International Insurance Law Review
ISSN: 0968-2090
Vol 33 S4 (2025): Special Issue
https://lumarpub.com/iilr

Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks

Ellias Aghili Dehnavi*[1], Radosław Fiedler[2]
[1]*Ph.D. Candidate, Political Science and Public administration, Faculty of Political Science and Journalism, Adam Mickiewicz University, Poznan, Poland
[2]Professor Of International Relations, Director of the Doctoral School of Social Sciences, Head of the Non-European Studies Department, Faculty of Political Science and Journalism, Adam Mickiewicz University, Poznan, Poland
Email: [1]*ellagh@amu.edu.pl, [2]fiedler@amu.edu.pl
ORCID: [1]*0009-0001-9238-056X, [2]0000-0003-1573-9898
*Corresponding Author: Ellias Aghili Dehnavi

Abstract
This paper examines the impact of British think tanks, with Chatham House and RUSI as the focal points, on the formation of cyber insurance policies. The research methodology is based on qualitative content analysis of policy documents (2018-2023) and semi-structured interviews with five experts. The results show how the differences in the conceptual frameworks of these think tanks have led to the formation of two distinct approaches. Chatham House focuses on economic risks and market-based solutions such as contractual transparency and financial incentives, while RUSI focuses on national security dimensions and government intervention such as state guarantee funds and mandatory standards. The findings suggest that these differences are due to different communication networks and distinct policy priorities. The interaction of these two approaches in a complementary manner can help develop a balanced ecosystem of cyber insurance regulations.
Keywords: Cyber insurance, digital governance, British think tanks, Chatham House, RUSI, legal framing, emerging risks, policy discourse analysis.

1. Introduction

In the digital age, the spread of new technologies and rapid developments in the cyber domain have created extensive challenges for governments, financial institutions, and various businesses. Meanwhile, cyber insurance, as a complementary mechanism alongside traditional security solutions, is becoming an essential tool for organizations in the face of increasing cyber threats (Tsohou et al., 2023). However, the complexity and dynamism of cyber threats, as well as the lack of comprehensive legal frameworks, have made it more and more evident that there is a need to redefine the role of policy-making institutions and think tanks in this area (Eling, 2024).

As a pioneer in the field of creating cyber insurance, the United Kingdom faces issues such as precisely defining coverable risks, determining legal responsibilities, and establishing effective regulatory mechanisms (Kshetri, 2020). Meanwhile, think tanks, as intermediaries between academia, industry, and government, can play a pivotal role in the legal framing of emerging digital risks. Content analysis of documents and reports published by these think tanks shows that the way they define and classify cyber threats has a direct impact on the prioritization of

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.

issues on the agenda of legislators. However, the mechanisms of this influence and how research findings are translated into operational policies have not yet been comprehensively examined. On the other hand, the diversity of perspectives and approaches among think tanks active in this field has itself led to the creation of new challenges in the legislative process. Some of these think tanks propose technology-based solutions, emphasizing the technical aspects of cyber threats, while others emphasize the need to strengthen the legal aspects and responsibilities of regulatory institutions.

The aim of this study is to systematically examine the role of UK think tanks in shaping the legal frameworks for cyber insurance and to provide a better understanding of the policy-making processes in this area. The main focus will therefore be on analysing the discourses that govern the reports and policy proposals of these think tanks, in order to identify how the concepts and definitions they provide influence the development of cyber insurance regulations. This study also seeks to explain the complex interactions between different actors in this field, including government, insurance companies, businesses, and research institutions, all of which play a role in ultimately shaping the legal framework for emerging digital risks.

2. Literature review

So far, limited studies have been conducted in this field, and this section introduces and describes some of the most important ones.

Joshi et al., (2019) examined the challenges in understanding and analyzing cyber insurance contracts. This study, citing the linguistic and legal complexities present in insurance documents, proposed a solution based on artificial intelligence technologies. In this regard, a framework was designed that is able to automatically extract key concepts, inclusions, and exclusions present in insurance policies and organize them in the form of a knowledge graph. Validation of the system using Federal Trade Commission standards and testing on the policies of seven insurance companies shows that this approach can help organizations analyze contracts more accurately and make informed decisions. This study is important because it takes an effective step towards clarifying and standardizing the risk assessment process in cyber insurance, and creates a bridge between the practical needs of businesses and the legal complexities of this area. Khalili et al., (2019) also analyzed practical solutions for managing cyber risk interdependencies between service providers and their customers. The findings suggest that by cleverly designing contracts—including incentives such as premium discounts for security investments—insurers can simultaneously increase their profitability and reduce systemic risks. In fact, this study, using real data, has provided a model of how insurance policies and appropriate frameworks in this area can become an effective tool for promoting cybersecurity at the ecosystem level. In addition, Romanosky et al., (2017) analyzed industry practices in risk assessment and premium determination by examining examples of cyber insurance contracts. The results of this study show that insurance companies use criteria such as organization size, security record, and the presence of protection systems to calculate premiums. However, there is a significant gap between theoretical discussions and practical practices in pricing cyber risks. This study also shows the extent to which the scope of insurance coverage and exclusions included in contracts are affected by various factors. These findings are important for policymakers and regulators in the field of cyber insurance.

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.

Woods & Simpson (2017) examine mechanisms for government-insurer collaboration to improve cybersecurity. Using qualitative analysis of policy reports and interviews with industry stakeholders, they provide a framework that explains how these two institutions interact in a public-private partnership. By identifying potential government interventions that could impact the cybersecurity insurance market, the study provides practical solutions for aligning private sector interests with public policy objectives. This framework not only highlights the role of the insurance industry in improving security standards, but also serves as a guide for policymakers in designing effective interventions. The results of this research can help to better understand the complex interactions between regulators and insurance market players in the face of emerging cyber challenges. Also, Markopoulou (2021) has examined the challenges of developing a cyber insurance market in the European Union, taking into account the experiences of the American market. Despite 15 years of efforts by the European Union to establish legal frameworks to protect information systems, the growth of the cyber insurance market has faced several obstacles, including the dynamic nature of cyber threats, the lack of a common language in defining risks and losses, and the lack of historical data. Therefore, by comparing these challenges with the longer experience of the US market, this study offers potential solutions to accelerate the development of the European market. The findings of this research can help European policymakers design effective interventions to create a more competitive and efficient cyber insurance market. Additionally, Sullivan & Nurse (2021) analyzed the impact of cyber insurance on improving security practices. The findings show that despite the potential for insurers to transfer security knowledge, challenges such as inappropriate pricing, ambiguity in contract coverage, and lack of awareness among organizations have hindered market growth. Also, by examining risk management policies, this study emphasizes the need to design incentive mechanisms in contracts and develop effective regulatory frameworks. These findings are important for developing cyber governance strategies, especially in the field of insurance regulation. In addition, Lubin (2020) examines the place of cyber insurance as a new tool in cyber diplomacy. By analyzing the Israeli initiative to establish a "Cyber Insurance Regulatory Pilot Site," the author shows how insurance norms can be transformed from a technical-legal domain into a strategic arena in international relations. This study argues that the development of international standards on cyber insurance – with the participation of public and private actors – can help to stabilize cyberspace and strengthen deterrence. This perspective presents cyber insurance not only as a compensation mechanism, but also as a tool for shaping global norms and facilitating transnational cooperation. Such an analysis is important for understanding the role of think tanks in developing legal frameworks for cyber insurance and their impact on public policymaking.

In general, a review of previous studies shows that although numerous studies have examined various aspects of cyber insurance, including contractual challenges, pricing models, public-private partnerships, and international dimensions, the role of intellectual institutions in shaping the legal frameworks of this field has received less attention. Previous studies have mainly focused on technical, economic, or macro-policy aspects, while the processes of discourse formation and directing the attention of regulators through institutions such as think tanks have not been examined in a targeted and comprehensive manner. This study, focusing on UK think tanks, seeks to fill this research gap. It analyses how these institutions define and frame cyber

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.

threats and their impact on legal orientations in the field of cyber insurance. The importance of this study is that it reveals indirect mechanisms of influence on policy-making and shows how discourse around cyber risks can lead to legal and regulatory change.

3. Research Method

This study, adopting a qualitative and interpretive approach, examines the role of UK think tanks in shaping legal frameworks for cyber insurance. Focusing on two influential think tanks, Chatham House and RUSI, the research uses a mixed methodology that includes qualitative content analysis of policy documents and semi-structured interviews with key stakeholders.

In the first step, a collection of policy reports, regulatory proposals, and public statements published by these two think tanks between 2018 and 2023 is examined. These documents are selected through purposive sampling and analyzed using thematic coding. The content analysis approach helps identify recurring patterns, conceptual frameworks, and how cyber threats are presented in the discourse of these institutions.

In the second step, interviews will be conducted with five experts and active policymakers to complete the data required for the analysis. Participants will include senior analysts from these think tanks, representatives from financial regulators, and experts from the insurance industry. The interviews will be conducted using a semi-structured interview guide and will focus on understanding the processes behind the scenes of influencing policymaking. To increase the validity of the findings, data triangulation, i.e. combining documentary sources and interviews, and peer review, will be used.

In order to analyze the data, the critical discourse analysis method is used to examine power relations and legitimization mechanisms in policy discourses. Also, mapping the actor network helps to better understand the interactions between think tanks, government institutions, and the private sector.

4. Findings and Discussion

Thematic codes identified from the content analysis of policy documents are shown in Table (1).

Table (1): Thematic codes identified from the content analysis of policy documents

Main criteria	**Sub-criteria**	**Related concepts**	**Frequency in Chatham House reports**	**Frequency in RUSI reports**
Definition of cyber risk	Financial risks	Direct financial losses, data recovery costs	23	9
	Operational Risks	Supply chain disruption	17	12

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.

Main criteria	Sub-criteria	Related concepts	Frequency in Chatham House reports	Frequency in RUSI reports
	National Security Risks	Nation-state attacks, infrastructure threats	5	28
Regulatory frameworks	Mandatory Standards	Minimum security requirements, certificates	14	7
	Financial incentives	Insurance discounts, tax exemptions	19	4
	International cooperation	Harmonization of rules, information sharing	8	15
Policy suggestions	Contractual transparency	Standardization of legal language, disclosure of terms	27	3
	Responsibility sharing	Industry and government contributions, limits of accountability	11	18
	Compensation mechanisms	Mutual funds, government insurance	6	13

As can be seen, the two think tanks, despite addressing the common topic of cyber insurance, have approached the issue from quite different perspectives. Chatham House has a significant emphasis and focus on the financial and operational aspects of cyber risks. Furthermore, it strongly pursues market-based solutions such as financial incentives and contractual transparency, while RUSI has a macro- and security-oriented approach, with a strong emphasis on national security risks and international cooperation. There are also marked differences in the policy proposals of the two think tanks. Chatham House pursues private sector solutions, while RUSI systematically emphasizes government intervention and government compensation mechanisms. These differences reflect two distinct paradigms in addressing the challenges of

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.

cyber insurance in different UK think tanks, some economic-market-oriented and some security-state-oriented.

4. 1. The role of Chatham House in the legal framing of digital risks

An analysis of the content of Chatham House documents and reports shows that this think tank has influenced the formation of cyber insurance regulations in three main ways:

The first path is to define insurable risks. In fact, this think tank, focusing on the economic aspects of cyber threats, has provided operational definitions of digital risks, which have become the basis for developing industry standards. For example, we can mention the classification of financial losses into two categories: direct (compensation to customers) and indirect (business interruption costs), which has been one of the policies of this think tank and is reflected in the draft "Cyber Contract Transparency Guidelines" (FCA 2022). Another example of how Chatham House has influenced the definition of insurable risks is the risk assessment criteria based on quantitative indicators such as the volume of data processed and the duration of system recovery, which have been accepted by the Association of British Insurers (ABI) as the basis for determining insurance premiums.

The second path is to design and provide market-based mechanisms. In this regard, the Chatham House think tank, with an emphasis on self-regulation, has made specific proposals to reduce the need for heavy government intervention. One of these proposals is a security rating system, under which companies receive premium discounts in exchange for meeting certain standards. The initiative was piloted by three major insurers in 2021. The think tank also proposes a standard contract model that aims to mitigate emerging digital risks and issues. The prototype was developed in collaboration with Lloyd's Market Association.

The third path is to facilitate stakeholder dialogue. In this regard, Chatham House has provided a platform for direct interaction between key players by creating specialized platforms. The establishment of the Joint Industry-Government Committee, whose annual report formed the basis for amending Article 5 of the Financial Services Act (2012) in the cyber insurance sector, has been one of the most important steps taken by the think tank to influence the legal framework for digital risks and the management of cyber insurance. In addition, the think tank has held quarterly roundtables with representatives from technology companies, insurers, and consumer organizations, the output of which has been published as a "Guide to Managing Digital Supply Chain Risks."

Chatham House has also played a key role in crises. For example, its response to the 2020 ransomware attacks demonstrates its catalytic role. The rapid publication of the 'Joint Response Framework' shortly after the crisis led to insurers voluntarily agreeing to suspend the 'war attacks' clause in 68% of their policies, as well as the creation of a £250m contingency reserve. These impacts have occurred mainly through indirect mechanisms, including producing expert knowledge in a language understandable to policymakers, translating research findings into specific actionable recommendations, and building consensus among stakeholder groups with conflicting interests.

Analysis of the interaction network shows that the think tank has influenced the legislative process not necessarily through direct lobbying but through intermediary institutions such as

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.

industry associations and parliamentary committees. This has led to a higher level of acceptance of the think tank's proposals in the long run.

4. 2. The role of the RUS think tank in the legal framing of digital risks

Analysis of documents and reports from the Royal United Services Strategic Studies Institute (RUSI) shows that this think tank, focusing on the national security and strategic dimensions of cyber threats, has played three key roles in shaping UK cyber insurance regulations, which are described separately below.

The first role can be seen as defining cyber threats with a national security focus. In this regard, RUSI has provided a different conceptual framework than Chatham House, emphasizing the risks arising from nation-state attacks and infrastructure threats. The classification of politically motivated cyber attacks, such as sabotage of critical infrastructure, as "traditionally uninsurable" risks led to the passage of the Cybersecurity Amendment 2021 to the UK National Defence Act. Furthermore, the think tank's emphasis on the shared responsibility of government and the private sector in protecting critical infrastructure was reflected in the "National Cybersecurity Strategy 2022".

The second role of RUSI in the legal framework of digital risks can be seen as designing interventionist government mechanisms. In contrast to the market-oriented approach of Chatham House, RUSI supports stronger regulatory models. For example, the think tank's proposal to create a state guarantee fund to cover losses from sophisticated cyberattacks, which was piloted for the energy sector in 2023, can be cited. In addition, the development of mandatory security standards for critical industries in accordance with the EU NIS Directive framework and its linkage to the terms of insurance contracts can be considered another important role of the think tank.

The third role is to make cybersecurity a strategic issue. In this regard, RUSI has developed the cyber insurance discourse from the economic to the security sphere, by directly engaging with security institutions such as GCHQ and the Ministry of Defence.

4. 3. Comparative Comparison of Chatham House and RUSI Think Tanks' Approaches to Cyber Insurance Governance

Chatham House analyzes cyber threats primarily from an economic, business-centric perspective. The think tank's reports focus on concepts such as "direct financial losses" and "data recovery costs." In contrast, RUSI takes a strategic view, focusing on national and security vulnerabilities. For example, its 2022 report on the digital supply chain focused primarily on threats posed by state actors and their security implications.

Chatham House, taking a market-oriented approach, proposes solutions such as a corporate security rating system and a model of standard contracts. These proposals are mainly based on voluntary mechanisms and financial incentives. On the other hand, RUSI, emphasizing the active role of the government, supports interventionist mechanisms such as a state guarantee fund and mandatory security standards.

Chatham House mainly influences private sector financial institutions and regulators, such as the Association of British Insurers. In contrast, RUSI has strong links with security and defence

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.

institutions, such as the Ministry of Defence and GCHQ. This difference in communication network is clearly visible in the type of proposals it makes and how they are implemented.

As a concrete example of the different influence of these two think tanks, we can mention that the Chatham House think tank's proposal on contractual transparency led to the development of the "Transparency Directive" by the Financial Conduct Authority, which focused more on consumer rights. While RUSI's influence was evident in the Department of Defense's new requirements for military contractors, which included stricter requirements for cyber insurance coverage, the two think tanks also have distinct and different approaches to responding to crises. For example, in the face of the 2020 ransomware crisis, Chatham House emphasized facilitating private sector collaboration and creating an emergency reserve fund. While RUSI, taking a broader view, argued for government intervention and sharing financial responsibility between the public and private sectors.

This comparison shows how two leading British think tanks, despite addressing a common subject, use distinct conceptual frameworks, networks of influence, and policy approaches. Chatham House takes an economic and market-oriented view, seeking to balance the interests of private actors, while RUSI sees cybersecurity as an integral part of national security and advocates a more active role for government. These fundamental differences, while sometimes leading to conflicting proposals, ultimately complement each other and help to create a balanced cyber insurance policy.

5. Conclusion

This study, by comparing the role of two leading British think tanks in shaping the legal frameworks for cyber insurance, reveals different patterns of influence. The findings show that Chatham House, with its focus on economic dimensions and a market-oriented approach, has contributed to the formation of regulations centered on contractual transparency and consumer rights through the provision of industry standards and self-regulatory mechanisms. In contrast, RUSI, with its emphasis on national and strategic security considerations, has paved the way for government interventions and strict requirements for critical industries. This study shows that the differences in the missions, communication networks, and analytical frameworks of these two institutions have led to the emergence of two complementary streams of cyber insurance policymaking. While Chatham House emphasizes market efficiency and commercial resilience, RUSI focuses on national security and infrastructure resilience. This dynamic interaction between economic and security approaches offers a unique model of multi-stakeholder governance in the area of emerging digital risks.

Based on the results, it is suggested that a mechanism combining market-based and security-based approaches be designed to develop cyber insurance governance frameworks in the face of emerging digital risks. This mechanism can be operationalized by forming a "joint policy council" consisting of representatives of think tanks, financial regulators, security authorities, and insurance industry activists. In this framework, mechanisms proposed by Chatham House, such as "corporate security ratings" and "standard contract models," can be used as private sector incentive tools.

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.

References

Eling, M. (2024). Cyber Risk and Cyber Insurance. In *Handbook of Insurance: Volume I* (pp. 199-224). Cham: Springer Nature Switzerland.

Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications policy*, *44*(8), 102007.

Joshi, K., Joshi, K. P., & Mittal, S. (2019, July). A semantic approach for automating knowledge in policies of cyber insurance services. In *2019 IEEE international conference on web services (ICWS)* (pp. 33-40). IEEE.

Khalili, M. M., Liu, M., & Romanosky, S. (2019). Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity*, *5*(1), tyz010.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk? *Available at SSRN 2929137*.

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, *22*(3), 737-748.

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*, *2*(2), 209-226.

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

Sullivan, J., & Nurse, J. R. (2021). Cyber security incentives and the role of cyber insurance. *RUSI Emerging Insights Paper*.

Lubin, A. (2020). Cyber Insurance as Cyber Diplomacy. *Asaf Lubin, Cyber Insurance as Cyber Diplomacy, Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization*, 22-37.

Received: 04 August 2025 | Accepted: 20 August 2025 | Published: 27 August 2025

Citation: Dehnavi, E. A & Fiedler, R (2025). Cyber Insurance Governance: UK Think Tanks and the Legal Framing of Emerging Digital Risks. *International Insurance Law Review*, 33 (S4), 105-113.