبادل المعلومات، وتوجيه السوق نحو إدارة أفضل للمخاطر غير القابلة للتنبؤ، إلا أن إقرار هذا النوع من البرامج يواجه تحديات تشريعية ولوجستية، في ظل تباين طبيعة الحوادث الإلكترونية الإرهابية (الإرهاب السيبراني) عن الأعمال الإرهابية التقليدية (Herr, 2021). إلا أن تفعيل هذا القانون يتطلب استيفاء شروط صارمة كالعنف والخطر على الأرواح، وهي شروط قد لا تتحقق في كل هجوم سيبراني، مما يقلل من فعاليته في السياق السيبراني (Bace et al., 2024).

في السياق العربي، بدأت المملكة العربية السعودية عبر الهيئة الوطنية للأمن السيبراني (NCA) بوضع إطار تنظيمي يُلزم شركات التأمين بتقييم أخطار الأمن السيبراني، وذلك من خلال إصدار وثيقة بعنوان "إطار الأمن السيبراني لقطاع التأمين" عام ٢٠٢٢، التي تُعد أول محاولة رسمية لربط قطاع التأمين بمخاطر الفضاء الرقمي (الهيئة الوطنية للأمن السيبراني، ٢٠٢٢). أما في الإمارات العربية المتحدة، فقد أطلق مجلس الأمن السيبراني منذ عام ٢٠٢١ عدة مبادرات وطنية لتعزيز الاستجابة للمخاطر الإلكترونية، خصوصًا في القطاعات الحيوية، رغم عدم صدور إعلان رسمي حتى الآن عن شراكات مباشرة مع شركات التأمين (وكالة أنباء الإمارات، ٢٠٢٣). وفي الأردن، ورغم غياب سياسة تشريعية مباشرة، تُطرح بعض التوصيات في تقارير رسمية لوزارة الاقتصاد الرقمي بخصوص أهمية تضمين التأمين السيبراني ضمن استراتيجيات مواجهة الأزمات والكوارث الوطنية (وزارة الاقتصاد الرقمي الأردنية، ٢٠٢٣).

ثالثاً: استثناءات موجهة للبنية التحتية

تعتمد بعض الشركات، مثل Munich Re، على استثناء الأضرار الناتجة عن انهيار بنى تحتية محددة (كشبكات الكهرباء أو أسماء النطاقات)، نظراً لما تحمله من خطر تجميعي يصعب نمذجته. ورغم فعاليتها، تواجه هذه الاستثناءات انتقادات نظرًا لاحتمال تجاهلها لمخاطر تنشأ من عناصر خفية ضمن سلاسل التوريد أو أنظمة الحوسبة المتداخلة .

رابعاً: التعاريف العامة أو الموجهة نحو التأثير

يقترح هذا النهج صياغة استثناءات بلغة مرنة تشمل "الخدمات الأساسية" أو "البنية التحتية الحيوية"، وتفعيل الاستثناء عند تجاوز ضرر معين حدودًا كمية أو جغرافية، وقد استند خبراء "دليل تالين" في هذا إلى معيار "المدى والأثر"، وفقًا لاجتهاد محكمة العدل في قضية نيكاراغوا، لتحديد ما إذا كان الهجوم السيبراني يرتقي إلى استخدام غير مشروع للقوة، حتى إن لم يُحدث أضرارًا مادية (Lubin, 2021).

تكشف هذه البدائل عن اتجاه مزدوج؛ فمن ناحية، هناك رغبة في تعزيز وضوح التغطية وحماية السوق التأميني من المخاطر غير القابلة للتنبؤ. ومن ناحية أخرى، هناك خطر حقيقي من توسع الاستثناءات على نحو يفرغ التأمين من مضمونه، وهو ما يخالف المبادئ التشريعية والقضائية العربية التي تُبطل الشروط التعسفية والفضفاضة.

ويتسق الفقه العربي في موقفه من بطلان الاستبعاد العام، وهو ما ينسجم مع التشريعات العربية كالقانون المدني الأردني (م ٩٢٠ وما بعدها) والمصري (م ٧٤٧)، إضافة إلى قوانين حماية المستهلك في الإمارات والسعودية التي تجرم الشروط التعسفية، كما أن القضاء العربي – سواء محكمة النقض المصرية أو محكمة التمييز الأردنية – رسّخ مبدأ أن عقود التأمين عقود إذعان، وأن البنود الغامضة تُفسر ضد مصلحة من صاغها.

وفي المقارنة الأجنبية، تُظهر تجربة لويدز وTRIA و Munich Reأن الأسواق المتقدمة تتجه نحو صياغات أوضح وأكثر تحديدًا، لكنها لا تزال تعاني من إشكالية التوازن بين استقرار السوق وحماية المؤمن له. ومن هنا، يمكن القول إن التحدي العالمي واحد، لكنه يتخذ في العالم العربي بعدًا مضاعفًا بسبب غياب أطر تنظيمية موحدة.

الخاتمة

يتبيّن من خلال هذا البحث أن الاستبعاد الاتفاقي للمخاطر السيبرانية ذات الطابع الحربي من نطاق التغطية في عقود التأمين السيبراني يمثل إشكالية قانونية مركّبة، تتداخل فيها المفاهيم التقنية مع المبادئ العقدية، ويتعزز هذا التعقيد في ظل غياب تعريفات قانونية واضحة لمفاهيم مثل "الحرب السيبرانية" و"الأعمال العدائية الإلكترونية"، وقد كشف التحليل أن الاستثناءات التقليدية المستمدة من التأمين البحري أو العسكري لا تصلح بذاتها للتطبيق على السياق السيبراني دون إعادة صياغة دقيقة تراعي طبيعة هذه المخاطر المتطورة، كما أن السوابق القضائية المقارنة، وعلى رأسها قضيتي Mondelezو Merck، أظهرت تباينًا في التفسير، وميلًا قضائيًا متزايدًا لرفض الاستثناءات الغامضة التي تضر بمصالح المؤمن لهم.

وعليه، فإن الحاجة باتت ماسة إلى تطوير بنية قانونية متخصصة تراعي خصوصية الفضاء السيبراني، وتحمي التوازن التعاقدي بين شركات التأمين والمستفيدين، وذلك من خلال تبنّي نماذج معيارية واضحة، وتشريعات صريحة تعالج الإسناد السيادي، وتعزّز من شفافية الالتزام التأميني في حالات النزاع.

Articles in Press

النتائج

١. كشفت الدراسة عن غموض واسع في بنود استثناء الحرب ضمن وثائق التأمين السيبراني، خاصة فيما يتعلق بعدم تحديد المقصود بـ"الحرب السيبرانية" أو "العدائية الإلكترونية"، مما يؤدي إلى تفسيرات قضائية متضاربة.

٢. أبرزت السوابق القضائية، مثل قضية Mondelez v. Zurich وMerck v. ACE, أن المحاكم تميل إلى تقييد تطبيق بنود الاستثناء عندما تفتقر إلى صياغة دقيقة أو لا تنص صراحة على المخاطر السيبرانية.

٣. أثبت البحث أن استخدام استثناءات الحرب التقليدية في السياق السيبراني دون تعديل يفتح المجال أمام شركات التأمين للتنصل من التغطية بطريقة تخلّ بالتوازن العقدي ومبدأ حسن النية.

٤. أظهرت التوجهات الحديثة، خاصة مبادرات سوق "لويدز"، محاولة لتقنين استثناء الحرب السيبرانية ضمن بنود أكثر تحديدًا، تتضمن تعريفات للإسناد والضرر الإلكتروني ذي الطابع السيادي.

الشكر والتقدير

نتوجه بخالص الشكر إلى المراجعين ورئيس التحرير على ملاحظاتهم القيّمة بشأن المسودة الأولية لهذه الورقة البحثية. كما نعرب عن تقديرنا للجامعة الأردنية لتسهيلها عملية جمع البيانات. وتبقى جميع الأخطاء أو أوجه القصور، إن وجدت، مسؤوليتنا الكاملة.

الإقرارات الأخلاقية

أُجري هذا البحث وفقًا لمبادئ النزاهة البحثية والأخلاقيات العلمية. ونظرًا إلى عدم وجود مشاركين بشريين في هذه الدراسة، لم تكن هناك حاجة إلى الحصول على موافقة مسبقة أو اتخاذ إجراءات أخلاقية خاصة بالمشاركين. ومع ذلك، تم التعامل مع جميع مصادر البحث ومواده بمسؤولية، وبما يضمن احترام حقوق الملكية الفكرية. كما تم الالتزام بمبادئ الدقة والشفافية والمصداقية؛ لضمان سلامة النتائج.

بيان توافر البيانات

تتوافر البيانات التي جُمعت وحُللت خلال هذه الدراسة عند الطلب من الباحثين.

التمويل

لم يتلقَّ الباحثان أي تمويل لإجراء هذا البحث.

تضارب المصالح

يؤكد الباحثان عدم وجود أي تضارب في المصالح.

مساهمة الباحثين

- وضع الباحثان تصور الدراسة وتصميمها، وجمعا البيانات وحللاها.
- أعدّ الباحثان المسودة الأولى للمقال.
- راجع الباحثان النص وحرراه، واعتمدا النسخة النهائية للنشر.

الموافقة على النشر

يوافق الباحثان على تقديم هذه الورقة البحثية للنشر، وعلى نشرها في حال قبولها بعد استكمال إجراءات التحكيم وصدور قرار هيئة التحرير. كما يؤكدان أن هذا العمل لم يُنشر سابقًا، ولم يُقدَّم إلى أي مجلة أخرى للنظر في نشره.

التوصيات

١. إضافة نص قانوني يُعرّف "الحرب السيبرانية" ويُحدّد شروط الإسناد القانوني، لتقنين استثناء التغطية. من خلال تعديل قانون الجرائم الإلكترونية الأردني رقم ١٧ لسنة ٢٠٢٣

٢. اعتماد نماذج عقدية موحدة تتضمّن استثناءات دقيقة تُراعي طبيعة الهجمات السيبرانية.

Articles in Press

٣. إلزام شركات التأمين بالاستناد إلى تقارير محايدة لتبرير الاستثناء، لا تقديرات سياسية.

٤. تدخل الجهات الرقابية (البنك المركزي الأردني) لفرض شفافية أكبر في صياغة حدود التغطية بلغة مفهومة.

٥. دعم البحث القانوني المتخصص لتطوير معايير تأويل حديثة في قضايا التأمين السيبراني.

المراجع

أبو السعود، رمضان .(٢٠١١) .*عقد التأمين في القانون المصري* .دار الجامعة الجديدة.

أبو الهيجاء، محمد إبراهيم. (٢٠١٨). القيود المفروضة على شركات التأمين في العقود الإلزامية .*مجلة نقابة المحامين النظاميين*.

إسماعيل، حسن .(٢٠٢١) .*التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة: دراسة في القانون القطري والمقارن* .دار نشر جامعة قطر.

الرشيد، حسين وليد والجابر، ماهر جابر عودة. (٢٠٢٥). التحكيم في عقود التأمين الشامل للمركبات وفقًا للتشريع الأردني .*مجلة البحوث الفقهية والقانونية، ٤٣* (١)، ١١٢-١٤٥.

الرعاش، فهد علي. (٢٠٢٤). الحرب السيبرانية: التهديدات وسبل المواجهة .*مجلة القانون والعلوم الإنسانية والاجتماعية، ١* (١)، ٧٣-٩٦.

الزعبي، محمد أحمد دوجان. (٢٠٢١). تفسير الشروط الغامضة في العقود المدنية: دراسة مقارنة .*دراسات: علوم الشريعة والقانون، ٤٨* (١)، ٢١٥-٢٣٤.

السنهوري، عبد الرزاق .(١٩٦٤) .*الوسيط في شرح القانون المدني: الجزء السابع، العقود التي تقع على التأمين* .دار النهضة العربية.

شامبي بغدادي. (٢٠٢٣). تأمين الخطر السيبراني .*مجلة هيرودوت للعلوم الإنسانية والاجتماعية، ٧* (١)، ٢٣٧-٢٥٧.

شنوف، زينب. (٢٠٢٠). الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش .*المجلة الجزائرية للأمن والتنمية، ٩* (٢)، ٨٩-١٠٣.

شويات، بشار محمود سليمان .(٢٠١٩) .*الرقابة القضائية على عقد الإذعان في القانون الأردني: دراسة تحليلية* [أطروحة دكتوراه غير منشورة]. جامعة العلوم الإسلامية العالمية.

شويرب، جيلالي، ومراد، فائزة. (٢٠٢٣). مفهوم الحروب السيبرانية والأمن السيبراني .*مجلة الحقوق والحريات، ١١* (١)، ١٥٧-١٧٨.

التميمي، فتحي ماجد محمد .(٢٠١٠) .*دور المحكمة في تحقيق التوازن العقدي في القانون المدني الأردني: دراسة مقارنة* [رسالة ماجستير غير منشورة]. جامعة عمان العربية.

عبد الرضا، أنعام. (٢٠٢٣). توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى .*قضايا سياسية*، (٧٣)، ٤٢٣-٤٣٧.

عبد العال، جيهان أحمد وعطوة، أحمد. (٢٠٢٢). الحروب السيبرانية: دراسة في المفهوم والنشأة ومعدلات النجاح .*المجلة العلمية للدراسات التجارية والبيئية، ١٣* (٢)، ٢٨٧-٣١٠.

حميد، ليث ناجح. (٢٠١٨). موقف القانون الدولي من الهجمات الإلكترونية .*مجلة كلية الحقوق للعلوم القانونية والسياسية، ٧* (٢٤).

الذيابات، إبراهيم أحمد إبراهيم .(٢٠٠٥) .*حسن النية في تنفيذ العقود في القانون المدني الأردني: دراسة مقارنة* [رسالة ماجستير]. جامعة آل البيت.

محمود، لمى عبد الباقي وكيطان، إسراء نادر. (٢٠٢١). المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الإلكترونية .*مجلة العلوم القانونية*، ٣٦ (عدد خاص)، ٣٣٦–٣٦٢. https://doi.org/10.35246/jols.v36i0.435

Articles in Press

الهيئة الوطنية للأمن السيبراني .(٢٠٢٢) .*إطار الأمن السيبراني لقطاع التأمين*.

وزارة الاقتصاد الرقمي والريادة الأردنية .(٢٠٢٣) .*تقرير التحول الرقمي الوطني: التحديات والتوصيات*.

وكالة أنباء الإمارات .(٢٠٢٣) .*مجلس الأمن السيبراني يعزز مبادرات الحماية الوطنية* https://www.wam.ae .

القوانين والقرارات القضائية

القانون المدني الأردني رقم ٤٣ لسنة ١٩٧٦.

القانون المدني المصري رقم ١٣١ لسنة ١٩٤٨.

القانون الاتحادي الإماراتي رقم ٥ لسنة ٢٠١٢.

محكمة النقض المصرية. (د.ت.). طعن مدني رقم ٢٥٩٢ لسنة ٦٨ قضائية. بوابة هيئة قضايا الدولة.

محكمة التمييز الأردنية. (٢٠٠٣). قرار حقوق رقم ٢٠٠٣/٤٤٩٥. قاعدة البيانات القضائية قسطاس.

محكمة التمييز الأردنية. (٢٠٠٥). قرار حقوق رقم ٢٠٠٥/١٨٠٥. قاعدة البيانات القضائية قسطاس.

محكمة التمييز الأردنية. (٢٠١٦). قرار حقوق رقم ٢٠١٦/٢٣٠٧. قاعدة البيانات القضائية قسطاس.

محكمة التمييز الأردنية. (٢٠١٦). قرار حقوق رقم ٢٠١٦/٢٥٣٩. قاعدة البيانات القضائية قسطاس.

References

Albalawi, K. (2025). Opportunities for cyber insurance to address the challenges of cyber-attacks: Repercussions for SMEs. *University of Sharjah Journal for Law Sciences, 22*(1).

Alhamdan, M. F. (2023). *The combined application of force under Article 2(4) and Article 51 of the United Nations Charter for cyber warfare: Examining and learning lessons from the Iranian cyber warfare threat to Saudi Arabia* [Doctoral dissertation, Lancaster University].

Bace, B., Dubois, E., & Tatar, U. (2024). Resilience against catastrophic cyber incidents: A multistakeholder analysis of cyber insurance. *Electronics, 13*(14), Article 2768. https://doi.org/10.3390/electronics13142768

Battah, M. (2020). Claim of transport commission agent liability and compensation provisions. *Journal of Social Sciences (COES&RJ-JSS)*.

Brunner, I. (2022). Insurance policies and the attribution of cyber operations under international law: A commentary. *New York University Journal of International Law and Politics, 55*, 179.

Chopra, A. (2021). Cyberattack—Intangible damages in a virtual world: Property insurance companies declare war on cyber-attack insurance claims. *Ohio State Law Journal, 82*, 121.

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B. J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. *Computers & Security*, Article 103886.

DeField, A., Perez, A. A., & Small, K. V. (2023, May 17). *Merck wins again in cyber coverage battle*. Hunton Insurance Recovery Blog. https://www.hunton.com/hunton-insurance-recovery-blog/merck-wins-again-in-cyber-coverage-battle

Articles in Press

Ferland, J. (2019). Cyber insurance—What coverage in case of an alleged act of war? Questions raised by the *Mondelez v. Zurich* case. *Computer Law & Security Review, 35*(4), 369–376.

Gordley, J. (2006). The enforceability of unfair terms in Latin civil law traditions. *European Review of Contract Law*.

Gordon, G. (2023). An introduction to risk allocation in oil and gas contracts from an English law perspective. In *Knock-for-knock indemnities and the law* (pp. 20–64). Informa Law from Routledge.

He, Q., Faure, M., & Chen, C. Y. (2025). Insuring the "uninsurable" cyberwarfare: Rethinking war exclusions in cyber policies and the role of insurance in global cybersecurity governance. *The Geneva Papers on Risk and Insurance—Issues and Practice*, 1–32.

Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance, 15*(1), 98–114.

Jones, D. (2022, November 8). *Mondelez settlement in NotPetya case renews concerns about cyber insurance coverage*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/mondelez-zurich-notpetya-cyber-insurance-settlement/636029

Lahmann, H. (2023). The plea of necessity in cyber emergencies: Unresolved doctrinal questions. *Nordic Journal of International Law, 92*(3), 422–445.

Lloyd's. (2022, August 16). *Market Bulletin Y5381: State-backed cyber-attack exclusions* [PDF]. https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf

Lubin, A. (2021). Public policy and the insurability of cyber risk. *Texas Journal of Law & Technology, 5*, 45.

Markopoulou, D. (2021). Cyber-insurance in EU policy-making: Regulatory options, the market's challenges and the U.S. example. *Computer Law & Security Review, 43*, Article 105627.

Mondelez International, Inc. v. Zurich American Insurance Co., No. 2018 L 011008 (Circuit Court of Cook County, Illinois, October 10, 2018). https://regmedia.co.uk/2022/11/02/pacer_mondelez_zurich_complaint.pdf

Nagurney, A., Pour, I., & Kormych, B. (2025). Integrated crop and cargo war risk insurance: Application to Ukraine. *International Transactions in Operational Research*.

NAIC Staff. (2024, October 15). *Report on the cyber insurance market* [Memorandum]. National Association of Insurance Commissioners.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity, 5*(1), Article tyz002.

Rovetto, J. M., Jr. (2022). Cyberwarfare and cyber insurance: Exploring when a cyberattack can negate a cyber insurance claim. *Journal of Business & Technology Law, 18*, 309.

Articles in Press

Schmitt, M. N. (2017). Computer network attack and the use of force in international law: Thoughts on a normative framework. In *The use of force in international law* (pp. 379–431). Routledge.

Shackelford, S. J. (2020). Wargames: Analyzing the act of war exclusion in insurance coverage and its implications for cybersecurity policy. *Yale Journal of Law & Technology, 23*, 362.

Smith, M., & Mulrain, G. (2017). Equi-failure: The national security implications of the Equifax hack and a critical proposal for reform. *Journal of National Security Law & Policy, 9*, 549.

Unegenova, Z., Adilgazy, S., & Teleuev, G. (2024). Legal basis for explaining the contractual terms of *contra proferentem*. *Bulletin of L. N. Gumilyov Eurasian National University: Law Series, 146*(1), 233–246.

United Nations. (1945). *Charter of the United Nations*. https://www.un.org/en/about-us/un-charter

Wolff, J. (2021). "Cyberwar by almost any definition": NotPetya, the evolution of insurance war exclusions, and their application to cyberattacks. *Connecticut Insurance Law Journal, 28*, 85.

Wolff, J. (2024). The role of insurers in shaping international cyber-security norms about cyber-war. *Contemporary Security Policy, 45*(1), 141–170.

Woods, D. W., & Weinkle, J. (2019, September). *Market definitions of cyber war*. Conference on Cyber Norms: Dealing with Uncertainty.

---

[١] تعرّضت شركة *Mondelez* لهجوم سيبراني بواسطة فيروس NotPetya في يونيو ٢٠١٧، ما عطّل آلاف الأنظمة وكبّدها خسائر تفوق ١٠٠ مليون دولار. رفعت دعوى ضد شركة *Zurich Insurance* مطالبةً بالتعويض بموجب بوليصة تأمين تغطي فشل الأنظمة، لكن *Zurich* رفضت، مستندة إلى بند استثناء "الأعمال الحربية". رغم عرضها لاحقًا دفع ١٠ ملايين دولار، تراجعت، مما دفع *Mondelez* لتوسيع الدعوى. وفي ٢٠٢١، حكمت المحكمة جزئيًا لصالح *Zurich*، معتبرةً أن التفاوض الإلكتروني لا يُنشئ التزامًا. انتهى النزاع بتسوية ودّية في ٢٠٢٢ دون إعلان تفاصيلها، وشكّلت القضية مرجعًا بارزًا في تفسير استثناءات الحرب بالتأمين السيبراني. بالرجوع إلى: (Mondelez International, Inc. v. Zurich American Insurance Co. 2018).

[٢] في يونيو ٢٠١٧، تعرّضت شركة *Merck* لهجوم *NotPetya* السيبراني عطّل أكثر من ٤٠,٠٠٠ جهاز وتسبب بخسائر قُدّرت بـ ١,٤ مليار دولار. رفعت الشركة دعوى في ٢٠١٨ ضد أكثر من ٣٠ شركة تأمين بموجب بوليصة "all-risks"، لكن التعويض رُفض استنادًا إلى بند استثناء "العمل العدائي". في ديسمبر ٢٠٢١، قضت محكمة نيوجيرسي لصالح *Merck* بأن الاستثناء لا يشمل هجومًا إلكترونيًا على شركة مدنية. أيدت محكمة الاستئناف الحكم في مايو ٢٠٢٣، مؤكدة أن البند يتطلب عملاً عسكريًا مباشرًا. وفي يناير ٢٠٢٤، تم التوصّل إلى تسوية قُدّرت بنحو ٧٠٠ مليون دولار قبل عرض القضية على المحكمة العليا. بالرجوع إلى (DeField et al., 2023).

Articles in Press