Infering the Unknowns: A Network Analysis of Cyber Incidents

Gidi Brandes - s3477452

23-12-2025

The following documents with codes are available at my github page:

An R script with the raw code, excluding all tables in this paper: `network test.R`

The R Markdown File that is rendered to the document you're currently reading: `Final Assignment - BrandesGidi.Rmd`

Introduction

In an era where digital connectivity is part of nearly every aspect of human existence, cyberspace has emerged as a domain shaping both individual lives and state policies. From everyday communications and economic transactions to critical infrastructure management and national security strategies, cyber technologies have become indispensable. Governments worldwide increasingly recognize cyberspace as a strategic arena, investing in policies to harness its benefits while mitigating risks. For instance, the proliferation of cyber incidents, ranging from data breaches to state-sponsored operations, has prompted regulatory responses, such as the U.S. Cyber Incident Reporting for Critical Infrastructure Act of 2022, which mandates reporting to enhance visibility into threats (Shore, 2022). This centrality underscores the social relevance: cyber disruptions can affect millions, exacerbating inequalities in access and resilience, particularly between developed and developing nations (Choucri, 2012a). Scientifically, understanding cyberspace is crucial for informing evidence-based policy, as incomplete knowledge of cyber dynamics leads to suboptimal decisions, such as overstated threat predictions or inefficient resource allocation (Whyte, 2018; Foulon & Meibauer, 2024).

The importance of comprehending cyberspace extends beyond immediate threats to broader policy implications. Effective governance requires insights into how cyber activities influence international stability, economic development, and societal well-being. Without robust analysis, policies may fail to address vulnerabilities, leading to escalations in conflicts or hindrances to sustainable development. In international relations (IR) research, a notable trend has been the shift from conceptual debates on cyber as a revolutionary domain to

more integrated examinations of its sociopolitical contexts. Early scholarship critiqued the direct application of traditional IR theories, like deterrence or offense-defence balance, to cyberspace, arguing that such transfers often result in biased conclusions and flawed predictions (Whyte, 2018). Instead, recent works emphasize cyberspace as a "structural modifier" that alters state interactions within existing international structures, influencing areas like uncertainty, foreign policy tools, and non-state actor roles (Foulon & Meibauer, 2024).

Despite these advances, significant gaps persist, particularly in quantitative studies of cyber phenomena. Empirical research remains limited, often relying on incomplete datasets that underrepresent covert operations or non-state activities (Gorwa & Smeets, 2019; Shore, 2022). A key shortfall is the absence of relational or network-based approaches, which could reveal interconnected patterns in cyber incidents rather than treating them as isolated events (Menninga & Goldberg, 2022). Traditional quantitative methods struggle with data missingness, attribution challenges, and the assumption of independence among variables, failing to capture the systemic nature of cyberspace (Kostyuk & Zhukov, 2019; Barnum, 2022).

This paper addresses these gaps by exploring a methodological approach rather than resolving a specific empirical puzzle. It aims to investigate how a network-based analysis can provide deeper insights into the cyber system, particularly by interpreting structured unknowns in cyber datasets. By modelling cyber incidents as interconnected networks where actors, motives, regions, and targets form relational clusters, this method shifts focus from individual attributions to systemic patterns, aiming to enhance our understanding of cyberspace's complexities and informing more nuanced policy frameworks.

Literature Review and Theory

Cyber research within IR has been dominated by conceptual debates, which prioritize theoretical explorations of cyberspace's ontology over empirical validation. Scholars have critiqued the application of predigital IR paradigms, such as realism or constructivism, to digital contexts, arguing that cyberspace introduces unique elements like anonymity, rapid evolution, and blurred boundaries between peace and war (Whyte, 2018; Kosenkov, 2016; Foulon & Meibauer, 2024). For example, debates often revolve around whether cyber operations constitute a new domain of warfare or merely an extension of existing tools, with emphasis on sociopolitical contexts over technical determinism (Whyte, 2018). While these discussions have enriched IR theory, highlighting needs for adapted concepts like power, violence, and deterrence, they have largely sidelined quantitative empirical work, leaving gaps in testable models of cyber dynamics (Gorwa & Smeets, 2019).

Empirical quantitative research on cyber conflict does exist but is limited in scope and depth. Studies like Valeriano and Maness's analysis of dyadic cyber incidents between rival states (2001–2011) and Kostyuk and Zhukov's examination of cyber activities in Ukraine and Syria demonstrate that cyber operations are often low-intensity, tied to preexisting rivalries, and ineffective at altering battlefield outcomes (Gorwa & Smeets, 2019; Kostyuk & Zhukov, 2019). However, these efforts are constrained by data issues: most rely on publicly reported

incidents, which underrepresent covert actions, and face challenges in coding dyads due to multinational malware spread, attribution ambiguities, and unclear victim targeting (Gorwa & Smeets, 2019). Broader datasets from sources like the Council on Foreign Relations or the CyberPeace Institute provide snapshots but remain fragmented and proprietary, limiting generalizability (Shore, 2022). Consequently, quantitative IR cyber research struggles to move beyond descriptive statistics, failing to uncover underlying structures or predict escalations.

A core problem exacerbating these limitations is the pervasive missingness of data in cyber datasets. Unlike other conflict fields, where data gaps might stem from logistical issues, cyber missingness is qualitatively distinct, driven by political motivations, secrecy, and strategic opacity (Shore, 2022). Governments and private actors often withhold incident details to avoid reputational damage or reveal capabilities, creating "structured unknowns" where absences are not random but patterned by factors like attribution difficulties or non-state involvement (Gorwa & Smeets, 2019; Kosenkov, 2016). This epistemic opacity, limits on what can be known, undermines robust theory-building, as incomplete data leads to biased inferences and weak causal claims (Pratt, 2022; Barnum, 2022).

Faced with this opacity, researchers confront two paths: accept the unknowns as inherent, resulting in tentative or "weak" theories reliant on qualitative narratives, or seek to extract patterns from the structured uncertainty itself. This paper opts for the latter, arguing that epistemic challenges in cyber IR demand innovative methods to interpret rather than ignore missingness. Importantly, this project eschews attribution-focused approaches, which often falter due to unverifiable claims, in favour of gaining systemic insights into cyber patterns (Kosenkov, 2016; Foulon & Meibauer, 2024).

Machine learning (ML) techniques offer potential but fall short for cyber data's unique characteristics. For instance, Random Forest struggles with high-cardinality categorical variables common in cyber incidents (e.g., diverse actors or motives), leading to overfitting or poor generalization. Similarly, Naïve Bayes assumes feature independence, which is untenable in interconnected cyber environments where variables like regions and targets covary (Choucri, 2024). These limitations highlight the need for a new approach: network-based analysis.

To overcome the limitations of traditional machine learning and dyadic quantitative methods in cyber IR research, this paper proposes a network-based approach as a promising alternative. Network analysis, long established in social sciences and increasingly applied in international relations, treats phenomena as interconnected systems rather than collections of independent observations (Menninga & Goldberg, 2022). In the context of cyber incidents, this method models entities (e.g. actors, motives, regions, and targets), not as isolated variables but as nodes linked by relational ties, enabling the detection of emergent patterns that reflect deeper structural dynamics.

Cyber incidents exhibit clear clustering tendencies around key dimensions: perpetrators (state, non-state, or proxy actors), motives (espionage, disruption, coercion), geographic regions (origin or impact zones), and targets (critical infrastructure, government, private sector). These clusters are not random. Co-occurrences, such as repeated pairings of specific actors with particular motives or regional hotspots, signal underlying structures, including alliance networks, proxy relationships, or geopolitical fault lines (Gorwa & Smeets, 2019;

Choucri, 2024). By constructing bipartite or multipartite networks (e.g., linking actors to incidents, incidents to targets, or motives to regions), analysts can reveal how these elements interconnect, providing a more holistic view than attribute-focused methods.

Crucially, the pervasive missingness in cyber datasets is itself relational rather than independent or purely random. Absences often stem from interconnected factors: strategic secrecy by state actors, attribution challenges in multinational operations, or underreporting in certain regions due to capacity constraints (Shore, 2022; Barnum, 2022). In network terms, missing data manifests as absent ties or nodes that are structurally implied by surrounding connections (e.g., an unreported actor inferred from co-occurring motives and targets). This relational missingness aligns with systems thinking, which positions cyberspace as deeply embedded in broader global pressures (Choucri, 2024). Cyberspace does not operate in isolation; it intersects with social and natural domains, amplifying feedbacks and intersections that traditional isolated-incident analyses overlook.

Given this inherently networked environment, characterized by fluid interactions, non-state empowerment, and cross-border permeations, network-based methods are particularly appropriate (Foulon & Meibauer, 2024; Choucri, 2012b). Tools like centrality measures, community detection, and brokerage analysis can uncover influential nodes, clustered subgroups, and bridging connections, transforming raw incident data into interpretable structures (Menninga & Goldberg, 2022).

This represents a significant theoretical move: shifting from viewing cyber incidents as discrete, isolated events, often hampered by attribution failures, to recognizing them as manifestations of systemic patterns within a complex global ecosystem. Practically, the approach involves building comprehensive networks from available data to gain initial insights, such as identifying dominant actors or regional clusters. Community detection algorithms can then delineate subgroups, revealing hidden alliances or rivalry structures. Finally, by applying these network-derived insights to the unknowns (e.g., imputing missing ties based on structural equivalence, simulating absent nodes via community affiliations, or assessing the robustness of patterns under varying missingness scenarios), the method allows researchers to make meaningful statements about structured absences, such as inferring likely motives in unreported incidents or highlighting systemic vulnerabilities driven by opacity.

Thus, the central research question is: **How can network analysis help interpret structured unknowns in cyber incidents?**

Research Design

The research design for this exploratory study centres on constructing and analysing a network from cyber incident data to interpret structured unknowns, aligning with the network-based approach outlined earlier. Given the proof-of-concept nature of this work, the design emphasizes simplicity, reproducibility, and a focus on relational patterns rather than causal inference or predictive modelling. It proceeds in four main steps: dataset selection, data preparation, network construction, and measurement of network properties. This is fol-

lowed by an inference procedure to address undetermined values, leveraging the network's structure.

Dataset Choice

For this analysis, we use the Cyber Events Database (CED) (Harry & Gallagher, 2018), which is a comprehensive repository of cyber incidents compiled from open-source reports, industry analyses, and government disclosures. The CED captures a wide array of events, including data breaches, denial-of-service attacks, espionage, and disruptions, spanning from 2014 to the present. It includes variables on actors, motives, event types, targets, and geographic details, making it suitable for relational modelling. In its raw form, the CED contains 14,981 observations, covering incidents across global contexts.

Several other databases exist for cyber IR research, but they vary in scope and focus. The most well-known include dyadic databases like the Dyadic Cyber Incident and Campaign Dataset (DCID) (Maness et al., 2022) and the Heidelberg Institute for International Conflict Research's dataset (Harnisch et al., 2021). Both are valuable for quantitative studies of interstate cyber aggression but are limited to state actors and often rely on numerical severity scores, which introduce subjectivity in assessing impact (e.g., low vs. high intensity).

The European Repository of Cyber Incidents (EuRepoC) (Zettl-Schabath et al., 2025) stands out as the most comparable in scope to the CED, and is more methodologically justified as their methodology ensures triangulation. For this project, the CED was selected for several reasons aligned with the exploratory goals. First, it represents incidents using categorical variables rather than numerical scores, which facilitates direct network construction without arbitrary scaling. Second, it avoids subjective constructs that could amplify interpretive bias, such as impact ratings, which is especially pertinent given the inherent subjectivity in cyber attribution and reporting. Other datasets often measure abstract elements like "severity" or "strategic value," which can vary by coder and complicate relational analysis.

Third, the CED provides clear, discrete categories (e.g., motives as "Financial" or "Protest") that are ideal for building nodes and edges in a network, minimizing preprocessing complexity. Finally, its simplicity supports a proof-of-concept demonstration, allowing us to focus on methodological innovation rather than data harmonization across disparate sources. While triangulation with EuRepoC could enhance robustness in future iterations, the CED's standalone structure suffices here, offering a balanced trade-off between comprehensiveness and usability. With 14,981 observations, it provides sufficient scale to reveal patterns without overwhelming computational demands.

Data Preparation

To prepare the data for network analysis, it was needed to clean and transform the CED to ensure suitability. First, we addressed duplicates, which can arise from multiple reporting sources for the same incident. Duplicates were identified by matching on description text, actor identifiers, and event dates to account for minor variations. This process removed

1,507 entries, leaving 13,474 unique incidents. This step was crucial to avoid inflating edge weights and distorting co-occurrence frequencies.

Next, variable selection was guided by the exploratory question: "Why did who what to whom?" This framed the focus on relational dynamics, leading to the inclusion of six key variables: actor_type (e.g., "Criminal," "Hacktivist"), industry (target sector, e.g., "Finance and Insurance"), event_subtype (e.g., "Data Attack," "External Denial of Service"), motive (e.g., "Financial," "Political-Espionage"), country (target location), and actor_country (origin location). These capture the core elements of cyber incidents without introducing excessive dimensionality, which could fragment the network.

Standardization was essential for consistency. Category names were harmonized for case sensitivity (e.g., "Finance and insurance" and "Finance and Insurance" merged). For motive and event_subtype, which often contained multiple entries separated by commas (e.g., "political-espionage, protest"), the categories were split into separate columns (motive1, motive2, etc.) to treat each as distinct nodes, preserving multiplicity without losing information (Table 1-3). Country names were to eliminate synonyms. Finally, to distinguish between similar categories across variables, such as "Germany" as a target (country) versus origin (actor_country), prefixed labels were used (e.g., "country:Germany," "actor_country:Germany"). This ensured substantive differentiation in the network, preventing conflation of roles.

Table 1: Distribution of Motives (Original Variable)

Motive	Count
Financial	8173
Industrial-Espionage	62
Personal Attack	77
Political-Espionage	643
Political-Espionage,Industrial-Espionage	3
Political-Espionage,Industrial Espionage	1
Protest	1367
Protest,Financial	1
Protest,Political-Espionage	1
Reputation	1
Sabotage	245
Undetermined	2900

Table 2: Distribution of Motives After Separation (motive1)

Motive	Count
Financial	8173
Industrial-Espionage	62
Personal Attack	77

Motive	Count
Political-Espionage	647
Protest	1369
Reputation	1
Sabotage	245
Undetermined	2900

Table 3: Distribution of Motives After Separation (motive2)

Motive	Count
Financial	1
Industrial-Espionage	4
Political-Espionage	1

Undetermined values were retained but excluded from the initial network construction, as they form the target of the inference procedure. This preparation yielded a clean dataset ready for relational modelling, with no imputation at this stage to avoid biasing the known structure.

Network Construction

The network was constructed as a multipartite graph, where nodes represent unique categories across the selected variables (e.g., "actor_type:Criminal," "motive1:Financial"). This design captures the relational essence of cyber incidents without assuming direct actor-to-actor ties, focusing instead on co-occurrences. Edges connect nodes if their categories appear together in the same incident, weighted by the frequency of such co-occurrences. For instance, if "actor_type:Criminal" and "motive1:Financial" co-occur in 500 incidents, the edge weight is 500. This weighting reflects prevalence, emphasizing dominant patterns.

Undetermined categories were excluded from nodes and edges during construction, as the goal is to infer them based on the known structure. The resulting full network comprises 321 nodes and 4,586 edges. The network is undirected, as co-occurrence implies mutual association rather than directionality, though future extensions could incorporate directed edges for causal flows (e.g., actor to motive).

Network Measurement

To understand the network and lay the groundwork for inference, several centrality and structural measures were computed, each selected for its relevance to interpreting cyber patterns. These metrics reveal how categories interconnect, highlighting generalists, dominants, connectors, and clusters. Community detection via the Louvain algorithm was also applied to identify natural groupings, treating it as a structural insight rather than a strict measure.

- **Degree**: This counts the number of unique connections a node has, indicating how many other categories it co-occurs with. A high degree suggests a "generalist" category versatile across contexts, such as a broadly used attack type or actor class. It helps identify elements involved in diverse incidents, informing where threats are most adaptable.
- **Strength**: As a weighted variant of degree, strength sums edge weights, capturing co-occurrence frequency. High-strength nodes dominate patterns, like common motives or targeted industries, revealing prevalence and "workload" in the cyber ecosystem, useful for prioritizing defences against high-volume threats.
- **Betweenness Centrality**: This quantifies how often a node lies on shortest paths between others, identifying bridges in the network. Categories with high betweenness connect disparate patterns (e.g., techniques shared across actors), acting as structural chokepoints where interventions could disrupt broad threat chains.
- **Closeness Centrality**: Measuring average shortest-path distance to all other nodes, high closeness indicates a category's proximity to the network's core. Such nodes interact quickly with diverse elements, spotlighting influential methods or actors that permeate the ecosystem.
- **Eigenvector Centrality**: This ranks nodes by connections to other high-centrality nodes, emphasizing embeddedness in influential clusters. It uncovers "anchors" of cyber activity, even if not the most frequent, capturing qualitative importance beyond raw counts.
- **Community Detection (Louvain)**: This algorithm partitions the network into clusters where intra-group connections are denser than inter-group. It reveals "threat ecosystems" (coherent combinations of actors, motives, industries, countries, and techniques), uncovering typologies of cyber incidents without predefined assumptions.

These measures collectively provide a multifaceted view: degree and strength for breadth and intensity, betweenness and closeness for connectivity, eigenvector for prestige, and communities for holistic patterns.

Network Results

The network analysis yields insights into the structure of known cyber incidents, revealing dominant patterns, key connectors, and clustered ecosystems. The top 20 nodes by frequency highlight the prevalence of criminal actors and financial motives, underscoring the economic underpinnings of many cyber events. For instance, "actor_type:Criminal" tops the list with 10,697 appearances, a degree of 228, and strength of 41,727, indicating it co-occurs broadly and frequently with other categories. This suggests criminals are generalists, involved in diverse incidents from data attacks to exploitations. Similarly, "motive1:Financial" (8,173

freq, degree 207, strength 33,786) dominates, reflecting profit-driven cybercrime as a core driver.

Table 4: Top 20 Nodes by Network Strength. Legend: Freq. = Frequency in incidents; Deg. = Degree; Str. = Strength; Betw. = Betweenness centrality; EC = Eigenvector centrality; Com. = Community

Node	Freq.	Deg.	Str.	Betw.	EC	Com.
actor_type:Criminal	10697	228	41727	39679.93	1.00	1
motive1:Financial	8173	207	33786	1169.78	0.92	1
country:United States of America	6808	85	26831	1117.67	0.79	1
event_type1:Exploitation of Application Server	5236	210	20242	10781.70	0.57	1
event_type1:Data Attack	3378	165	14759	1688.58	0.45	1
industry:Public Administration	2397	225	9706	12810.65	0.21	2
actor_country:Russia	1581	124	7980	1074.95	0.16	2
industry:Health Care and Social Assistance	1952	93	7787	1.25	0.30	1
actor_type:Hacktivist	1515	225	6858	7358.72	0.04	2
motive1:Protest	1369	203	6311	1366.97	0.04	2
event_type1:External Denial of Service	1327	167	5458	1534.27	0.06	2
industry:Finance and Insurance	1322	156	5255	1667.00	0.16	1
industry:Information	1362	172	5132	862.92	0.13	2
industry:Educational Services	1269	110	4958	448.00	0.17	1
event_type1:Exploitation of End Hosts	1227	141	4798	1952.92	0.14	3
event_type2:Exploitation of Application Server	894	122	4577	8.08	0.13	1
industry:Professional, Scientific, and Technical Services	1156	109	4543	261.00	0.15	1
event_type1:Message Manipulation	993	188	3872	1863.17	0.06	2
industry:Other Services (except Public Administration)	807	126	3136	624.12	0.07	3
actor_type:Nation-State	636	158	3018	2068.58	0.03	3

High-strength nodes like "country:United States of America" (strength 26,831) and "event_type1:Exploitation of Application Server" (20,242) point to the U.S. as a frequent target and application exploits as a common vector, aligning with reports of widespread vulnerabilities in digital infrastructure (Shore, 2022). Betweenness values reveal connectors: "actor_type:Criminal" (39,841) and "industry:Public Administration" (12,894) act as bridges, linking disparate clusters (e.g., criminals connecting financial motives to health sectors). Closeness scores, such as 0.459 for "actor_type:Hacktivist," indicate proximity to the core, allowing quick propagation of protest-driven disruptions. Eigenvector centrality emphasizes embedded influence: "actor_type:Criminal" (1.000) and "motive1:Financial" (0.918) anchor high-impact areas, while lower values for "actor_type:Nation-State" (0.0253) suggest state actors operate in more peripheral, specialized niches.

Community Results

Community detection identifies three main clusters, each representing distinct threat ecosystems:

- Community 1, the largest by strength, captures economically motivated cybercrime targeting U.S. entities via data exploits, reflecting the dominance of ransomware and breaches in private sectors (Kosenkov, 2016).
- Community 2 centers on politically charged incidents, with hacktivists and Russian actors using denial-of-service against public administration, echoing cases like Estonia and Georgia (Whyte, 2018).
- Community 3 focuses on state-sponsored espionage, exploiting end hosts in non-public services, highlighting covert operations (Choucri, 2024). These clusters validate the shift from isolated incidents to systemic patterns, showing how co-occurrences form interpretable typologies (e.g., financial-criminal vs. protest-hacktivist ecosystems)

Table 5: Community-Level Structure of the Cyber Incident Network

Com.	Nodes (n)	Total Strength	Average Degree	Dominant Categories
1	81	184701	37.8	Criminal, Financial, United States of America, Exploitation of Application Server, Data Attack
2	175	66469	24.5	Public Administration, Russia, Hacktivist, Protest, External Denial of Service
3	64	22444	28.5	Exploitation of End Hosts, Other Services (except Public Administration), Nation-State, Political-Espionage, Exploitation of End Hosts

The Approach for Inferring the Unknowns

Building on the observed incident network, undetermined values can be inferred by exploiting the relational structure of known categories. Rather than treating missingness as random or purely descriptive, this approach assumes that unknown attributes are embedded in, the same contextual patterns that characterize observed incidents. Inference is therefore probabilistic and relational: an undetermined category is assigned based on its structural proximity to the known attributes of an incident.

Operationally, this approach evaluates how strongly each candidate category connects to an incident's observed context. For a given variable (e.g., *motive1*), incidents labelled "Undetermined" are isolated, and all known categories of that variable are treated as candidates. For each such incident, the weighted connections between its known nodes and each candidate

are summed. The candidate with the highest cumulative edge weight is selected as the most plausible inference. This process leverages undirected edge weights, capturing co-occurrence strength without imposing causal directionality.

This approach is implemented in R via a custom function. Through this function, the procedure was applied iteratively across all variables.

Results of the Unknowns

The inferred categories are not evenly distributed but instead concentrate around structurally dominant nodes in the network. For actor type, *Criminal* actors overwhelmingly dominate the inferred cases, with only a handful attributed to *Hacktivists*. Similarly, motives are heavily skewed toward *Financial*, with limited assignment to protest or espionage-related motives. These results reflect the centrality and strength of criminal–financial nodes, which are densely connected across industries, event types, and countries.

Industry-level inferences most frequently point to *Health Care and Social Assistance* and *Public Administration*, sectors that occupy prominent positions in the network due to their repeated co-occurrence with high-frequency attack types. Event-type inferences further reinforce this pattern: *Exploitation of Application Server* is by far the most common inferred event type, followed by denial-of-service attacks. Together, these results suggest that unknown incidents are structurally aligned with a high-volume exploitation ecosystem rather than niche or novel attack modes.

At the geopolitical level, inferred target countries cluster around the *United States of America*, while inferred actor countries are overwhelmingly attributed to *Russia*. This reflects both empirical concentration in the dataset and the strong embedding of these nodes within multiple communities, particularly those associated with criminal activity and political contention.

Substantively, these inferences suggest that many "unknown" cases are not anomalous but instead resemble well-established incident profiles: financially motivated attacks, exploiting common vulnerabilities, targeting high-value public and private sectors.

Discussion

Taken together, the results demonstrate how network analysis can be used not only to map cyber incident ecosystems but also to interpret structured uncertainty within them. The identified communities, ranging from criminal–financial clusters to political-hacktivist and state-espionage groupings, provide the structural backdrop against which unknown values are inferred. In this sense, inference does not introduce new information but situates missing attributes within existing systemic patterns.

However, the dominance of high-prevalence categories in the inferred results warrants careful interpretation. Because inference is driven by connection strength, structurally central nodes, such as *Criminal*, *Financial*, or *Russia*, exert disproportionate influence. This may reflect

Table 6: Predicted Categories for Undetermined Cyber Incidents

Predicted category	Number of incidents
Actor type	
Criminal	437
Hacktivist	6
Industry	
Health Care and Social Assistance	173
Public Administration	52
Event type	
Exploitation of Application Server	833
External Denial of Service	56
Data Attack	1
Motive	
Financial	2757
Protest	142
Political-Espionage	1
Target country	
United States of America	417
Actor country	
Russia	10697
Saudi Arabia	5
India	2
North Korea	1

real-world asymmetries, including the scale and adaptability of profit-driven cybercrime, but it may also amplify reporting biases inherent in the underlying data. As such, inferred dominance should be read as probabilistic alignment rather than definitive attribution.

The key contribution of this approach lies in its treatment of missingness as relational rather than accidental. Unknowns are not excluded or imputed arbitrarily; instead, they are interpreted as outcomes of systemic pressures embedded in the global cyber incident network. This allows researchers to extract meaningful signals from incomplete data while remaining attentive to epistemic limits. At the same time, the method underscores an important constraint: network-based inference can reproduce existing patterns more readily than it can detect emerging or underreported threats.

Overall, this proof-of-concept illustrates the analytical value of network methods for cyber conflict research. By integrating inference with community structure, the approach enhances both empirical coverage and theoretical insight, framing cyberspace not as a collection of iso-

lated events but as a structured environment in which uncertainty itself becomes analytically informative.

Future Research Directions

Future work can refine this approach in several directions to address limitations and expand applicability. First, incorporating more variables, such as severity levels, tools used, or temporal indicators, could enrich contextual depth, reducing overdominance by providing finer-grained associations. For example, adding "impact type" from triangulated sources like EuRepoC might differentiate clusters, yielding more nuanced inferences.

Second, time-series analysis, such as constructing annual sub-networks, would capture evolution, revealing shifts in patterns (e.g., rising hacktivism post-2010) and aiding policy forecasting (Choucri, 2012a). This could use dynamic metrics like temporal community stability to track changes in global pressures.

Third, narrowing the research question (e.g., focusing on state-sponsored incidents) might produce more balanced networks, where dominance holds greater substantive weight, avoiding dilution from broad scopes.

Fourth, iterative inference strategies could improve accuracy: predict variables with fewest undetermineds first, then update the network with these inferences before tackling others. Moreover, probabilistic extensions, could assign confidence intervals, accounting for ties or weak connections.

Finally, a critical reflection: networks excel at interpolating within known structures but fail on "new" cases or emergent patterns, such as novel AI-driven threats or new state strategies. Integrating real-time data or hybrid ML-network models could mitigate this, ensuring relevance in fast-evolving cyberspace. These avenues promise to advance cyber scholarship toward more robust, adaptive theories.

Bibliography

Attatfa, A., Renaud, K., & De Paoli, S. (2020). *Cyber diplomacy: A systematic literature review. Procedia Computer Science, 176*, 60–69. https://doi.org/10.1016/j.procs.2020.08.007

Barnum, M. (2022). Dealing with missing and incomplete data. In R. J. Huddleston, T. Jamieson, & P. James (Eds.), *Handbook of research in international relations* (pp. 425–445). Edward Elgar.

Choucri, N. (2012a). Cyberspace: New domain of international relations. In *Cyberpolitics in international relations* (pp. 49–70). The MIT Press.

Choucri, N. (2012b). Cyber content: Leveraging knowledge and networking. In *Cyberpolitics in international relations* (pp. 71–88). The MIT Press.

Choucri, N. (2024). *Lateral pressure in international relations: A review of theory, data, method, analysis. SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.4948942.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development, 20*(2), 96–121. https://doi.org/10.1080/02681102.2013.836699.

Foulon, M., & Meibauer, G. (2024). *How cyberspace affects international relations: The promise of structural modifiers. Contemporary Security Policy, 45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Gorwa, R., & Smeets, M. (2019). *Cyber conflict in political science: A review of methods and literature.* SocArXiv. https://osf.io/preprints/socarxiv/fc6sg/

Harnisch, S., Zettl, K., & Steiger, S. (2021). *Heidelberg Cyber Conflict Dataset (HD-CY.CON)* (Version 1) [Data set]. heiDATA. https://doi.org/10.11588/DATA/KDSFRB

Harry, C., & Gallagher, N. (2018). *Classifying cyber events. Journal of Information Warfare, 17*(3), 17-31

Kosenkov, A. (2016). *Cyber conflicts as a new global threat. Future Internet, 8*(3), Article 45. https://doi.org/10.3390/fi8030045

Kostyuk, N., & Zhukov, Y. M. (2019). *Invisible digital front: Can cyber attacks shape battlefield events? Journal of Conflict Resolution, 63*(2), 317–347. https://doi.org/10.1177/0022002717737138

Maness, R. C., Valeriano, B., Hedgecock, K., Jensen, B. M., & Macias, J. (2022). *Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 2.0* (Dataset documentation).

Menninga, E. J., & Goldberg, L. A. (2022). Network analysis. In R. J. Huddleston, T. Jamieson, & P. James (Eds.), *Handbook of research methods in international relations* (pp. 477–494). Edward Elgar.

Pratt, S. F. (2022). Epistemology: logic, causality, and explanation. In R. J. Huddleston, T. Jamieson, & P. James (Eds.), *Handbook of research methods in international relations* (pp. 25–40). Edward Elgar. https://doi.org/10.4337/9781839101014.00011.

Shore, J. (2022, October 12). *Data incoming: How to close the cyber data gap.* War on the Rocks. https://warontherocks.com/2022/10/data-incoming-how-to-close-the-cyber-data-gap/

Whyte, C. (2018). *Dissecting the digital world: A review of the construction and constitution of cyber conflict research. International Studies Review, 20*(3), 520–532.

Zettl-Schabath, K., Bund, J., Müller, M., Borrett, C., Hemmelskamp, J., Alibegovic, A., Bajra, E., Jazxhi, A., Kellenter, E., Sachs, A., & Shelley, C. (2025). *Global Dataset of Cyber Incidents* (Version 1.3.2) [Dataset]. EuRepoC.