



INNOVATIVE: Journal Of Social Science Research Volume

4 Nomor 4 Tahun 2024 Page 10076-10093

E-ISSN 2807-4238 and P-ISSN 2807-4246

Website: <https://j-innovative.org/index.php/Innovative>

Tren Publikasi Asuransi Siber: Evaluasi Melalui Lensa PRISMA dalam Literatur Ilmiah

Muhammad Ibrahim Rachman^{1✉}, Ali Sadikin^{1✉}
Sekolah Tinggi Management Risiko & Asuransi

Email: greet.ibrahim@gmail.com^{1✉}

Abstrak

Keamanan siber menjadi aspek krusial dalam melindungi informasi dan merupakan infrastruktur kritis di era digital saat ini. Meskipun perkembangan teknologi informasi memberikan manfaat besar, namun juga membuka celah terhadap serangan siber yang semakin canggih dan merugikan. Penelitian ini bertujuan untuk menginvestigasi dan mengevaluasi tren publikasi dalam domain asuransi siber. Dengan menggunakan metode analisis bibliometrik dan pendekatan metodologi PRISMA, penelitian ini menganalisis literatur yang tersedia, mengungkapkan dinamika perkembangan, fokus penelitian, dan topik-topik penelitian yang mendominasi literatur terbaru mengenai asuransi siber. Data dikumpulkan melalui pencarian di Scopus dengan kata kunci terkait asuransi siber, dengan fokus pada judul artikel selama periode penelitian. Hasil analisis memberikan informasi yang komprehensif, memungkinkan pemahaman mendalam tentang kontribusi penelitian dan arah masa depan dalam menghadapi tantangan keamanan siber. Penelitian ini memberikan wawasan bagi praktisi, akademisi, dan pemangku kepentingan yang berkepentingan dalam mengoptimalkan strategi asuransi siber di tengah lanskap ancaman yang terus berkembang.

Kata Kunci: Cyber Attack, Cyber Crime, Cyber Insurance, Cybersecurity, PRISMA

Abstract

Cyber security is a crucial aspect in protecting information and is a critical infrastructure in the current digital era. Although the development of information technology provides great benefits, it also opens up opportunities for cyber attacks that are increasingly sophisticated and detrimental. This research aims to investigate and evaluate publication trends in the cyber insurance domain. Using bibliometric analysis methods and the PRISMA methodological approach, this research analyzes the available literature, revealing the dynamics of development, research focus, and research topics that dominate the latest literature on cyber insurance. Data was collected through a search on Scopus with keywords related to cyber insurance, with a focus on article titles during the research period. The analysis results provide comprehensive information, enabling an in-depth understanding of research contributions and future directions in addressing cybersecurity challenges. This research provides insights for practitioners, academics and stakeholders interested in optimizing cyber insurance strategies amidst an ever-evolving threat landscape

Keywords: Cyber Attack, Cyber Crime, Cyber Insurance, Cybersecurity, PRISMA;

PENDAHULUAN

Era digital yang semakin terkoneksi membuat internet berkembang menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari (Zheng et al., 2016). Studi saat ini menunjukkan bahwa pengguna internet meningkat di seluruh dunia (Kumar & Chaudhary, 2014). Manfaat positif yang dapat diperoleh dari teknologi informasi adalah memudahkan individu atau kelompok dalam melakukan aktifitasnya, sedangkan dampak negatif timbul karena penyalahgunaan teknologi oleh individu atau kelompok untuk tindakan kejahatan dunia maya (cybercrime) yang dapat merugikan orang lain (Gani, 2018). Kemajuan teknologi yang semakin pesat juga diiringi dengan sistem keamanan yang semakin meningkat sebagai respon dari tindakan cybercrime yang semakin meningkat drastis (Peters et al., 2018).

Beberapa kasus kejahatan siber di kancah international yang menggemparkan dunia di antaranya pada tahun 2017, serangan ransomware global "WannaCry". Serangan ini masuk ke sistem operasi Windows, mengenkripsi data, dan menuntut pembayaran tebusan dalam bentuk bitcoin senilai \$600. Selain itu, serangan ini memengaruhi sekitar 200.000 komputer di lebih dari 150 negara. Secara keseluruhan, ransomware ini berdampak besar pada beberapa industri dengan biaya global sekitar 6 miliar poundsterling untuk perbaikan. Pada tahun 2014, Yahoo menjadi korban salah satu serangan siber terbesar tahun itu ketika 500 juta akun terpengaruh. Selama serangan tersebut, informasi pengguna dan kata sandi dicuri.

Sedangkan di Indonesia pada Mei 2023, Bank Syariah Indonesia dikejutkan oleh serangan ransomware dari kelompok hacker Lockbit yang berasal dari Rusia. Menjadikan server bank lumpuh selama 5 hari, sehingga nasabah tidak dapat mengakses aplikasi mobile banking. Lockbit berhasil mencuri 1,5 terabyte data, termasuk informasi pribadi nasabah dan pegawai. Kasus ini menjadikan salah satu serangan ransomware terbesar di Indonesia. Pada tahun 2022, terjadi serangkaian kasus pembobolan data yang menghebohkan di Indonesia. Salah satu peretas yang menjadi sorotan adalah hacker yang dikenal dengan nama Bjorka. Hacker ini mencuri data pribadi dari beberapa perusahaan di Indonesia, dan aksinya sempat viral pada awal Januari 2022.

Dari rentetan kejadian tersebut menggambarkan kompleksitas tantangan keamanan siber yang dihadapi oleh organisasi maupun individu. Oleh karena itu, hal tersebut mendorong peneliti untuk melakukan penelitian dan kajian yang lebih mendalam guna menghadapi tantangan tersebut. Tujuan penelitian ini adalah untuk menginvestigasi dan mengevaluasi tren publikasi dalam domain asuransi siber, dimana keamanan siber telah menjadi fokus utama dalam melindungi informasi dan infrastruktur kritis. Dalam konteks ini, analisa terhadap tren publikasi dengan menggunakan suatu metodologi yang telah ditentukan akan memberikan wawasan yang berharga terkait perkembangan literatur di bidang asuransi siber. Dengan pemahaman yang lebih mendalam terhadap tren ini, diharapkan dapat ditemukan strategi yang lebih efektif untuk mengatasi risiko keamanan siber yang terus berkembang.

Systematic Literature Review (SLR) merupakan istilah suatu cara identifikasi, evaluasi, dan interpretasi semua ketersediaan penelitian yang relevan terhadap rumusan masalah atau area topik yang diteliti (Calderón & Ruiz, 2015). Metode ini melibatkan pencarian literatur yang sistematis dan terstruktur, serta pengevaluasian kualitas literatur yang ditemukan (Saputro et al., 2021). Tinjauan literatur sistematis yang melibatkan panggung global melalui basis data seperti Scopus akan memberikan pandangan komprehensif tentang perkembangan penelitian dalam asuransi siber. Melalui tinjauan ini, tren penelitian, topik yang paling dibahas, serta pendekatan dan metode yang digunakan dapat diidentifikasi. Analisis bibliometrik akan dilakukan dengan fokus pada dua pendekatan, yaitu co-occurrence dan co-citation. Dalam analisis co-occurrence, akan diidentifikasi kata kunci atau istilah yang sering muncul bersama dalam literatur tentang asuransi siber. Hal ini akan membantu dalam mengidentifikasi topik yang paling sering dibahas dan hubungan antara konsep-konsep tersebut. Sementara itu, dengan menganalisis co-citation, kita dapat memahami sejauh mana dua sumber atau lebih dianggap memiliki keterkaitan atau

relevansi dalam konteks penelitian tertentu. Ini dapat memberikan wawasan tentang hubungan antara sumber-sumber yang sering dikutip bersama dalam literatur ilmiah.

Tinjauan ini menggunakan artikel-artikel dari hasil pencarian di basis data Scopus. Pencarian dilakukan pada 30 Agustus 2023. Artikel yang digunakan dalam tinjauan ini harus memenuhi kriteria kriteria yang sudah ditentukan dan dipublikasikan pada tahun 2002-2023. Tujuan dari tinjauan ini adalah untuk mencoba menjawab Research Questions (RQ) diantaranya :

RQ1 : Bagaimana tren penelitian dalam asuransi siber telah berkembang dari waktu ke waktu berdasarkan analisis bibliometrik?

RQ2 : Apa saja topik-topik penelitian yang paling dominan dalam literatur terkait asuransi siber?

RQ1 bertujuan untuk memahami evolusi penelitian dalam bidang asuransi siber seiring berjalannya waktu. Analisis bibliometrik akan digunakan untuk mengidentifikasi perubahan tren penelitian, seperti jumlah publikasi setiap tahun, penulis yang paling aktif dalam melakukan penelitian asuransi siber, subjek area penelitian, sumber dokumen publikasi, sebaran afiliasi dan negara yang aktif melakukan penelitian asuransi siber. Tujuan dari penelitian RQ2 adalah untuk mengidentifikasi dan menganalisis topik-topik penelitian yang paling mendominasi dalam literatur terbaru mengenai asuransi siber.

Dengan menjawab kedua tujuan penelitian ini, kita dapat memberikan pemahaman yang lebih baik tentang perkembangan dan arah penelitian dalam bidang asuransi siber serta topik-topik yang sedang mendominasi dalam literatur terkini.

METODE PENELITIAN

Untuk menemukan jawaban atas pertanyaan penelitian yang diajukan, dua metode standar diterapkan – PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Page et al., 2021) dan Analisis Bibliometrik. Penulis menggunakan pendekatan PRISMA untuk memilih karya-karya ilmiah mengenai asuransi siber dari basis data ilmiah populer dengan kriteria inklusi dan eksklusi yang jelas. Roemer & Borchardt Rachel (2015) menyebutkan bibliometrik merupakan seperangkat metode kuantitatif yang digunakan untuk mengukur, melacak, serta menganalisis literatur ilmiah berbasis cetak.

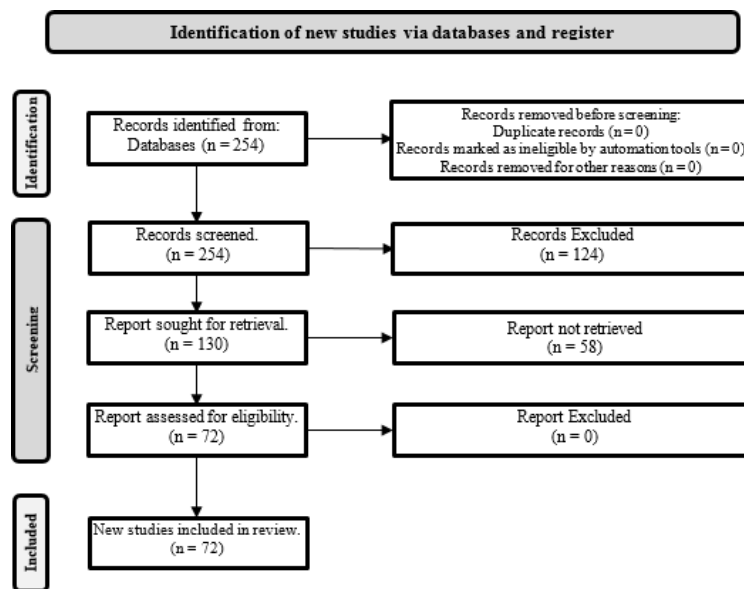
Metode bibliometrik menganalisis domain keilmuan tertentu dengan menggunakan data bibliografi melalui dua pendekatan utama yaitu analisis kinerja dan pemetaan ilmu pengetahuan (Cobo et al., 2011). Untuk menentukan dampak dan pengaruh dari berbagai publikasi yang berbeda, pertama mempelajari jumlah absolut dan relatif dari artikel yang paling banyak dikutip. Kedua, mengikuti pendekatan pemetaan bibliometrik dengan

menggunakan perangkat lunak VOS Viewer dari van Eck & Waltman (2010), yang memungkinkan penulis memvisualisasikan beragam jaringan yang dihasilkan dari analisis co-word dan co-citation. VOS Viewer digunakan untuk menganalisis bibliometrik, mencari referensi yang paling banyak digunakan pada disiplin ilmu tertentu, mencari topik penelitian yang berpotensi untuk diteliti, dan masih banyak lagi (Effendy et al., 2021).

Metode PRISMA merupakan pendekatan yang telah diakui secara luas untuk mengorganisir dan menyajikan informasi dengan sistematis dalam penelitian yang sudah ada. Tinjauan sistematis menggunakan metode standar PRISMA diterapkan dalam penelitian ini untuk mengevaluasi literatur yang ada dalam bidang asuransi siber. Untuk memvisualisasikan langkah-langkah proses, digunakan diagram alir PRISMA, yang dapat dilihat pada Gambar 1.

Artikel-artikel tersebut ditinjau selama periode 2002 hingga 2023, dalam basis Scopus. Scopus merupakan salah satu basis data untuk analisis bibliometrik, memiliki jangkauan yang lebih luas pada penerbitan artikel serta mencakup jurnal yang unggul namun terbatasnya akses untuk artikel terbaru (Shukla, 2019). Pencarian kata kunci yang digunakan untuk mencari data dokumen adalah Cyber Insurance, Cyber Risk Insurance, Cyber Attack Insurance, Cyber Security Insurance, dan Cybercrime Insurance. Pencarian dilakukan terhadap judul artikel dari karya-karya tersebut. Pencarian dilakukan pada tanggal 30 Agustus 2023.

Kriteria pencarian tersebut menghasilkan 254 dokumen. Kemudian, proses screening dengan kriteria kueri pencarian dimodifikasi untuk membatasi hasil pencarian dokumen hanya yang ditulis dalam bahasa Inggris saja. Selain itu, kueri lebih lanjut dibuat dengan membatasi sumber tipe dokumen pada Journal dan Conference proceeding. Lalu kueri disempurnakan dengan memasukkan jenis dokumen berupa article dan document review dan mengecualikan conference paper, editorial, note, erratum dan letter. Dalam screening awal tersebut total sebanyak 124 dokumen yang dikeluarkan dan menyisakan sebanyak 130 dokumen. Selanjutnya, kriteria akhir adalah menentukan dokumen yang dapat diunduh untuk dipelajari dan memastikan dokumen tersebut sesuai dengan topik pembahasan. Berdasarkan kriteria tersebut diperoleh sebanyak 72 dokumen. Sehingga kumpulan data akhir yang telah disempurnakan mencakup semua dokumen yang diterbitkan dari pertama kali penelitian diterbitkan yang terindeks Scopus tahun 2002 hingga Agustus 2023 sebanyak 72 dokumen. Berikut sebagian dari format penelusuran yang dilakukan:



Gambar 1. Proses informasi SLR menggunakan Diagram Alir PRISMA

HASIL DAN PEMBAHASAN

Negara dan Instansi Penulis

Tabel 1. Distribusi Artikel Berdasarkan Negara dan Institusi yang Paling Berpengaruh.

R	Negara		Institusi			
	N	%	N	%	N	%
1	United States	44	43.1%	Nanyang Technological University	6	3.9%
2	United Kingdom	7	6.9%	University of Wisconsin-Milwaukee	4	2.6%
3	Singapore	6	5.9%	University of Oxford	4	2.6%
4	China	5	4.9%	University of Houston	3	2.0%
5	Germany	5	4.9%	Michigan Technological University	3	2.0%
6	France	4	3.9%	University of St. Gallen	3	2.0%
7	Italy	4	3.9%	Sorbonne Université	2	1.3%
8	Switzerland	4	3.9%	RAND Corporation	2	1.3%
9	Sweden	3	2.9%	Gottfried Wilhelm Leibniz Universität Hannover	2	1.3%
10	Austria	2	2.0%	Libera Università Maria Ss. Assunta	2	1.3%

Terlihat pada Tabel 1, sebanyak 43.1% dari daftar 10 negara yang paling banyak berkontribusi dalam publikasi penelitian asuransi siber yaitu dari Amerika dengan 44 publikasi, sementara beberapa negara lain seperti Inggris, Singapura, China, Jerman, Prancis, Italia, Swis, Swedia dan Austria memiliki kontribusi dibawah 10%. Tingginya

presentase Amerika tidak lepas dari popularitas asuransi siber dinegara tersebut, berdasarkan menjadi wilayah terdepan di pasar asuransi siber (Ravi R & Vineet K, 2023).

Institusi yang berperan dalam publikasi asuransi siber tersebar di berbagai universitas di dunia. Nanyang Technological University dari Singapura mendominasi dalam penelitian asuransi siber, yang menerbitkan 6 publikasi atau 3.9%. Angka ini tidak terlalu signifikan jika dibandingkan dengan jumlah publikasi di universitas lainnya. University of Wisconsin-Milwaukee dan University of Oxford yang masing masing memunyai 4 publikasi atau 2.6%. University of Houston, Michigan Technological University dan University of St. Gallen, masing-masing menerbitkan 3 pulikasi atau 2.0%, serta Sorbonne Université, RAND Corporation, Gottfried Wilhelm Leibniz Universität Hannover dan Libera Università Maria Ss. Assunta menerbitkan 2 publikasi atau 1.3%.

Publikasi oleh Penulis

Tabel 2. Penulis Paling Produktif dalam Publikasi Penelitian Asuransi Siber

No	Nama Penulis	Universitas/Institusi	Jumlah Publikasi
1	Niyato, D.	Nanyang Technological University	5
2	Wang, L.	University of Wisconsin-Milwaukee, Milwaukee	5
3	Wei, W.	University of Wisconsin-Milwaukee, Milwaukee	5
4	Eling, M.	Institute of Insurance Economics, University of St. Gallen.	4
5	Franke, U.	RISE Research Institutes of Sweden	4
6	Hillairet, C.	Ensaie Paris, Centre de Recherche en Economie et Statistique, CREST.,	4
7	Liu, Z.	University of Wisconsin-Milwaukee, Milwaukee	4
8	Mazzocchi, A.	University of Rome Tor Vergata	4
9	Ten, C.W.	Michigan Technological University, Houghton	4
10	Wang, P.	Nanyang Technological University	4

Tabel 2 memaparkan 10 penulis paling produktif yang menerbitkan penelitian mengenai asuransi siber, dimana jumlah publikasi yang diterbitkan tidak terdapat selisih yang besar, yaitu berjumlah 4 hingga 5 publikasi untuk setiap penulis. Dua penerbit paling produktif berasal dari Amerika Serikat, khususnya University of Wisconsin-Milwaukee, Milwaukee. Peringkat ini masih tidak lepas dari popularitas asuransi siber di negara tersebut.

Penulis paling produktif lainnya yang berasal dari Nanyang Technological University,

Singapura yaitu Niyato, D. dan Wang, P. dengan 5 dan 4 publikasi untuk setiap penulis kemudian 2 publikasi lainnya yang tidak masuk kedlam 10 besar dalam penulis paling produktif. Hal ini menunjukkan mengapa universitas tersebut menjadi peringkat pertama sebagai universitas paling banyak berkontribusi dalam publikasi asuransi siber. Penulis produktif lainnya berasal dari berbagai negara seperti Switzerland, Swedia, Prancis, dan Italia.

Publikasi Paling Sering Dikutip

Tabel 3. Publikasi yang Paling Sering Dikutip

No	Judul	Penulis	TC	C/Y
1	Cyber-insurance survey	Marotta A.; Martinelli F.; Nanni S.; Orlando A.; Yautsiukhin A.	126	18.0
2	Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: A cyber insurance-based model	Hoang D.T.; Wang P.; Niyato D.; Hossain E.	117	16.7
3	Content analysis of cyber insurance policies: How do carriers price cyber risk?	Romanosky S.; Ablon L.; Kuehn A.; Jones T.	76	15.2
4	What do we know about cyber risk and cyber risk insurance?	Eling M.; Schnell W.	92	11.5
5	The cyber insurance market in Sweden	Franke U.	56	8.0
6	A framework for using insurance for cyber-risk management	Gordon L.A.; Loeb M.P.; Sohail T.	155	7.4
7	A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks	Zhang R.; Zhu Q.; Hayel Y.	46	6.6
8	A framework for incorporating insurance in critical infrastructure cyber risk strategies	Young D.; Lopez J., Jr.; Rice M.; Ramsey B.; McTasney R.	51	6.4
9	Why IT managers don't go for cyber-insurance products	Bandyopadhyay T.; Mookerjee V.S.; Rao R.C.	75	5.0
10	Should your firm invest in cyber risk insurance?	Shackelford S.J.	48	4.0

Tabel 3 menunjukkan publikasi dengan jumlah kutipan tertinggi yang diurutkan berdasarkan kutipan per tahun (C/Y). Publikasi Marotta et al. (2017) yang paling banyak dikutip secara relatif dapat dianggap sebagai tinjauan menyeluruh mengenai asuransi siber, yang pada saat itu publikasi tersebut terbit di era pertumbuhan kesadaran terhadap risiko siber meningkat. Publikasi yang paling banyak dikutip secara absolut (155 kutipan)

diterbitkan oleh Gordon et al. (2003), dan dapat dianggap sebagai karya penting dari aliran penelitian utama dalam topik ini.

Dua dari publikasi yang paling banyak dikutip membahas mengenai praktik tentang asuransi siber. Franke (2017) fokus pada karakteristik pasar asuransi siber di Swedia, termasuk pertumbuhan pasar, perubahan regulasi, dan preferensi konsumen di wilayah tersebut. Bandyopadhyay et al. (2009) menggali alasan di balik ketidakcakapan manajer IT dalam mengadopsi produk asuransi siber, mencakup faktor psikologis, hambatan praktis, atau mungkin kurangnya pemahaman.

Tiga publikasi membahas mengenai kebijakan dan praktik asuransi siber. Romanosky et al. (2019) membahas fokus pada analisis isi kebijakan asuransi siber untuk memahami bagaimana perusahaan penanggung menghargai risiko siber dalam produk asuransi mereka. Gordon et al. (2003) mengembangkan kerangka kerja untuk menggabungkan asuransi sebagai alat utama dalam strategi manajemen risiko siber, melibatkan identifikasi, evaluasi, dan mitigasi risiko. Young et al. (2016) mengusulkan kerangka kerja yang mengintegrasikan asuransi ke dalam strategi manajemen risiko siber untuk infrastruktur kritis, dengan fokus pada perlindungan dan pemulihan.

Tiga lainnya berisi mengenai inovasi dalam model asuransi siber. Zhang et al. (2017) menerapkan pendekatan permainan bi-level dalam konteks asuransi siber, dengan mempertimbangkan serangan dan keamanan jaringan komputer sebagai faktor strategis. Shackelford (2012) membahas pertanyaan kritis tentang kebijakan investasi dalam asuransi risiko siber, mencakup analisis cost-benefit dan pertimbangan strategis untuk perusahaan.

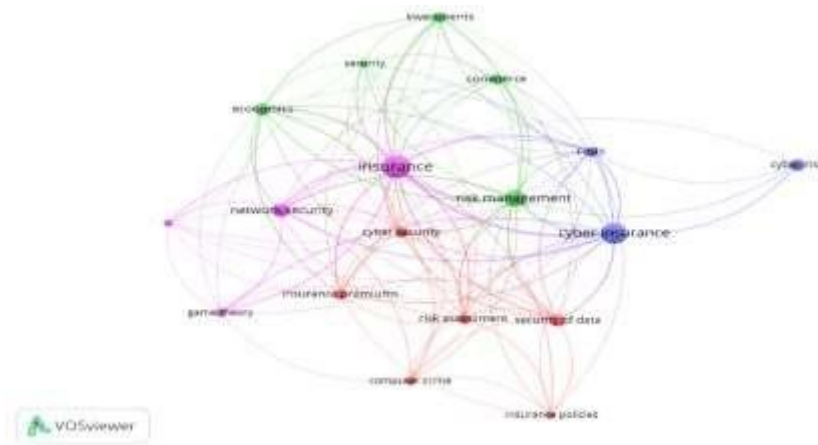
Secara keseluruhan, data di atas menunjukkan bahwa topik keamanan siber dan asuransi siber telah menarik perhatian yang signifikan dari komunitas akademis.

Peta Perkembangan Publikasi Berdasarkan Kata Kunci

Dalam 72 artikel yang dianalisis, diperoleh 485 kata kunci, di mana 21 di antaranya memenuhi ambang batas minimal 4 kemunculan. Kata kunci "Insurance" dengan 35 kemunculan dan 125 total kekuatan tautan, "Risk Management" dengan 19 kemunculan dan 87 total kekuatan tautan dan "Cyber Insurance" 30 kemunculan dan 80 total kekuatan tautan, merupakan kata kunci utama.

Tabel 4. Kata Kunci yang Paling Sering Digunakan

Kata Kunci	Frekuensi	Total Link Strength
Insurance	35	125
Risk Management	19	87
Cyber Insurance	30	80
Economics	10	51
Network Security	12	51
Security Of Data	10	45
Investments	7	35
Insurance Premiums	7	34
Risk Assessment	7	34
Cyber Security	8	30



Gambar 2. Analisis Kata Bersama, Disiapkan dengan menggunakan Perangkat Lunak VOS Viewer

Dalam kluster merah, terdapat fokus yang kuat pada keamanan siber dan asuransi. Keyword seperti "Computer Crime", "Cyber Security", "Insurance Policies", "Insurance Premiums", "Risk Assessment", dan "Security of Data" menunjukkan perhatian terhadap isu kejahatan komputer, keamanan siber, dan implementasi kebijakan asuransi sebagai upaya perlindungan terhadap risiko keamanan siber.

Kluster hijau menunjukkan keterkaitan antara keamanan siber dengan aspek ekonomi dan manajemen risiko. "Commerce", "Economics", "Investments", "Risk Management", dan "Security" mencerminkan pemahaman bahwa keamanan siber tidak hanya berdampak pada teknis, tetapi juga pada keputusan ekonomi dan strategi manajemen risiko.

Dalam kluster ungu, fokus pada Infrastruktur teknis terlihat melalui "Electric Power Transmission" dan "Game Theory". Penambahan kata kunci "Insurance" menyoroti peran asuransi dalam mengelola risiko terkait dengan infrastruktur teknis seperti transmisi listrik

dan aplikasi teori permainan dalam pengambilan keputusan asuransi dan keamanan siber.

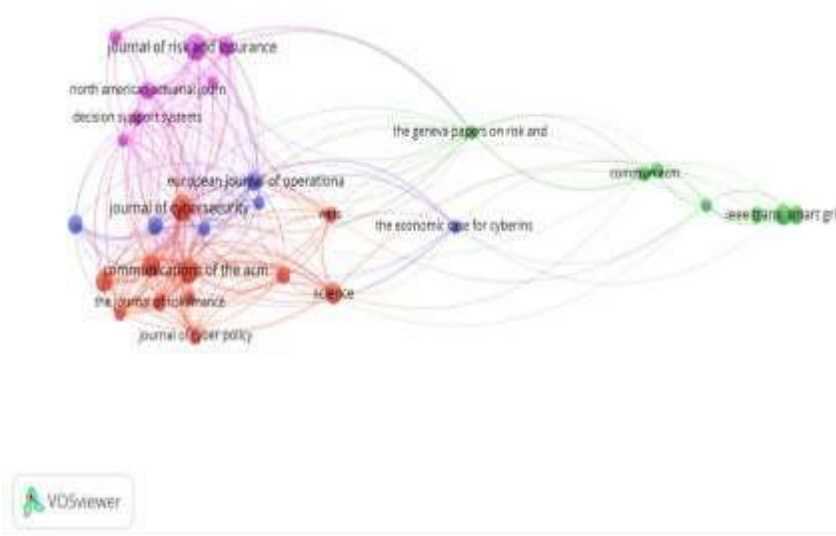
Kluster biru mencakup konsep biaya operasional (Cost) dan elemen-elemen terkait keamanan siber seperti "Cyber Insurance" dan "Cyber Risk". Ini mencerminkan pemahaman bahwa keamanan siber juga terkait erat dengan biaya operasional, perlindungan aset melalui asuransi siber, dan pengelolaan risiko yang terkait dengan serangan siber.

Analisis ini memberikan gambaran holistik tentang keterkaitan berbagai konsep dalam keamanan siber, mencakup aspek teknis, ekonomi, manajemen risiko, dan peran asuransi dalam mengelola risiko dan melindungi aset terhadap ancaman keamanan siber.

Peta Perkembangan Publikasi Berdasarkan Kutipan Jurnal

Tabel 5. Kata Kunci yang Paling Sering Digunakan

Source	Citations	Total Link Strength
Communications of The Acm	21	241
Journal of Cybersecurity	22	220
Journal of Risk And Insurance	22	188
Computers & Security	16	167
The Geneva Papers on Risk and Insurance - Issues and Practice	13	158



Gambar 3. Jaringan Kutipan Jurnal, Disiapkan menggunakan Perangkat Lunak VOS Viewer

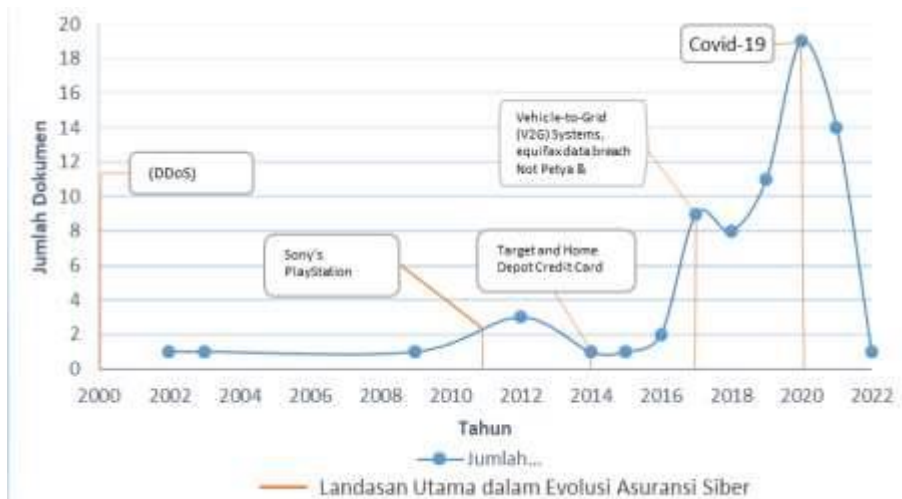
Dalam 72 artikel yang dianalisis, diperoleh 1806 sumber artikel, di mana 35 di antaranya memenuhi ambang batas minimal 6 penerbitan. Cluster Merah menonjolkan keamanan siber, komputer, dan isu-isu privasi. Communications of the ACM dan Computers & Security menjadi pusat perhatian utama, menandakan bahwa literatur dalam cluster ini banyak membahas tentang keamanan siber dan isu-isu terkait di dunia komputer.

Cluster Hijau perhatian tertuju pada hubungan antara keamanan siber dan isu-isu asuransi serta risiko. *Journal of Cybersecurity* dan *The Geneva Papers on Risk and Insurance - Issues and Practice* memiliki hubungan yang kuat, menunjukkan bahwa diskusi keamanan siber dalam konteks asuransi dan risiko sering kali terjalin bersama.

Cluster Biru menyoroiti aspek keuangan dan aktuaria dalam literatur asuransi. Jurnal seperti *Journal of Risk and Insurance* dan *North American Actuarial Journal* menjadi pusat perhatian, menandakan bahwa isu-isu keuangan dan aktuaria saling terkait dalam konteks ini.

Cluster Ungu fokus pada keamanan siber dan teknologi informasi dalam konteks smart grid. *IEEE Transactions on Smart Grid* dan *IEEE Transactions on Power Systems*. memiliki hubungan erat, menunjukkan bahwa literatur dalam dua jurnal ini sering kali saling mengacu karena fokus bersama pada keamanan dan manajemen risiko dalam konteks smart grid.

Jumlah Publikasi Asuransi Siber per Tahun dan Peristiwa yang Mempengaruhinya



Gambar 4. Tren Publikasi Asuransi Siber per tahun dan peristiwa yang mempengaruhinya

Dekade 2000-an: Konsep Awal dan Integrasi Asuransi Siber dalam Manajemen Risiko

Pada era ini, jumlah publikasi mengenai asuransi siber masih sangat terbatas, hanya tercatat tiga publikasi yang tersebar di tahun 2002, 2003, dan 2009. Meskipun terbatas, dekade awal abad ke-21 ditandai oleh peristiwa serangan DDoS pada bulan Februari 2000 (Siegel et al., 2002). Serangan tersebut menargetkan beberapa situs web paling canggih seperti Yahoo, Buy.com, dan CNN, menyebabkan kerugian finansial mencapai \$ 1,2 miliar. Kejadian DDoS attacks ini menjadi fokus utama pada awal dekade tersebut yang membuat literatur berfokus pada pengembangan konsep dan kerangka kerja awal dalam manajemen risiko siber. Gordon et al. (2003) dan Siegel et al. (2002) membentuk dasar bagi integrasi

asuransi dalam strategi keamanan perusahaan. Meskipun demikian, tantangan dalam mengadopsi produk asuransi siber tetap ada, seperti yang diungkapkan oleh Bandyopadhyay et al. (2009) mereka menyoroti keengganan manajer IT untuk mengadopsi produk asuransi siber.

Dekade 2010-an: Pertumbuhan Kesadaran terhadap Risiko Siber

Pada era ini, serangkaian serangan besar seperti Sony's PlayStation Network and Sony Pictures Suffers Multiple Attacks, WannaCry, NotPetya, dan Equifax breach serta pencurian data pribadi pengguna Yahoo! menarik perhatian pada isu keamanan siber. Serangan-serangan ini menjadi poin sentral dalam pembahasan tentang keamanan siber. Dampaknya mendorong pengembangan strategi dan kebijakan baru terkait asuransi siber.

Dalam 35 publikasi yang dirilis selama dekade tersebut, beberapa tema utama mencuat, menunjukkan tren dan fokus diskusi pada masa itu. Beberapa penelitian memusatkan perhatian pada pemodelan dan penetapan harga asuransi siber, menggunakan metode matematis dan ekonometrika. Xu & Hua (2019) serta Fahrenwaldt et al. (2018) membahas cara mengelola risiko siber melalui model-model terukur. Selain itu, penggunaan teori permainan semakin mendominasi pembahasan, terutama dalam merancang asuransi kolektif dan manajemen risiko siber perusahaan. Inisiatif ini tercermin dalam publikasi yang diungkapkan oleh Zhang et al. (2017) dan Vakili & Sengupta (2019).

Tantangan dan strategi dalam asuransi siber juga menjadi fokus, dengan penelitian yang mencerminkan upaya untuk mengatasi kendala seperti terminologi yang membingungkan dan strategi analisis risiko. Teknologi juga memainkan peran kunci, terutama dalam sektor transportasi dan adopsi kendaraan listrik, sebagaimana yang diungkapkan oleh Tonn et al. (2019) dan Niyato et al. (2017). Dari segi ekonomi, beberapa publikasi mengeksplorasi aspek keuangan asuransi siber, termasuk dampaknya terhadap kesejahteraan sosial. Kuru & Bayraktar (2017) serta Kshetri (2018) menunjukkan bahwa asuransi siber tidak hanya berfungsi sebagai perlindungan, tetapi juga menjadi bagian integral dari keberlanjutan ekonomi dan sosial.

Dekade 2020-an: Pengembangan Model dan Desain Asuransi yang Komprehensif

Dekade 2020an mencerminkan dinamika yang kompleks dan perubahan dalam riset asuransi siber, dengan pandemi Covid-19 pada tahun 2020 menjadi pemicu utama yang memengaruhi arah dan fokus riset. Meskipun pandemi tersebut tidak secara eksplisit tercakup dalam judul-judul publikasi yang dianalisis, dampaknya menciptakan lanskap keamanan siber yang berubah secara drastis. Dalam 34 publikasi yang dirilis, pembahasan mengenai pengembangan model matematis diungkapkan Zeller & Scherer (2022) dan

Bessy-Roland et al. (2021) mencerminkan upaya untuk mengantisipasi dan mengelola risiko tambahan yang muncul selama masa ketidakpastian global.

Analisis dampak peristiwa siber dan klaim oleh Farkas et al. (2021) dan Palsson et al. (2020) menyoroti kebutuhan akan pemahaman yang mendalam tentang risiko siber yang diperparah oleh perubahan dalam pola serangan dan kerentanan sistem selama masa pandemi. Sementara itu, pandemi juga memunculkan aspek baru seperti peningkatan risiko siber di sektor kesehatan dan peningkatan ketergantungan pada teknologi dalam skenario kerja jarak jauh (online). Leong & Chen (2020) dan Samhan (2020) menunjukkan bagaimana risiko siber semakin meresapi sektor kesehatan, menandai pentingnya pendekatan asuransi siber dalam menghadapi tantangan khusus di bidang ini. Sementara itu menurut Yang et al. (2020), peningkatan risiko siber di sektor ini menggambarkan urgensi untuk mengintegrasikan asuransi siber dengan perkembangan teknologi dalam infrastruktur kesehatan.

SIMPULAN

Berdasarkan hasil analisis dan pembahasan, dapat disimpulkan bahwa perkembangan dan pertumbuhan dalam bidang publikasi asuransi siber pada rentang waktu 2002-2023, yang terindeks oleh Scopus mencapai puncak tertinggi pada tahun 2023 dengan jumlah publikasi sebanyak 25 (19,2%). Ini mencerminkan peningkatan signifikan perhatian terhadap isu-isu keamanan siber. *Jurnal Geneva Papers on Risk and Insurance Issues and Practice* memainkan peran sentral sebagai penyumbang publikasi internasional terbanyak dalam asuransi siber, menyumbang sebanyak 23,5% dari total publikasi. Sementara itu, Nanyang Technological University – Singapura, sebagai lembaga paling produktif, mencatatkan 15,8% dari total publikasi, menegaskan peran kunci perguruan tinggi sebagai penyokong utama dalam pengembangan literatur asuransi siber. Penulis paling produktif, seperti Niyato, D., Zhang, Wang, L., dan Wei, W., bersama-sama berkontribusi sebanyak 10,6% dari total publikasi. Subjek penelitian utama terletak dalam kategori *Computer Science, Economics, Econometrics and Finance*, mencapai 32,1% dari total penelitian, menunjukkan adanya kolaborasi lintas disiplin yang substansial dalam pemahaman dan penanganan tantangan asuransi siber.

Dengan mempertimbangkan pertumbuhan teknologi yang pesat, penelitian selanjutnya dapat difokuskan pada pengembangan model asuransi yang lebih spesifik dan adaptif terhadap tren teknologi terkini. Mengingat kontribusi yang signifikan dari subjek *Computer Science*, penelitian dapat mengeksplorasi cara menggabungkan kecerdasan buatan dalam pemodelan dan pengelolaan risiko siber. Ini mencakup

pengembangan algoritma prediktif untuk mendeteksi ancaman potensial dan strategi keamanan siber yang lebih responsif. Dalam melihat potensi penelitian mendatang, penelitian lebih mendalam terhadap kluster instrumentasi menjadi sangat relevan. Fokus penelitian dapat ditempatkan pada pemahaman elemen-elemen spesifik di setiap kluster, dengan tujuan mengembangkan instrumen dan metode baru untuk meningkatkan efektivitas perlindungan asuransi siber.

DAFTAR PUSTAKA

- 10 Biggest Cyber Attacks in History | Clear Insurance. (n.d.). Tersedia melalui:<
<https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/>> [Diakses 28
November 2023]
- Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C., 2009a. Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, 52(11), 68–73.
:<<https://doi.org/10.1145/1592761.1592780>>
- Bessy-Roland, Y., Boumezoued, A., & Hillairet, C., 2021. Multivariate Hawkes process for cyber insurance. *Annals of Actuarial Science*, 15(1), 14–39.
:<<https://doi.org/10.1017/S1748499520000093>>
- Calderón, A., & Ruiz, M., 2015. A systematic literature review on serious games evaluation: An application to software project management. *Computers & Education*, 87, 396–422. :<<https://doi.org/10.1016/j.compedu.2015.07.011>>
- Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F., 2011. Science mapping software tools: Review, analysis, and cooperative study among tools. *Journal of the American Society for Information Science and Technology*, 62(7), 1382–1402.
:<<https://doi.org/10.1002/asi.21525>>
- Effendy, F., Gaffar, V., Hurriyati, R., & Hendrayati, H., 2021. Analisis Bibliometrik Perkembangan Penelitian Penggunaan Pembayaran Seluler Dengan Vosviewer. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, 16(1), 10–17. :<<https://doi.org/10.35969/interkom.v16i1.92>>
- Fahrenwaldt, M. A., Weber, S., & Weske, K., 2018. PRICING OF CYBER INSURANCE CONTRACTS IN A NETWORK MODEL. *ASTIN Bulletin*, 48(3), 1175–1218.
:<<https://doi.org/10.1017/asb.2018.23>>
- Farkas, S., Lopez, O., & Thomas, M., 2021. Cyber claim analysis using Generalized Pareto regression trees with applications to insurance. *Insurance: Mathematics and Economics*, 98, 92–105. :<<https://doi.org/10.1016/j.insmatheco.2021.02.009>>

- Franke, U., 2017. The cyber insurance market in Sweden. *Computers & Security*, 68, 130–144. :<<https://doi.org/10.1016/j.cose.2017.04.010>>
- Gani, A. G., 2018. CYBERCRIME (KEJAHATAN BERBASIS KOMPUTER). *Jurnal Sistem Informasi Universitas Suryadarma*, 5(1). :<<https://doi.org/10.35968/jsi.v5i1.18>>
- Gordon, L. A., Loeb, M. P., & Sohail, T., 2003a. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3), 81–85. :<<https://doi.org/10.1145/636772.636774>>
- Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A., 2022. PRISMA2020: An R package and Shiny app for producing PRISMA 2020 - compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell Systematic Reviews*, 18(2). :<<https://doi.org/10.1002/cl2.1230>>
- Kshetri, N., 2018. The Economics of Cyber-Insurance. *IT Professional*, 20(6), 9–14. :<<https://doi.org/10.1109/MITP.2018.2874210>>
- Kumar, N., & Chaudhary, P., 2014. Minimize Cyber Losses in Cyber World through the Optimization Technique. *International Journal of Computer Applications*, 96(20), 18–22. :<<https://doi.org/10.5120/16910-6993>>
- Kuru, D., & Bayraktar, S., 2017. The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime*, 24(2), 329–346. :<<https://doi.org/10.1108/JFC-05-2016-0035>>
- Leong, Y.-Y., & Chen, Y.-C., 2020. Cyber risk cost and management in IoT devices-linked health insurance. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 45(4), 737–759. :<<https://doi.org/10.1057/s41288-020-00169-4>>
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A., 2017. Cyber-insurance survey. *Computer Science Review*, 24, 35–61. :<<https://doi.org/10.1016/j.cosrev.2017.01.001>>
- Niyato, D., Hoang, D. T., Wang, P., & Han, Z., 2017. Cyber Insurance for Plug-In Electric Vehicle Charging in Vehicle-to-Grid Systems. *IEEE Network*, 31(2), 38–46. :<<https://doi.org/10.1109/MNET.2017.1600321NM>>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D., 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, n71. :<<https://doi.org/10.1136/bmj.n71>>
- Palsson, K., Gudmundsson, S., & Shetty, S., 2020. Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 45(4), 564–579. :<<https://doi.org/10.1057/s41288-020-00171-w>>

- Peters, G., Shevchenko, P. V., & Cohen, R., 2018. Understanding Cyber-Risk and Cyber-Insurance. SSRN Electronic Journal. :<<https://doi.org/10.2139/ssrn.3200166>>
- Ravi R, & Vineet K., 2023. Cyber Insurance Market Research, 2032.
- Roemer, & Borchardt Rachel., 2015. Meaningful METRICS: A 21st-Century Librarian's Guide to Bibliometrics, Altmetrics, and Research Impact. Association of College & Research Libraries.
- 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). :<<https://doi.org/10.1093/cybsec/tyz002>>
- Samhan, B., 2020. Can cyber risk management insurance mitigate healthcare providers' intentions to resist electronic medical records? *International Journal of Healthcare Management*, 13(1), 12–21. :<<https://doi.org/10.1080/20479700.2017.1412558>>
- Saputro, W. A., Kusriani, K., & Luthfi, E. T., 2021. Tinjauan Literatur Sistematis Chatbot Untuk Pelayanan Pelanggan. *Jurnal Informa: Jurnal Penelitian Dan Pengabdian Masyarakat*, 7(1), 15–20. :<<https://doi.org/10.46808/informa.v7i1.194>>
- Shackelford, S. J., 2012. Should your firm invest in cyber risk insurance? *Business Horizons*, 55(4), 349–356. :<<https://doi.org/10.1016/j.bushor.2012.02.004>>
- Shukla, R., 2019. Indian research output on genetic disorder publication using the Scopus database: A scientometric study. *COLLNET Journal of Scientometrics and Information Management*, 13(1), 91–102. :<<https://doi.org/10.1080/09737766.2018.1550044>>
- Siegel, C. A., Sagalow, T. R., & Serritella, P., 2002. Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Systems Security*, 11(4), 33–49. :<<https://doi.org/10.1201/1086/43322.11.4.20020901/38843.5>>
- Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J., 2019. Cyber risk and insurance for transportation infrastructure. *Transport Policy*, 79, 103–114. :<<https://doi.org/10.1016/j.tranpol.2019.04.019>>
- Vakilinia, I., & Sengupta, S., 2019. A Coalitional Cyber-Insurance Framework for a Common Platform. *IEEE Transactions on Information Forensics and Security*, 14(6), 1526–1538. :<<https://doi.org/10.1109/TIFS.2018.2881694>>
- van Eck, N. J., & Waltman, L., 2010. Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, 84(2), 523–538. :<<https://doi.org/10.1007/s11192-009-0146-3>>

- Xu, M., & Hua, L., 2019. Cybersecurity Insurance: Modeling and Pricing. *North American Actuarial Journal*, 23(2), 220–249. :<<https://doi.org/10.1080/10920277.2019.1566076>>
- Yang, Z., Liu, Y., Campbell, M., Ten, C.-W., Rho, Y., Wang, L., & Wei, W., 2020. Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations. *IEEE Access*, 8, 78890–78900. :<<https://doi.org/10.1109/ACCESS.2020.2988548>>
- Young, D., Lopez, J., Rice, M., Ramsey, B., & McTasney, R., 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14, 43–57. :<<https://doi.org/10.1016/j.ijcip.2016.04.001>>
- Zeller, G., & Scherer, M., 2022. A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*, 12(1), 33–85. :<<https://doi.org/10.1007/s13385-021-00290-1>>
- Zhang, R., Zhu, Q., & Hayel, Y., 2017a. A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks. *IEEE Journal on Selected Areas in Communications*, 35(3), 779–794. :<<https://doi.org/10.1109/JSAC.2017.2672378>>
- Zheng, Y., Wei, D., Li, J., Zhu, T., & Ning, H., 2016. Internet Use and Its Impact on Individual Physical Health. *IEEE Access*, 4, 5135–5142. :<<https://doi.org/10.1109/ACCESS.2016.2602301>>