Business Research Proceedings

ISSN: 2993-0049 (Online)
Volume 0, Issue 0 | 10.51300/BRP-2026-1

LUMINOUS INSIGHTS

Extended Abstract | Proceedings of the 1st International Conference on Sustainable Economies and Inclusive Growth

Modeling the Diffusion of Interstate Cyber Conflict through Dyadic Spatial Relations

Eduardo Delso Muñoz [1], **Gema Fernández-Avilés** [1], **and María Cristina Sánchez Figueroa** [2]

[1]Universidad de Castilla-La Mancha, Spain
[2]Universidad Nacional de Educación a Distancia, Spain

KEYWORDS

Spatial Weight Matrix, Spatial Diffusion, Dyadic Framework, Cyber Conflict, Network Analysis

ARTICLE HISTORY
Published: 7 July 2026

Interstate cyber conflict exhibits diffusion dynamics that do not conform to traditional spatial assumptions based on geographic contiguity. Instead, it unfolds through relational structures shaped by political and economic interdependencies. However, the literature lacks a dyadic spatial framework capable of systematically modeling these diffusion processes, which is particularly significant given the growing frequency and geopolitical relevance of state-sponsored cyberattacks.

This study develops a dyadic spatial approach to analyze the propagation of cyber conflict, introducing two specific mechanisms: (i) target contagion, which captures correlation in victimization across states with similar attributes, and (ii) source contagion, which models the diffusion of offensive behavior among states sharing strategic alignments or common interests. These two mechanisms reflect distinct logics of conflict propagation and are treated as complementary rather than mutually exclusive perspectives on how cyber conflict spreads.

Both mechanisms are operationalized through spatial weight matrices constructed from measures of relational similarity. Specifically, we employ (a) political affinity, proxied by voting patterns in the United Nations General Assembly, and (b) economic interdependence, measured through bilateral trade in services. The political affinity matrix is constructed by computing weighted agreement rates across United Nations General Assembly resolutions for each country pair over a rolling ten-year window, yielding a symmetric measure of diplomatic alignment. The trade-based matrix is built from the Organisation for Economic Cooperation and Development Balanced Trade in Services dataset and captures the relative importance of bilateral service flows for each reporting country. Both matrices are subsequently transformed into negative exponential form to satisfy the convergence conditions required for consistent estimation, and a time-invariant version is derived by averaging across the years covered by the cyber incidents data. Multiple matrix normalization schemes are considered, and their structural properties (density, clustering, and connectivity) are assessed to ensure robustness.

CORRESPONDING AUTHOR

Eduardo Delso Muñoz · eduardo.delso1@alu.uclm.es · Universidad de Castilla-La Mancha, Spain

The empirical application relies on cyber incident data from the European Repository of Cyber Incidents dataset, covering state-attributed incidents with a political dimension or against critical infrastructure. The study sample is restricted to countries with sustained involvement in cyber conflict, defined as a minimum combined threshold of launched and received attacks over the study period, in order to ensure analytical tractability. This yields 4,422 directed country pairs and a panel of over 57,000 observations over the period 2011–2023. A descriptive analysis is conducted and complemented with network-based visualizations to identify diffusion patterns and centrality structures.

The descriptive results reveal a highly skewed distribution of cyber activity, with a small number of states consistently acting as dominant attackers or recurring victims, a pattern consistent with the strategic and geopolitical drivers of state-sponsored cyber operations. The analysis also uncovers heterogeneity in diffusion patterns depending on the contagion mechanism and similarity metric employed, as well as the presence of clusters of states with high centrality in the spread of cyber conflict.

From a theoretical standpoint, the study contributes to the literature by integrating a dyadic spatial framework that is consistent with the relational nature of cyberspace, moving beyond geographic contiguity as the base principle of spatial dependence. From a policy perspective, the identification of structural patterns and high-centrality states in the contagion networks has direct implications for the design of cyber defense strategies and international cooperation frameworks, as these states represent priority candidates for early warning systems and coordinated diplomatic or defensive responses. The study also suggests avenues for future research, including the incorporation of alternative relational similarity measures and alternative matrix specifications.

Funding Statement

This work has been partially funded by the research group Applied Economics & Quantitative Methods (University of Castilla-La Mancha).

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

ORCID

Eduardo Delso Muñoz
| https://orcid.org/0009-0000-9591-3651
Gema Fernández-Avilés
| https://orcid.org/0000-0001-5934-1916
María Cristina Sánchez Figueroa
| https://orcid.org/0000-0002-4386-8825

Publisher Disclaimer

Cite as
Delso Muñoz, E., Fernández-Avilés, G., Sánchez Figueroa, M. C. (2026). Modeling the Diffusion of Interstate Cyber Conflict through Dyadic Spatial Relations. In *Proceedings of the 1st International Conference on Sustainable Economies and Inclusive Growth* (pp. 1–2). Business Research Proceedings. 10.51300/BRP-2026-1