Navigating Geopolitical Storms: Assessing the Robustness of Canada's 5G Research Network in the Wake of the Huawei Conflict

Anas Ramdani[1], Catherine Beaudry[2], Mario Bourgault[3], and Davide Pulizzotto[4]

[1]*anas.ramdani@polymtl.ca,* [2]*catherine.beaudry@polymtl.ca,* [3]*mario.bourgault@polymtl.ca,* [4]*davide.pulizzotto@polymtl.ca*
Polytechnique Montréal, Département de Mathématique et de Génie Industriel
2500 Chemin de Polytechnique, Montréal, H3T 1J4, Canada

Abstract

Amid geopolitical tensions over 5G technology, concerns about foreign firms like Huawei collaborating with academia have surfaced. This paper examines Huawei's role in Canadian research, analyzing its impact on network robustness and research themes over time. Robustness in network research has been extensively explored, yet there remains a notable gap in understanding the influence of geopolitical factors and foreign corporate presence, such as Huawei's, on these networks. The main results of this research show that: (1) The 5G network exhibits a decreasing trend in network robustness, with the potential for fragmentation increasing over time; (2) The impact of Huawei's removal on the network's Largest Connected Component (LCC) is relatively minor; (3) The network retains its small-world properties irrespective of Huawei's presence, and its removal has a minor impact on knowledge transfer efficiency; (4) Huawei's removal does not significantly affect network centralization, nor does it influence the prevailing trend observed over time; (5) Hierarchical clustering and specificity analysis identify Huawei's strategic focus on the silicon and optical photonic domain within the 5G research; (6) The collaboration-topic network shows a high degree of robustness, suggesting that Canada's research contributions in these areas are unaffected by the absence Huawei. This study provides a nuanced view of Huawei's role in Canadian 5G research, suggesting that while the company is a significant player, its impact is in general neither singular nor irreplaceable within the academic network.

Introduction

In the current geopolitical landscape, where tensions surrounding advanced technologies like 5G and the rift between China and the Western world are intensifying, these conflicts have begun to permeate the academic research sector. Amidst growing suspicion in the West regarding collaborations between academia and foreign firms such as Huawei, it has become crucial to examine their role and influence within the academic research sphere. In a country where "business-funded R&D in the higher education sector is relatively high and the number of academia-business research partnerships is increasing" (Council of Canadian Academies, 2018, p.11), this may have important repercussions.

Network robustness is defined as the ability of a network to maintain its overall functionality despite the removal or failure of some of its components, such as nodes or edges (Liu et al, 2017; Nguyen et al, 2022). There is a vast literature on network robustness, with geopolitical contexts frequently mentioned in domains such as energy (Chen et al., 2022; Wei, Xie, & Zhou, 2022) and air transport networks (Zhang et al., 2021; Papadopoulos et al., 2023). However, in our knowledge, there is a gap in such robustness studies of academic-business networks within geopolitical tension frameworks. A network's robustness is assessed by simulating perturbations, such as the removal of links or nodes. This process is commonly referred to in literature as "attacks". Previous literature has explored the impacts of attacks on network centralization (Rueda, Calle, & Marzo, 2017). For small-world networks, the focus has often been on how they withstand attacks, particularly in comparison with other network types like scale-free and random networks (Duan et al., 2016). Additionally, some studies contrast the effects of targeted versus random attacks on small-world

networks (Sawai, 2013). However, there is a lack in the literature when it comes to assessing the impact of targeted attacks within the context of academic-business research networks.

Our study contributes to the literature by assessing the robustness of academic-business networks in the context of geopolitical tensions using both business-academic and collaboration-topics network analysis. We examine how networks composed of a range of businesses, including large multinationals, and academic researchers respond to targeted attacks by evaluating key structural properties, such as small-world characteristics and network centralization. By also considering research themes as a third node type in the collaboration-topics network, we analyze the effects of such disruptions on the thematic research direction in the Canadian 5G network. More specifically, given the recent geopolitical tensions surrounding China, we will focus on Huawei's involvement in the Canadian research network. We will explore the company's impact on the structural robustness of this network over time (2010-2021) and its influence on the thematic research directions within Canada. Following this context, the research question we pose is:

"How does the presence and geopolitical conflicts involving Huawei affect the network structural robustness and the landscape of the 5G research topics network in Canada?"

The results of our study point to a downward trajectory in the robustness of the 5G network. The structural properties of the network experience minimal disruption upon the exclusion of Huawei. The analysis of the collaboration-topic network reveals a high level of robustness, suggesting that Canada's research contributions in these 5G topics remain strong, even in the absence of Huawei. The remainder of this paper is organized as follows. The next section reviews the backdrop of geopolitical tensions that justify this study. The subsequent section presents the social network analysis literature pertinent to assess network robustness. The paper then present the methodology, which details the procedures and metrics used to evaluate network robustness and Huawei's specific impact on the structural properties of the network as well as on 5G research topics. The subsequent section presents a detailed analysis of the findings. The final section of the paper concludes by summing up the implications for 5G research and Huawei's role.

Canadian science amid escalating tensions between China and the USA

Geopolitical tensions between China and the USA reached a peak in 2018 under Trump's administration. Adopting a confrontational approach towards Chinese businesses, it particularly targeted Huawei (BBC, 2019; Jaisal, 2020; The Star, 2022). The U.S. Commerce Department took the significant step of prohibiting American firms from doing business with Huawei (The Globe and Mail, 2018; U.S. Department of Commerce, 2020). At the heart of the U.S.'s concerns with Huawei were not just trade imbalances with China but profound national security fears (Kaska, Beckvard and Minárik, 2019; Parsons, 2020). The U.S. expressed apprehensions about Huawei's technological capabilities, suggesting that they could be exploited by the Chinese government to compromise 5G networks (Kaska, Beckvard & Minárik, 2019; Jaisal, 2020). Starting in 2019, the U.S. imposed tough sanctions on Huawei, labeling it a security risk (BBC, 2019; Hertzberg & Platt, 2022; The Star, 2022).

This broader U.S.-China conflict saw Canada inadvertently drawn into the fray on December 1, 2018, in Vancouver, Canada. On that day, Canadian officials detained Huawei's Chief Financial Officer, Meng Wanzhou, at the US government's request (Jaisal, 2020; The Globe and Mail, 2018; Friis & Lysne, 2021; Azad, 2022). In what many perceived as a retaliatory move, China detained two Canadians on charges of endangering Chinese national security (BBC, 2019). After several years of escalating geopolitical tensions between China and Canada, the Canadian government announced on May 20, 2022, its decision to ban Huawei from participating in its 5G networks (Hertzberg & Platt, 2022).

The conflict between Huawei and Western nations has had ripple effects in the academic world (Owens, 2022). The concerns over intellectual property theft and potential espionage began to overshadow the ethos of open collaboration (Friis & Lysne, 2021). In response to the evolving geopolitical landscape, on February 14, 2021, Canada's major national research agencies introduced stringent measures (Mervis, 2023). They announced that they would no longer fund proposals involving foreign collaborators that pose a security risk. While these guidelines did not explicitly name China, they echoed similar protective measures adopted by other nations (Mervis, 2023), such as Sweden (Ministry of Foreign Affairs, 2019) and India (Kumar, 2019). In Canada, researchers seeking grants from the Natural Sciences and Engineering Research Council (NSERC) were now required to undergo a security risk assessment. These guidelines specifically highlighted concerns about organizations, such as Huawei, potentially acting against Canadian interests (Wexler, 2022). The atmosphere of suspicion in the academic sector indeed predates the official government ban on Huawei and the formalization of funding agency guidelines for research collaboration with foreign firms. Canada's response in banning Huawei and imposing these guidelines was relatively delayed compared to other Western countries. The Canadian government's limited communication regarding the progress of its decision on banning Huawei can be attributed to the delicate situation involving the two Canadians arrested in China (Tunney & Raycraft, 2022).

Huawei's financial commitment to research and development, both globally and in Canada, is substantial. Between 2009 and 2019, Huawei invested at least $630 million (CAD)[1] in Canada. More specifically, from 2014 to 2019, the company contributed over $56 million (CAD) to Canadian universities (Parsons, 2020). This funding was channeled into research labs, scholarships, and various academic-focused research initiatives, underscoring Huawei's significant role in supporting Canadian academia (Parsons, 2020).

Having delineated the complex geopolitical landscape and its ramifications on the Canadian research area, the aim of this paper is to gain a deeper understanding of Huawei's impact on Canadian 5G research. One effective method to study Huawei's impact in academic-business collaboration is through network analysis. By mapping the network, we can thoroughly identify the significance of various nodes (academics and businesses), understand the intricacies of their interconnectivity, and analyze the overall structure of the network. In network analysis, one of the most insightful avenues to simulate and understand the importance of nodes or edges on the network's properties is through the lens of robustness. By employing robustness metrics, we gain a comprehensive understanding of the network's robustness and stability, especially in the context of Huawei's involvement.

Network robustness in the literature

Network robustness has become a central focus in network studies, highlighting the ability of a network to withstand disruptions (Bilal et al., 2018). At its core, robustness represents the enduring ability of a network to maintain its functionality, even when subjected to disruptions (Dekker & Colbert; 2004; Carchiolo et al., 2019; Nguyen et al., 2022). The concept of robustness transcends theoretical applications and holds significant value in real-world scenarios. For instance, Xie, Wei, & Zhou (2021) applied this notion to evaluate the robustness of the international oil trade network. By simulating disruptions such as national bankruptcy and economic sanctions, their research explains the network's susceptibility to such geopolitical events. Lordan et al., (2014) define and apply a robustness-oriented methodology to identify airports whose isolation would critically undermine the global air transport network's connectivity. This robustness assessment helps in planning contingency plans to maintain network integrity in the event of such airport

[1] Amount converted to CAD from Parsons (2020), where the reported amount was $500 million USD.

closures. The use of robustness as a key analytical tool extends into other disciplines, including mathematics, biology, and physics (Morales, Paiva & Bustos-Jiménez, 2018).

Assessing network robustness is complex, with many methods available in the literature. A widely adopted approach involves the systematic removal of nodes or edges, followed by an analysis of the subsequent structural changes. This method aims to measure the repercussions on the network's interconnectivity as its nodes/edges are progressively eliminated. Two foundational metrics in this context are node and edge connectivity (Wu et al., 2011; Liu et al., 2017). They measure the minimal number of vertices or edges that need to be removed to fragment the network.

The evolution of the Largest Connected Component (LCC) is frequently referenced in the literature as a metric for robustness. It tracks the changes in the size of the most extensive group of interconnected nodes in the network (Iyer et al., 2013; Nguyen et al., 2021). Expanding on this, serves as one of the key metrics for assessing network robustness, particularly regarding targeted node attacks (Schneider et al., 2011). This measure not only pinpoints the moment the network fragments but also monitors the size of the LCC throughout the node removal process, providing a nuanced understanding of network robustness (Ma, Liu & Duan, 2016). When considering the evolution of network robustness over time, measures such as the composition of the LCC and the robustness measure R are more direct and relevant than others commonly found in the literature, like network diameter (Beygelzimer et al., 2005; Liu et al., 2017) and assortativity (Rotolo & Frickel, 2019; Nguyen et al., 2022).

Additionally, two other structural network properties metrics used in robustness literature are small-world network score and network centralization metrics. These measures are particularly insightful for our study of an academic-business research network, as they shed light on how effectively information spreads (Cowan & Jonard, 2004) and how central knowledge hubs contribute to the overall knowledge exchange (Hu et al., 2023).

Small-world networks are optimal for efficient knowledge dissemination. They are characterized by a low average path length and a high clustering coefficient. The ratio of closed triangles to triples in the network is represented by the clustering coefficient (Watts & Strogatz, 1998; Ebadi & Schiffauerova, 2015). Essentially, it quantifies the interconnectedness of a node's immediate neighbors (Hansen, Shneiderman, Smith, & Himelboim, 2020). On the other hand, the average path length denotes the mean number of connections in the shortest path between any two nodes in the network (Chen, 2023).

Research on network robustness explores small-world network characteristics in response to various attacks. For instance, Zhang et al. (2014) developed a method aimed at improving the robustness of small-world networks under attack. In a similar vein, Duan et al. (2017) examined the reactions of small-world networks to different types of attacks compared to scale-free, random, and regular networks. Their findings indicate that networks, despite varying topologies, can exhibit comparable levels of robustness according to the metrics used for assessing robustness. Despite these contributions, there seems to be a gap in understanding the persistence of small-world features when an academic-business network faces targeted attacks that remove a key node, such as Huawei.

Network centralization provides insights into the structural characteristics of a network. Central nodes in a highly centralized network are crucial for quick information spread. However, if these central nodes fail, they can become bottlenecks, slowing down or even halting communication within the network (Luke et al., 2013). Network centralization is also employed as an indicator of network robustness. In this context, Rueda, Calle & Marzo (2017) show that networks with high centralization values generally exhibit greater robustness. In our study, we employ network centralization alongside small-world analysis to examine the effects of targeted attacks on network structure. By investigating how these properties change following

targeted removals, particularly the extraction of a key node like Huawei, we aim to provide a comprehensive picture of the network's structural robustness.

In social network analysis, it is possible to model a network disruption and evaluate the ensuing effects. This is known as an "attack" in the literature. Networks can be subjected to two primary types of attacks: random and targeted (Xiaohong et al., 2020). Random attacks involve the removal of nodes or edges with an equal probability, without any specific targeting (Liu et al., 2017; Nguyen et al., 2022). In contrast, targeted attacks are more strategic and deliberate. In these attacks, the most important node or edge is removed sequentially based on specific metrics like centrality measures (Iyer et al., 2013; Louzada et al., 2015; Ma, Liu & Duan, 2016; Liu et al., 2017).

According to Nguyen et al. (2022), there are two main strategies within targeted attacks. The initial attack strategy operates on a predetermined hierarchy, typically based on centrality measures such as degree, closeness, and betweenness. This approach aims to swiftly disrupt the network by targeting its most influential nodes from the outset. The objective is to observe the network's response and determine if it will disintegrate or maintain its structural integrity despite the targeted removals (Iyer et al., 2013). In contrast, the recalculated attack strategy adopts a dynamic approach. After each node or edge removal, the significance of the remaining entities is reassessed. This iterative process, which prioritizes nodes by their nodal degrees, persists until the network disintegrates into isolated nodes (Yang et al., 2015; Moore, Small and Yan, 2021). The underlying objective of these targeted strategies is to inflict maximal disruption, with the network's robustness measured by the proportion of nodes it can afford to lose without breaking apart. In this study, to measure the robustness of our network, we employ a targeted attack strategy. Adopting a targeted attack strategy is appropriate, as it aligns with our objective to examine the repercussions of specific geopolitical tensions and the influence of Huawei on the network.

Data and methodology

Data

The data necessary for this research stem from three sources: two research funding databases from the Natural Sciences and Engineering Research Council of Canada (NSERC), Mitacs, and Clarivate's Web of Science (WoS). The complete database is built by pulling together information from various sources to complement the main data from NSERC on 5G research in Canada.

NSERC is a federal agency that supports national research and funds both university and industry-related projects, fostering a collaborative environment between them. The NSERC data, which are publicly available, provide details on project funding, researcher collaborations, and university-industry partnerships. These data have been structured into three distinct annual CSV files since 1991. The "Awards" files provide in-depth project details, name of principal applicant, affiliated institutions, research themes, grant amounts, and project abstracts, among other metadata. The "Co-applicants" files link principal researchers to their co-applicants using unique installment identifiers. Finally, the "Partners" file bridge researchers and co-applicants to their corresponding institutional partners.

The NSERC database assigns a unique identifier to each annual funding installment for a project, which leads us to count the project on an annual basis. For instance, a project that spans three years will be considered as three distinct entries when analyzing the academic-business network. This method ensures that the temporal dimension of collaboration is captured. We focused on projects from 2010-2021[2] that had

[2] This specific timeframe was chosen for two main reasons: First, very few projects and grants exist prior to 2010; Second, NSERC has not released the databases for 2022 and 2023.

references to 5G in their title or abstract. This first search yielded 877 yearly installment-projects. The exclusive use of '5G' as the keyword was key to ensure the selection of projects genuinely related to the fifth generation of mobile communication[3]. Recognizing that 5G is an umbrella term for a myriad of technologies[4], opting for broader terms might lead to inaccuracies because they are not specific to 5G and could be related to other topics or goals. To mitigate this, a manual review was conducted to filter out non-relevant projects. After this step, we were left with 840 yearly installment-projects. Then, we pinpointed the co-applicants and industrial partners associated with each project.

To enhance the completeness of the database, we integrated data from MITACS and Web of Science. This method allowed us to enrich our dataset with pertinent NSERC projects by adding researchers focused on 5G, whom we identified through MITACS and Web of Science databases. MITACS is a national organization that primarily funds university-industry partnerships. We extracted data on project titles that included the term '5G' for the 2010-2019 period. Researchers from these projects were then cross-referenced with the NSERC database and additional NSERC project subsequently added to the main database. This additional step added 24 researchers to the database.

From the Web of Science, we extracted the articles that referenced '5G' in the title, abstract or keywords for the 2010-2021 period, that was coauthored by had at least one Canadian author. Each article was manually scrutinized for its relevance. After identifying Canadian researchers from the metadata of these articles, we incorporated the specific NSERC projects associated with these additional researchers into our database. Adding the 370 additional authors yields a final database that comprise 5,537 NSERC yearly installment-projects which correspond to 1,871 NSERC unique multi-year projects in which 947 researchers and 774 partners are involved.

A significant aspect of this process was the manual standardization of researcher names. Name disambiguation was carried out both within each individual database and between the three databases to rectify inconsistencies and variations in name representation. This ensured that any identical or similar names were accurately differentiated. The process was further supported by bibliometric information and references from official university web pages. This comprehensive approach ensured a robust database of '5G' NSERC-funded projects.

As previously mentioned, NSERC provides abstracts for each project, which we used to identify the key topics for constructing our collaboration-topics network. The initial step, however, was to clean our textual data to ensure accurate clustering results. We followed these steps:

- *Exclusion of French abstracts:* The NSERC database includes projects with abstracts in both French and English. Due to the limitations of our traditional text mining techniques, which do not easily support a multilingual framework, we opted to exclude the less represented language. Given the predominant presence of English projects, those in French were systematically excluded to ensure consistency across our final database. This approach led to the exclusion of 339 French unique multi-year projects.
- *Removal of empty abstracts:* We identified and removed 4 empty abstracts from our dataset.

[3] We initially extracted articles using keywords such as network slicing, massive MIMO, network function virtualization (NFV), millimeter wave (mmWave), and software-defined networks (SDN), resulting in a total of 10,360 final yearly installment-projects articles. Following expert consultation, we adopted the strategy of selecting only those articles where the term '5G' is explicitly mentioned, ensuring the elimination of false positives. This process resulted in a final selection of 5,537 yearly installment-projects.

[4] The term 5G is not exclusive to 5th generation. For example, some projects contain this abbreviation to refer to 5 grams. These projects have been removed from our database.

- *Morphosyntactic analysis:* Leveraging the Udpipe package from the R library (Wijffels et al., 2019), we executed tokenization and lemmatization of abstracts. This tool also facilitated the categorization of each term's grammatical nature. The Udpipe package in R includes part-of-speech tagging, which labels words in a text according to their grammatical role, such as nouns, verbs, adjectives, adverbs, etc. Since our methodology was specifically designed to analyze the most frequent and significant topics, we focused on retaining only nouns and adjectives[5]. This approach is based on the assumption that these parts of speech can effectively capture the main topics of a corpus. This selective retention of words is recognized as a standard approach by the literature (see Jacobi et al., 2018; Parinov et al., 2021; Lind et al., 2022). To address variations in similar words, we prioritized lemmas over tokens in our analysis.
- *Term filtration and document-term matrix construction:* After iterative evaluations, a decision was made to adopt n-grams of size 2. Only terms recurring more than five times and manifesting in over twenty distinct documents were preserved. This filtration strategy was pivotal in omitting less significant terms. Subsequently, a document-term matrix was devised, showcasing term frequencies across abstracts.
- *Term weighting strategy:* Numerous methodologies exist for term weighting in textual computer analysis. Among them, Tf-IDF (Term Frequency-Inverse Document Frequency) stands out as a widely recognized technique (Roul, Sahoo, & Arora, 2017). This approach involves the multiplication of two metrics: TF (Term Frequency) and IDF (Inverse Document Frequency). Consequently, a term is assigned a higher weight if it frequently appears in a document (elevated TF) but is scarcely found across other corpus documents (low DF, amplified IDF).

Following the preprocessing of our database, we were left with a total of 1,528 unique multi-year projects. Given our primary aim to evaluate Huawei's influence on specific topics in comparison to other industrial partners, we first start with the count of projects for each industrial partner that applied for NSERC funding, as shown in Fig. 1. This figure shows that Ericsson (63 projects) and Huawei (54 projects), the two primary competitors in Canada's 5G landscape, are at the forefront in terms of the number of projects.

[5] We manually examined the verbs, nouns, and adjectives in the dataset and chose to retain only the nouns and adjectives, as verbs were not pertinent for extracting the most significant topics.

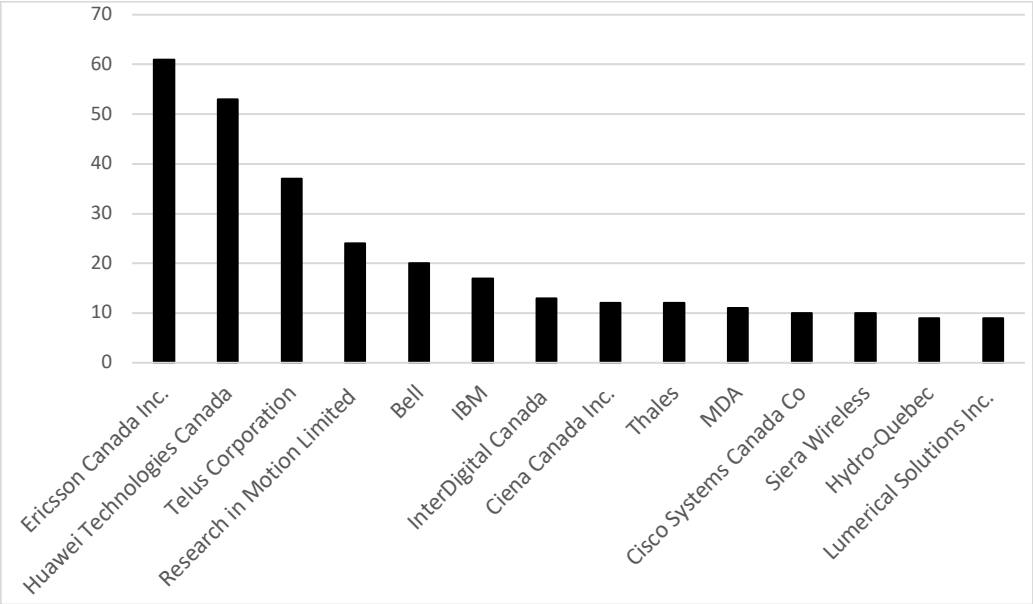


Fig. 1 Number of projects for industrial partners

Assessing the Academic-Industry collaboration network

Several structure elements are necessary to characterize the network prior to the targeted attacks analysis: centrality measures of each node, size of the largest connected component, average path length and clustering coefficient (both needed to assess the small-world-ness), and network centralization.

Centrality measures

Measures of node centrality serve two purposes in our analysis. First, they provide a clear picture of how the most central nodes in the network change over time. Since our focus is on Huawei, understanding the position of the company within the network is crucial for interpreting robustness findings. Second, the robustness measure, R, calculation requires to remove the nodes with the highest to the lowest centrality. We use three specific centrality measures: degree, betweenness and closeness[6].

The degree centrality of a node represents its direct connections to other nodes. Nodes with higher centrality are more collaborative in nature (Zare-Farashbandi, Geraei, & Siamaki, 2014). The betweenness centrality of a node quantifies its function as an intermediary or bridge within the network. It measures the frequency with which a node is found on the shortest path connecting other node pairs (de Nooy, Mrvar, & Batagelj, 2005). Nodes with high betweenness centrality values play a pivotal role in facilitating knowledge and information flow across diverse network groups. Lastly, closeness centrality determines how close a node is to all its peers in the network. It provides insight into a node's ability to efficiently interact with others. Nodes with higher closeness centrality are better positioned to connect with the entirety of the network, underscoring their central role (Freeman, 1978).

Attack strategy and metrics

Measuring the network's overall robustness to targeted attacks first requires building a baseline to which the attacks will be compared. For this purpose, we calculate the Schneider et al. (2011) robustness measure, R. We then employ a targeted attack strategy. Targeted attacks are particularly relevant for our analysis in

[6] In the interest of conciseness, we will show only the degree centrality results for evaluating robustness (R), as the conclusions drawn are consistent with those from the other centrality measures.

comparison to random attacks, given that we are specifically examining the impact of geopolitical tensions surrounding Huawei on the network. Our approach is twofold:

- *Overall network robustness using R as a robustness indicator for the entire network:* Nodes are first ranked based on their centrality. We then simulate a targeted attack by systematically removing nodes, starting from those with the highest centrality and progressing towards those with lower centrality. This sequential removal allows us to compute the robustness measure R, providing a comprehensive understanding of the network's robustness against targeted attacks. Proposed by Schneider et al. (2011), the robustness measure, R, is defined as:

$$R = \frac{1}{N}\sum_{i=1}^{N} s(i)$$

  Where N represents the total number of nodes in the network, while $s(i)$ denotes the size of the largest connected component[7] (LLC) following the removal of i node. In a star network, the minimum value of R equals 1/N, while in a complete network, the maximum value of R is 0.5 (Nguyen et al., 2022). This measure focuses on the evolution of the LLC as the highest-degree nodes in the network are systematically targeted and removed. This process corresponds to what is referred to as a series of targeted attacks, with the robustness being assessed after each node's removal. The larger the value of R, the more robust the network is deemed to be.
- *Comparative robustness assessment:* Our next objective is to discern the network's robustness in the context of Huawei's removal and compare this with the removal of each of the other nodes. In our analysis, we contrast the impact of Huawei on the network's robustness with that of other key players in the Canadian ecosystem, particularly focusing on Ericsson, Huawei's main competitor in the country. We systematically eliminate each node from the network, also taking out nodes that only collaborated with the node being removed. We measure the subsequent changes in the following metrics: The size of the Largest Connected Component (LCC), the network's centralization, the small-world indicator. These metrics are described below.

The size of the LCC

This allows us to measure the impact of each node's absence on the overall network robustness. Specifically, by measuring the change in the size of the LCC after each node removal, we can determine the relative importance of each node, including Huawei, to the network's robustness.

Small-world indicator

Another method to evaluate a node's effect on network robustness is by determining its influence on the network's small-world characteristics. With our targeted attack strategy, we assess the small-world properties of the network following the removal of each node.

To verify if a network has a small-world structure, it needs to be compared with a random network of similar size and density. A network is considered to have small-world characteristics if its average path length [l_G] is similar to that of a random network and its clustering coefficient [$CC_l(G)$] is much greater than that of a random network (Humphries, Gurney, & Prescott, 2006):

$$\frac{l_G}{l_{rd}} \approx 1 \; et \; \frac{CC_l(G)}{CC_l(rd)} \gg 1$$

[7] The size of the largest connected component (LLC) of the network is given by the number of nodes that are directly connected to each other.

Here, l_{rd} and $CC_l(rd)$ stand for a random network's average path length and clustering coefficient, respectively. These equations can be combined to calculate the small-world metric, known as SW:

$$SW = \frac{\frac{cc_l(G)}{CC_l(rd)}}{\frac{l_G}{l_{rd}}}$$

A value of SW greater than 1 indicates the existence of a small-world structure. We start by confirming whether our network exhibits small-world characteristics. After establishing this, we then examine how Huawei's presence affects the small-world score, SW[8]. Given the high sensitivity of the small-world (SW) score to randomness, we conducted 100 simulations to measure it accurately. For both the initial network and for each subsequent node removal, we calculated the average of the SW scores to ensure a reliable analysis.

Network centralization

The final approach in evaluating the effect of node removal on network robustness involves analyzing changes in network centralization. We start by observing the progression of network centralization over time. Next, we evaluate the influence of each individual node on the network centralization.

Freeman (1978) defines network centralization as the degree to which communication is concentrated through a few key members, rather than being uniformly spread across all members. While there are multiple ways to measure network centralization, for our study, we extended the previously mentioned node centrality measures to a broader network context.

Degree centralization assesses how much the network's cohesion is centered around specific pivotal nodes (Bales et al., 2014). In a highly degree-centralized network, a few nodes have many connections, while most others have fewer edges. This indicates that a small fraction of nodes primarily controls the network's interactions. High betweenness centralization implies that a few nodes mainly dictate the network's flow, serving as crucial bridges. Networks with pronounced closeness centralization feature a select group of nodes that can efficiently access all other nodes.

Our analysis will focus on the network's robustness and Huawei's impact on it over time. This will allow us to observe the evolution of Huawei's role and identify any notable patterns that emerged during the period when geopolitical tensions involving Huawei increased. We have segmented the timeline into three-year periods.

Assessing topic robustness

Hierarchical clustering

The next step involved carrying out the hierarchical clustering process on our prepared database. First, we calculated the cosine distance between the TF-IDF weighted terms in our document-term matrix. In the context of text data, this metric effectively captures the semantic similarity between documents.

With the cosine distance matrix in hand, we proceeded to perform hierarchical clustering. The Ward's minimum variance method was employed, with the objective of reducing the overall within-cluster variance.

[8] We acknowledge the sensitivity of the small-world (SW) metric to network size in our study. An alternative size-adjusted metric proposed by Telesford et al. (2011), which involves a latticization algorithm, was considered. However, due to the computational complexity of this approach, we opted for the traditional SW metric. In our analysis, we have carefully considered the impact of network size sensitivity on our findings to ensure accurate interpretation of the results.

The two clusters that have the smallest distance between them at each phase are combined. To facilitate visualization and further analysis, the hierarchical clustering result was then converted into a dendrogram structure.

After obtaining the dendrogram from the hierarchical clustering, a more nuanced approach was adopted to determine the optimal number of clusters. Instead of conventionally cutting the dendrogram at a predetermined height or specifying the number of clusters a priori, an iterative manual parsing was employed to ensure the coherence and relevance of each cluster. Each branch of the dendrogram was meticulously examined. The coherence of a cluster was primarily determined by inspecting the most frequent words within that cluster. If the words collectively suggested a clear and distinct topic, the cluster was deemed coherent. In instances where a branch did not exhibit coherence, it was further split. This division continued iteratively until the resulting sub-clusters were coherent, as evidenced by their most frequent words aligning with a clear topic. Conversely, there were scenarios where two distinct branches, when evaluated separately, seemed to share thematic similarities. In such cases, the two branches were amalgamated to form a single, coherent cluster with a well-defined topic.

This iterative and manual approach to dendrogram parsing ensured that each cluster was contextually meaningful. By prioritizing the semantic coherence of clusters, this method provided a more refined and contextually relevant clustering outcome, tailored to the nuances of the dataset.

After the iterative dendrogram parsing and cluster refinement, the next pivotal step was to assign meaningful labels to each cluster. To ensure the labels accurately represented the content and essence of each cluster, we read the most representative abstracts within them. These representative abstracts were identified by computing the cosine similarity between them and the centroid of their respective clusters. Centroid is the mean of the Tf-IDF frequency scores of documents within the same cluster. By thoroughly reading these abstracts, we were able to discern the predominant themes and topics that characterized each cluster.

With the clusters clearly defined and labeled, we proceeded to analyze the involvement of specific nodes, with a particular focus on Huawei. For each cluster, we identified abstracts that had contributions from Huawei. This allowed us to ascertain the thematic areas and research domains where Huawei had made significant contributions.

Assessing Huawei's effect on clusters robustness

To evaluate Huawei's involvement in each cluster, we approached it in four distinct ways. First, we measured Huawei's research priorities by determining the proportion of their projects within each cluster (RP score):

$$RP = \frac{Number\ of\ Huawei's\ projects\ in\ the\ Cluster\ k}{Total\ number\ of\ Huawei'sprojects}$$

In other words, the RP score is the distribution of Huawei's projects across different clusters. Next, we computed the share of Huawei's projects relative to the total projects in each cluster (RI score):

$$RI = \frac{Number\ of\ Huawei'sprojects\ in\ the\ Cluster\ k}{Total\ number\ of\ projects\ in\ the\ Cluster\ k}$$

Also, we assessed Huawei's contribution to the uniqueness of each cluster in comparison to others (RS score). Finally, we constructed a network that includes both academics, partners, and topics as nodes, and then measured the impact of Huawei's removal on the centrality of these topic nodes.

First, to assess Huawei's contribution to the uniqueness of the clusters, we start by conducting a keyness analysis[9] (Bondi & Scott, 2010) to identify terms that are uniquely prevalent within a cluster when compared to others. This was achieved through the application of the Chi-square test, which allowed us to statistically determine whether the frequency of certain terms in a cluster was significantly different from their distribution across other clusters (Durán-Muñoz, 2019). To ensure the robustness of our specificity analysis, we further refined our results by considering only those terms that met a statistical significance threshold. Specifically, only words with a p-value smaller than 0.01 were retained, ensuring that the terms we highlighted were statistically significant. Finally, for each cluster we extracted the most specific words and their Chi-square scores that we named α in the equation below. Subsequently, for each cluster, we quantified the extent to which Huawei's project terms contributed to the terms that are distinctive to that cluster using the following equation:

$$RS_k = \frac{\sum(\alpha_k * PH_k)}{\sum(\alpha_k * PT_k)}$$

α is defined as a collection of chi-squared statistics that correspond to specific words within each cluster k; PH represents the sum of normalized frequencies of the words in α for cluster k for Huawei's documents in k, and PT is the total sum of normalized frequencies for all words in α across documents belonging to cluster k.

Second, we use the attack strategy typically used for assessing network robustness to instead measure the effects on specific nodes. In this context, we are focusing on the impact on individual nodes within the network. Our aim is to evaluate whether Canada risks losing research contribution in certain topics if the network faces targeted attacks.

We constructed a Canadian 5G research network integrating academics, researchers, and previously identified clusters (topics) as its nodes. With this framework set, our primary focus was to evaluate the robustness of the network in terms or research contribution (topics) considering Huawei's potential absence. Our strategy was to measure the impact of Huawei's removal on these nodes and then compare this effect against the impact of removing any other player in the Canadian ecosystem, particularly Ericsson.

We employed a simulation-based approach with a targeted attack strategy to measure the robustness and vulnerability of cluster nodes. We removed each node from the network, ensuring that nodes exclusively collaborating with the removed node were also eliminated. After each removal, we recalibrated the centrality measures of the cluster nodes. We use the same centrality measures we described earlier. Through this approach, we aimed to identify which cluster nodes were particularly robust to nodes removal (i.e., Huawei's removal) based on changes in their centrality measures after each node removal.

Results

NSERC 5G collaborative projects

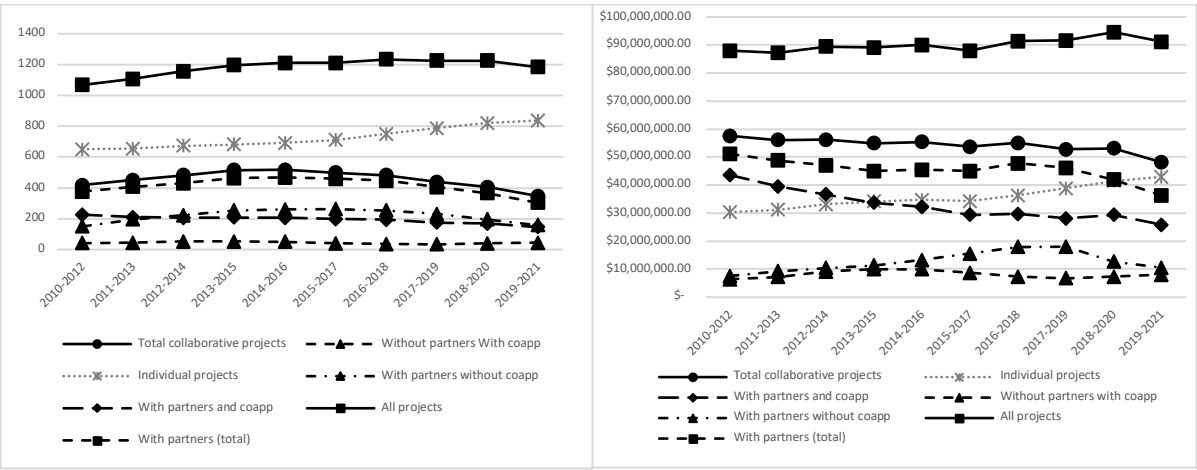
For a comprehensive understanding of our network landscape, we categorized the NSERC collaborative projects into two main groups: those with partners (both with and without co-applicants) and those without partners. Various types of organizations partner with academics on those grants: research institutions, private sector companies, non-profit organizations, and governmental agencies. Industrial partners, constitute the bulk (over 83%) of the partners in our 5G database. From Fig.2.a, a discernible trend emerges[10]: while the

[9] The R package "quanteda" and the function textstat_keyness() were used to carry out the keyness analysis (Benoit et al., 2018).

[10] The amounts provided in the NSERC data are presented in current Canadian dollars.

total number of yearly instalments remained relatively stable after increasing until 2014-2016, those associated with collaborative projects (with co-applicants and/or partners) followed the same trend until the 2014-2016 period, after which the number has declined steadily.

Correspondingly, the overall budget allocated to collaborative projects (Fig. 2.b) has declined over the period, mainly due to a displacement between projects with co-applicants and partners towards projects involving only partners[11], but only up to 2017-2019. The decline in the most recent period is evident. More specifically, the budget for collaborative projects with partners has seen a substantial reduction, dropping from $46 million during 2017-2019 to $36 million in the 2019-2021 period.



(a) **(b)**

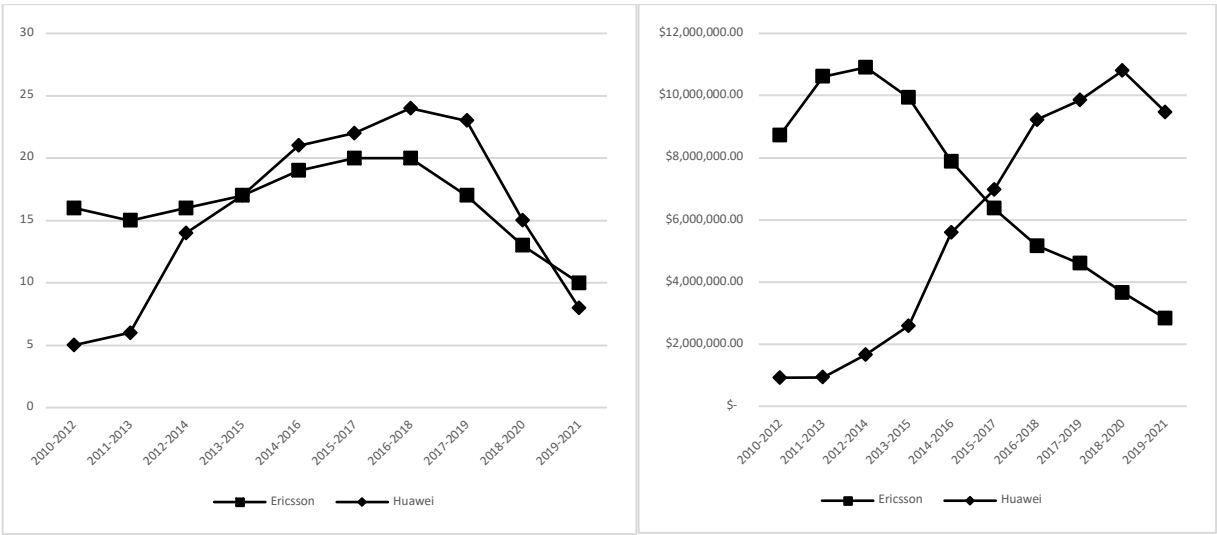
Fig. 2 Evolution of **a** the number of NSERC instalments and **b** the grant amounts in Canadian dollars (CAD)

This decline can be attributed to multiple factors. One plausible explanation is the maturation of 5G research, suggesting that as the technology matured, there might have been fewer collaborative projects initiated. Fig. 1 illustrates a clear trend: while the number and budget of collaborative projects with industrial partners are declining, individual project numbers and budgets are on the rise. This divergence suggests that the research field itself remains vibrant and growing, as evidenced by the sustained increase in the number of scientific publications and patents (Mao, 2021; Zhang, Wong, & Chang, 2021; Mendonça et al., 2022) during the same period when collaborative efforts declined. The observed decline in collaborations with partners in 5G projects could also be explained by the introduction of new funding programs within Canada. One significant development is the establishment of ENCQOR 5G[12] in 2017, a consortium that includes several firms, most notably Ericsson, a key competitor of Huawei in the country. This consortium is a public-private partnership dedicated to fostering research and collaboration opportunities in the realm of 5G technology.

Also, this timeframe aligns with heightened geopolitical tensions surrounding 5G and a deteriorating environment in the scientific community regarding collaborations with specific firms. To further understand the implications of this shift, we will delve into the trends of Huawei's projects. Fig. 3 displays the evolution of the number and budget of projects in which Huawei and its main competitor, Ericsson, are named partners. Fig. 3.a seems to suggest that the involvement of both Huawei and Ericsson slowly diminishes

[11] This can be attributed to the predominant presence of the Engage program grants (49%). The Engage program, designed for short-term collaborations spanning six months, aims to catalyze partnerships between academics and partners who have not jointly applied for a grant previously.
[12] https://quebec.encqor.ca/

after 2016-2018. As mentioned before, after that period, Ericsson becomes involved in a large, coordinated entity called ENCQOR 5G, and its participation both in terms of numbers and grant amounts of projects dwindles away. Fig. 3.b shows that the budget allocated to projects involving Huawei follows an upward trend over time, yet there is a noticeable decrease during the last period, 2019-2021.The decline in collaborations with Huawei can be attributed to the increasing apprehensions within the academic community about engaging with the company, concerns which ultimately culminated in the establishment of guidelines such as those introduced by the Natural Sciences and Engineering Research Council of Canada (NSERC) in July 2021 (Fife & Chase, 2021).

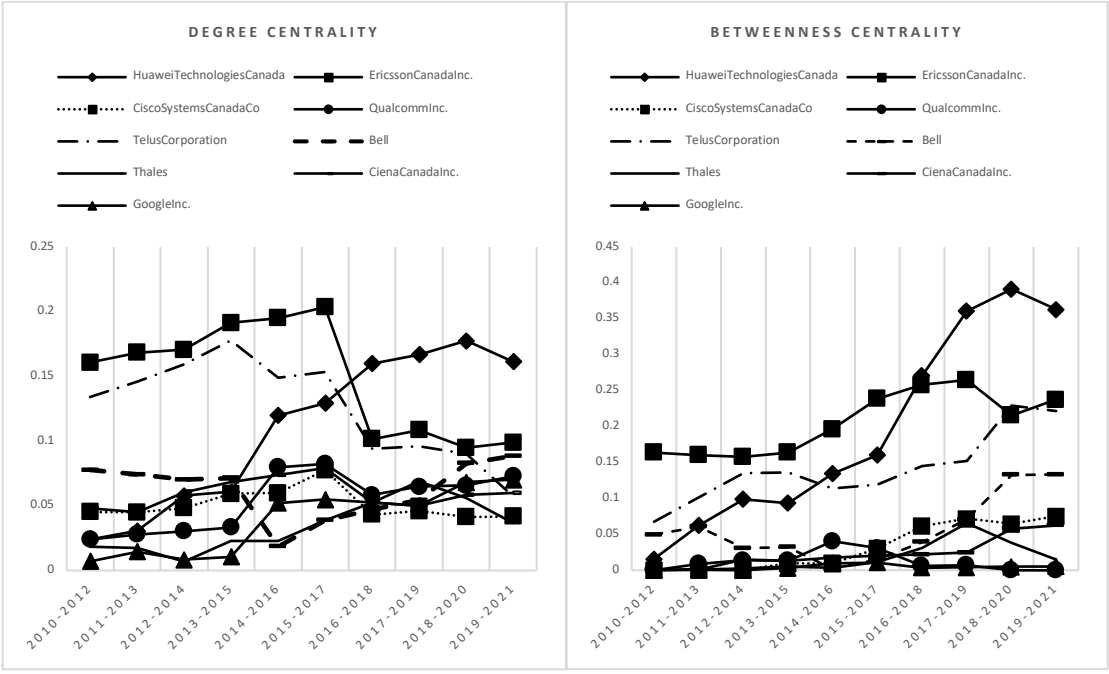


(a) **(b)**

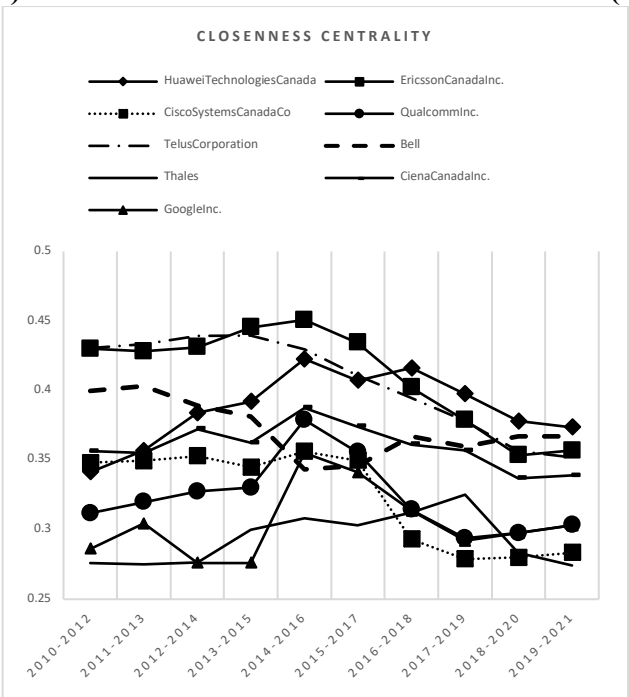
Fig. 3 Evolution of **a** the number of projects and **b** the grant amounts of the projects in which Huawei and Ericsson are involved

Centrality dynamics of industrial partners in NSERC 5G network

Central nodes often play a critical role in the network's robustness. Three centrality measures are tracked over time: degree centrality, betweenness centrality, and closeness centrality. The results, showing the most central industrial partners over the years, are presented in Fig. 4.



(a) **(b)**



(c)

Fig. 4 Degree **a**, betweenness **b**, and closeness **c** centrality measures for most central industrial partners

Huawei, Ericsson, and TELUS [13]emerge as the most central industrial partners over time. Ericsson relinquished its top position to Huawei during the 2016-2018 period across all three metrics. Specifically, in the subsequent four timeframes, Huawei not only established the most connections with other entities (as

[13] Telus is a major telecommunication company in Canada: https://www.telus.com/en.

indicated by degree centrality) but also emerged as a pivotal bridge linking various academics and companies (highlighted by betweenness centrality). Furthermore, Huawei surpassing Ericsson in closeness centrality indicates that Huawei is, on average, closer to all other nodes in the network, enhancing its accessibility and influence within the collaborative network. This shift in centrality dynamics occurred amidst heightened government scrutiny on Huawei. During this specific period, Canadian academics continued to receive NSERC funding for partnerships with Huawei as we previously showed in Fig. 3.b.

Robustness of the NSERC 5G network

Measuring R and LCC size

Fig. 5 shows that the NSERC 5G network exhibits strong initial connectivity. The largest connected component consistently encompasses over 80% of the nodes in the network across different time periods and stays strongly connected in the last two periods (63% in the last period). Such a high proportion suggests a well-integrated network.

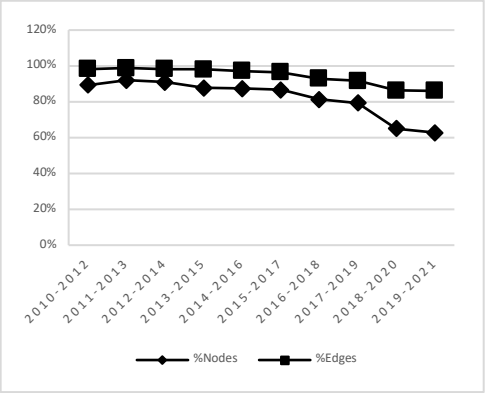


Fig. 5 Evolution of the largest connected component (LLC)

To delve deeper into the network's robustness and its ability to withstand targeted disruptions, let us examine the evolution of R over time. Two key observations emerge regarding the robustness of our network (see Fig. 6). First, the R value is consistently low. Throughout the observed periods, it remains below 0.2, far below the maximum threshold of 0.5, indicating inherent vulnerabilities in the network's structure. Secondly, beyond the low scores, there's a clear downward trajectory in the R value. By the 2019-2021 period, it reaches a mere 0.05. Such a value, nearing zero, underscores a pronounced vulnerability in the network's robustness, which seems to be intensifying over time. This diminishing robustness implies that our network is increasingly vulnerable to targeted disruptions. Specifically, if strategies focus on eliminating the most central nodes, the network experiences swift fragmentation. This rapid disintegration of the largest connected component upon removal of pivotal nodes is illustrated in Fig. 7.

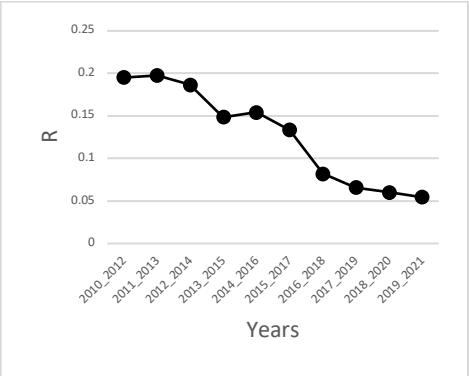


Fig. 6 Evolution of the robustness measure R

During the initial three periods, the network becomes disconnected after the removal of approximately 25% of its central nodes (see Fig. 7). This vulnerability intensifies in the subsequent periods, where a mere removal of less than 10% of the nodes leads to graph disconnection. These observations clearly show that the network is not robust, and its robustness is diminishing over time. Moreover, the network exhibited signs of declining robustness prior to the escalation of geopolitical concerns regarding Huawei and the 5G technology.

The observed decline in the R value and the swift decomposition of LCC after the removal of only a small fraction of the most central nodes intriguingly coincide with Huawei's ascent to a high centrality position in the 5G network. To definitively ascertain whether Huawei plays a pivotal role in this dynamic, we assess the impact on the LCC when Huawei is specifically removed from the network and juxtapose this effect with the consequences of removing other central nodes. To provide a comparative perspective, we also included the effects of removing Ericsson, another central node in the network. The results of this analysis are presented in Fig. 8.

A multifaceted trend about the influence of Huawei's removal is apparent on the LCC over time. Throughout the observed periods, the repercussions of Huawei's removal remain relatively low, reaching a maximum of 6% during 2019-2021. An intriguing pattern emerges between 2010-2012 and 2013-2015. Despite Huawei's less central position in the network compared to other entities, its extraction leads to a more pronounced contraction in the LCC. This phenomenon can be traced back to the methodology of node removal, where a node's exclusive collaborators are also removed. Huawei had more unique partners that only worked with it. On the other hand, Ericsson, even with its strong position during this period, had fewer unique partners, leading to a smaller impact when it was removed.

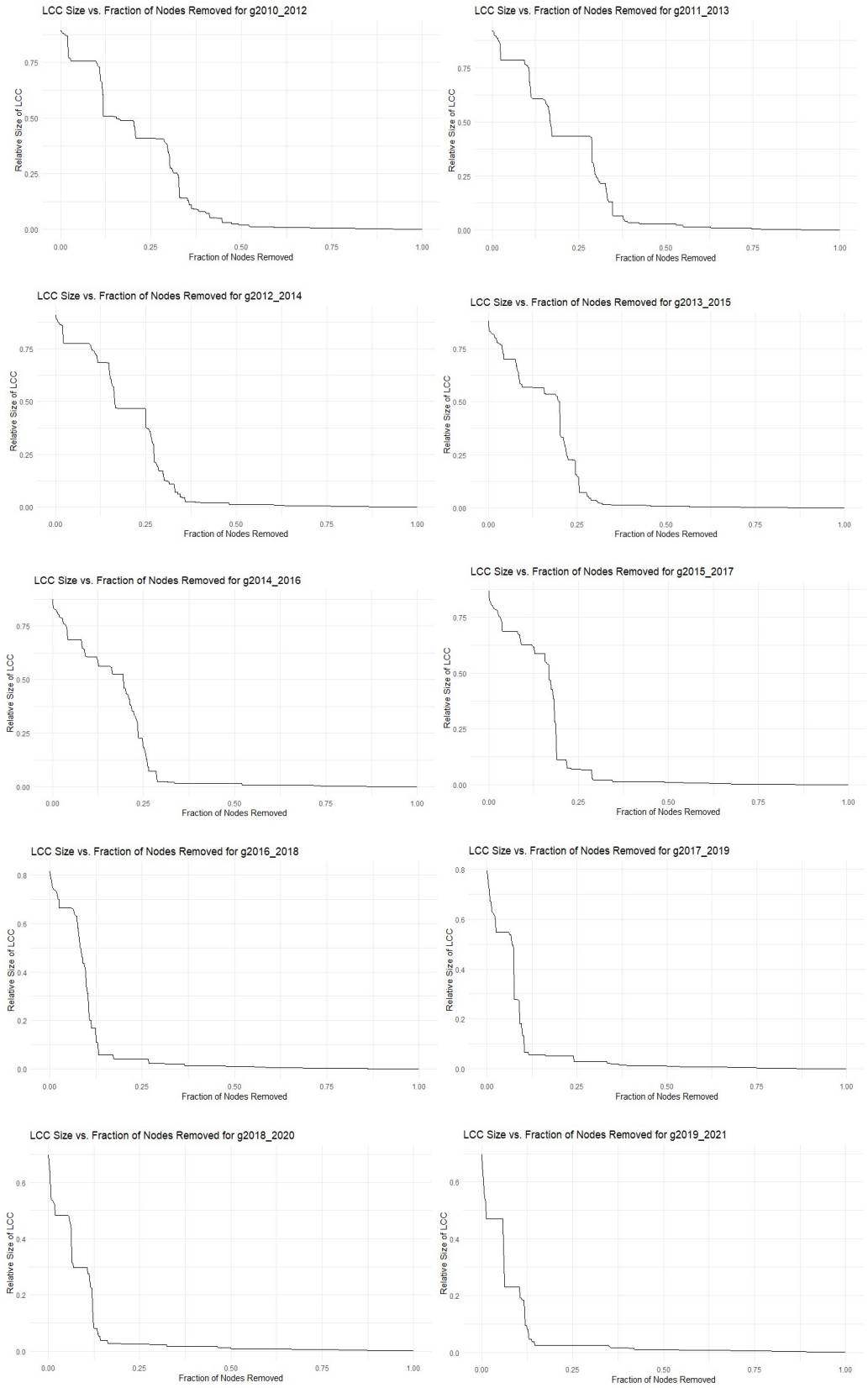


Fig. 7 LCC size vs Fraction of nodes removed

The story changes between 2013-2015 and 2014-2016, where the impact of Huawei's removal decreases, coinciding with Ericsson's strong presence in the network. After 2014-2016, as the importance of Huawei grows and becomes more central in the network, the impact of its removal on the LCC starts to increase, even more so than in the initial phase. Although the company was among the industrial partners with a higher impact score on the LCC, the magnitude of this impact was comparable to other major players in the field. This observation implies that Huawei doesn't have a unique or dominant role in influencing the robustness of the network and its impact stays relatively minor over time.

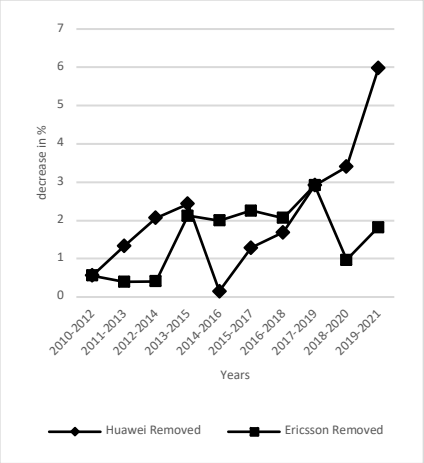


Fig. 8 Impact of the removal of Huawei and Ericsson on LCC Trends

Small-world properties

As the size of the LCC is a rather crude measure, this article proposes to explore the impact of targeted attacks on the small-world properties of the network. Table 1 shows that the network exhibits a small-world structure in every period, with the SW score being consistently greater than 1, which represents an optimal structure for knowledge and information flow, which is particularly crucial in the context of a research collaboration network. In our case, despite the decreasing size of the network over time, the small-world (SW) score remains relatively stable, indicating consistent small-world characteristics irrespective of network size changes.

Table 1 Small-World score

	NUMBER OF NODES	SW SCORE
2010-2012	710	19.3
2011-2013	755	20.8
2012-2014	728	19.5
2013-2015	659	24
2014-2016	652	23.2
2015-2017	620	25
2016-2018	532	27.9
2017-2019	480	23.6
2018-2020	412	18.4
2019-2021	385	23.2

Table 2 presents the influence of both Huawei and Ericsson on the network's small-world properties. A key observation is that, upon the removal of either Huawei or Ericsson, the network retains its small-world characteristics, as evidenced by the SW score consistently remaining above 1.

Table 2 Impact of Huawei and Ericsson Removal on SW

		SW Score after removing		Impact (%) of removing	
	Initial SW score	**Huawei**	**Ericsson**	**Huawei**	**Ericsson**
2010-2012	18.9	18.8	18.7	-0.8%	-1.0%
2011-2013	20.5	20.1	20.7	-2.3%	1.0%
2012-2014	20.3	19.7	20.6	-3.0%	1.4%
2013-2015	22.4	21.7	22.5	-3.0%	0.7%
2014-2016	23.8	24.1	23.6	0.9%	-0.9%
2015-2017	24.5	24.0	24.2	-2.4%	-1.3%
2016-2018	29.2	29.5	27.9	0.9%	-4.8%
2017-2019	26.8	25.9	25.8	-3.4%	-3.7%
2018-2020	22.3	21.0	21.6	-5.7%	-3.0%
2019-2021	21.3	20.8	20.5	-2.5%	-4.0%

The results presented in Table 2 indicate that the removal of Huawei does not substantially affect the small-world score of the network. While there is a minor decrease in the small-world score for nearly all observed periods, the overall impact is relatively minor. This suggests that Huawei, despite its central position in the network, is not a crucial dependency for most nodes. A similar pattern is observed when Ericsson is removed from the network, indicating that its absence also does not significantly impact the network's small-world score. The majority of nodes in the network seem to be well interconnected independently of both Huawei and Ericsson. This can be explained by the minimal changes in both the clustering coefficient and the average path length.

Upon comparing the impact of Huawei's removal with the effects of removing other nodes across each time period, our findings reveal that Huawei does not rank among the top nodes influencing the small-world score. In fact, several other industrial partners exhibit a more pronounced effect on the network's small-world properties than Huawei does.

Network centralization

Prior to the removal of Huawei and its subsequent impact analysis on network centralization, two distinct patterns emerged in the network's centralization trends over time. Firstly, the trends for degree and closeness centralization differ notably from that of betweenness centralization. Specifically, during the initial periods, both degree and closeness centralization exhibit an upward trajectory, only to follow a declining trend in the subsequent periods. Fig.9.a shows a clear drop in degree centralization over time. This means that connections in the network are spreading out more evenly among nodes, rather than just a few nodes having most of the connections.

Contrastingly, when we examine betweenness centralization, its trajectory is opposite to that of degree and closeness centralization (see Fig. 9.b). Initially, there's a decline in betweenness centralization during the early periods, but this trend reverses, showing an increase in subsequent periods.

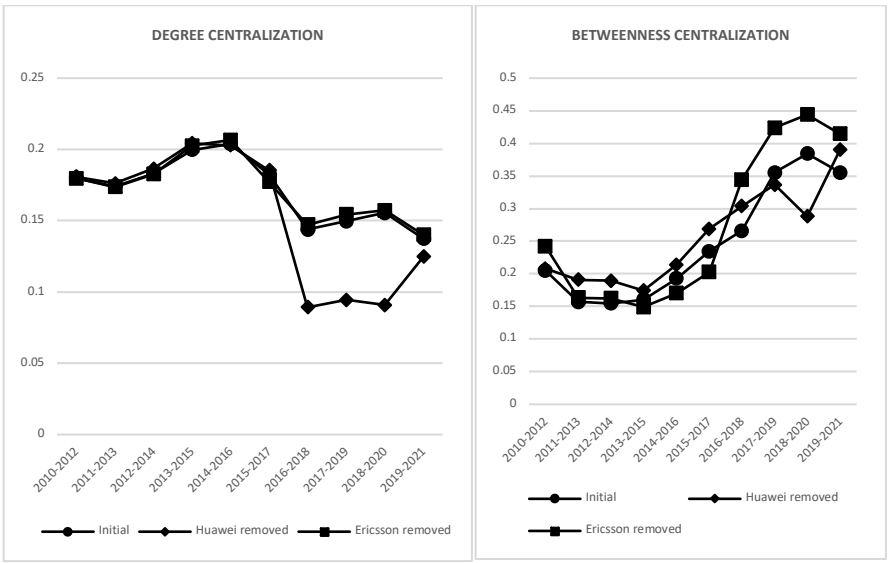
The decline in degree centralization, as depicted in Fig. 9.a, not only corresponds with a reduction in the overall number of nodes in the network (see Table 1), but we also verified that some nodes, which were previously central, have either disappeared from the network or now possess fewer connections during this period of decreasing centralization. Concurrently, some nodes are emerging as critical bridges, connecting different parts of the network, which results in an increase in betweenness centralization. These shifts in node importance and the evolving network structure suggest that the network's overall robustness is on the decline.

Degree, betweenness and closeness (network) centralization measures offer a deeper understanding of the robustness of the network, as represented by the R value over time (see Fig. 6). While connections are well distributed between nodes, the network structure is becoming heavily dependent on a few key nodes. The removal of these pivotal nodes compromised the entire network, leading to a decrease in its robustness (R).

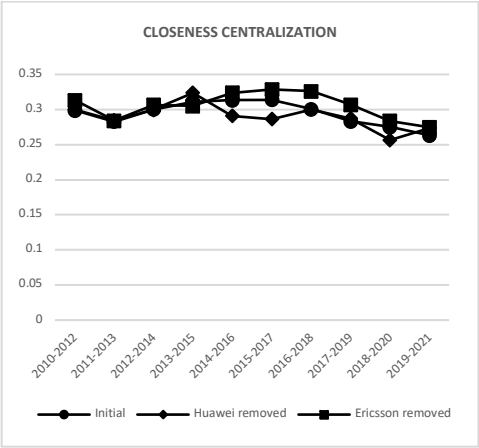
The removal of either Huawei or Ericsson from the network (in Fig. 9.b and Fig. 9.c) does not significantly alter the initial closeness and betweenness centralization values, suggesting that neither organization plays an overwhelmingly pivotal role in the network's structure. The overall network dynamics and interconnections remain largely consistent, even when either of these major players is excluded from the equation.

These results are a stark contrast to what we observe with degree centralization. In that case, Huawei's influence becomes more pronounced, especially post the 2015-2017 period. Its removal from the network during these later periods leads to a noticeable decrease in degree centralization. This suggests that Huawei had established itself as a significant node with numerous direct connections within the network. While several nodes displayed a decreasing trend in their degree centrality, as illustrated in Fig. 4.a, Huawei's degree centrality was on the rise. This suggests that while some nodes were losing their direct connections or becoming less central in terms of immediate ties, Huawei was expanding its direct collaborations, further solidifying its position as a major hub within the network.

We found that Huawei's removal had the most noticeable effect when evaluating the effects of removing other nodes on degree centralization during the last period. Even while Huawei is a vital link in the network, the trend toward less centralization remains unchanged when it is removed, indicating that it is not the sole driver of this trend. However, the more pronounced decrease in degree centralization upon its removal underscores Huawei's role as an important node with extensive connections. This suggests that while Huawei contributes quantitatively to the network's centralization, it does not fundamentally change the network's overall structural shift towards decentralization.



(a) **(b)**



(c)

Fig.9 Impact of the removal of Huawei and Ericsson on **a** degree, **b** betweenness and **c** closeness centralization

Key 5G topics

From a science policy point of view, it is relevant to examine whether the removal of one player in the network, here Huawei, creates a void of topics on which university and industry normally work hand in hand. In other words, observing various network characteristics changes following targeted attacks only tell part of the story. Firstly, we will employ a hierarchical clustering approach to identify distinct topics. Once the topics are identified, we will then proceed to analyze Huawei's contributions within each topic. Understanding Huawei's contribution to specific topics, requires a three-fold investigation: 1) assessing Huawei's research priorities (RP score); 2) examining Huawei's involvement in terms of projects within these research topics (RI score); and 3) measuring Huawei's contribution to the uniqueness of these topics (RS score).

A hierarchical clustering algorithm on 5G projects summaries from the NSERC database found 67 unique clusters (see Table 5 of Appendix 1), each representing different 5G subtopics in Canada. Some of these include subtopics on the core technologies integral to 5G. The main topics associated with these clusters of projects highlight advancements and challenges in areas such as MIMO, millimeter-wave frequencies, edge computing, and innovations in both silicon and optical technologies. For instance, the integration of 5G with the Internet of Things (IoT) emerged as a significant theme, showcasing the potential of 5G to elevate and transform IoT applications. Security in the 5G framework was another main theme among the clusters, highlighting the focus on data privacy and creating secure 5G protocols. Another discernible theme revolved around energy management within the 5G infrastructure, emphasizing the balance between the capabilities of 5G and its energy demands. Furthermore, the results highlighted the application of 5G in interdisciplinary research areas, particularly its potential implications in sectors like health and aerospace.

Huawei's research priorities (RP score) within the 5G domain exhibit a pronounced concentration in Cluster 1, which focuses on silicon and optical photonic technologies (see Table 3): 32.08% of the research projects in which Huawei is involved align with this theme. Of lesser importance, Cluster 17, centered around MIMO technology, and Cluster 30, dedicated to network management and optimization, each capture 7.5% of Huawei's research collaboration. These percentages, although substantial, are far behind the overwhelming focus on silicon and optical photonic technologies (C1), indicating a primary research direction for the company in this domain. Conversely, Ericsson shows a more distributed research priorities approach across the various topics identified (see Table 3). While some clusters capture a notable proportion of Ericsson's research priorities, such as C21, which delves into edge and cloud computing (11.5%), and C30-Resource management for next-generation wireless networks, C12- Optimization and management in next-generation

small cell cellular networks and C13- Innovative strategies for massive data traffic and low latency in 5G networks, centered on network management and optimization (with contributions of 9.8% and 6.6% respectively), the company's contributions span a broader spectrum of research topics, hence suggesting a multifaceted research strategy.

Table 3 Research priorities of Huawei and Ericsson

Cluster number	Huawei research priorities	Ericsson research priorities	Title
1	32.0%	4.9%	Advancements in silicon photonics and optical communication systems
12	3.7%	6.6%	Optimization and management in next-generation small cell cellular network
13	5.6%	6.6%	Innovative strategies for massive data traffic and low latency in 5G networks.
17	7.5%	4.9%	Advancements and challenges in MIMO and 5G wireless communication technologies
21	1.8%	11.5%	Cloud computing, resource management, and privacy in Fog Networks
30	7.5%	9.8%	Resource management for next-generation wireless networks

Note: The percentages in this table represent the Research Priorities (RP) scores for Huawei and Ericsson. These scores are calculated by dividing the total number of projects each company has in each cluster by the total number of projects conducted by the respective company.

Fig. 10 emphasizes Huawei's role as a leading contributor in C1, which focuses on advancements in silicon photonics and optical communication systems. Here, the RI score 16.83%, reflects the proportion of Huawei's projects in this cluster relative to the total number of projects present in the same cluster. On the other hand, the RS score 17.51%, is a percentage that serves as a measure of Huawei's contribution to the distinct characteristics that make this cluster specific compared to others. It highlights how Huawei's projects contribute uniquely to the specific themes and topics of C1, surpassing all other entities. This data reinforces Huawei's significant commitment and leadership in the research areas encapsulated by C1.

However, beyond Cluster 1 where Huawei demonstrates a significant impact, the company does not particularly stand out in terms of contributing to the volume or specificity of other clusters when compared to other companies. In C17, which focuses on 5G innovations such as massive MIMO, mm wave communication, and wireless backhaul solutions, both Huawei and Ericsson significantly contribute to the cluster's uniqueness. Huawei is the leading contributor with 18.18% of the projects in this cluster (RI score), and its contribution to the cluster's uniqueness is substantial, at a 19.04% of RS score. Ericsson, with a slightly smaller share of projects at 13.64%, closely matches Huawei's contribution to the cluster's distinctiveness with 17.15% in RS score. This highlights that despite having fewer projects, Ericsson's projects are nearly as impactful as Huawei's in defining the unique characteristics of C17.

Similarly, in C30, which focuses on resource management for next-generation wireless networks, the analysis in terms of specificity (RS) reveals a more significant role for Ericsson compared to Huawei. Ericsson contributes a substantial 25.99% to the cluster's specificity, underscoring its considerable involvement in the research topics of this cluster. This high contribution rate indicates that Ericsson's projects are not just numerous but also play a defining role in shaping the unique characteristics of Cluster 30. Also, in C13-Innovative strategies for massive data traffic and low latency in 5G networks, Ericsson not only has a larger share of projects in this key area but also exerts a stronger impact on the cluster's distinctiveness compared to Huawei.

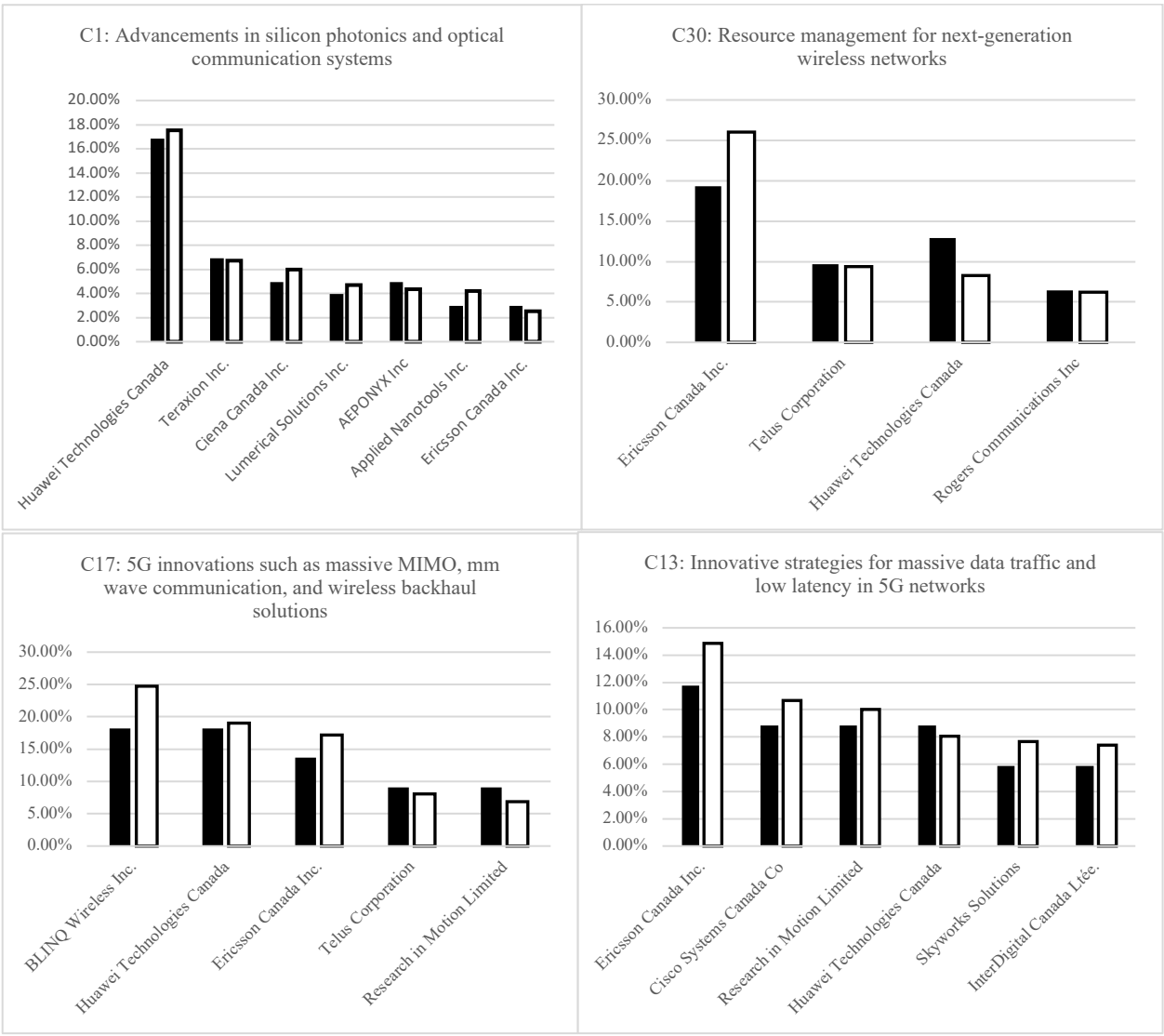


Fig. 10 Contribution of Huawei and Ericsson in terms of project volume in the cluster (black) and on lexical specificity of clusters (white)

To sum up, Huawei differentiates itself from Ericsson and other industrial partners primarily in terms of silicon and optical photonic technologies (C1). This is evident in their research priorities, their role in populating this topic, and their significant contribution to the topic's uniqueness.

To gain a deeper understanding of Huawei's influence within the 5G research topics landscape, we will conduct a simulation that entails the hypothetical removal of Huawei from the network. This approach will allow us to analyze and quantify the impact of Huawei's absence on the 5G research topics. We add to the previously characterized network a new set of nodes that correspond to each of the 67 topics identified in Table 5 of Appendix 1. Then, we replicate the targeted attack approach to evaluate the robustness of this new 5G collaboration-topic network. The results presented below highlight the effects of a targeted attack strategy on the centrality measure of these topic nodes. When we specifically focus on the removal of Huawei, we identify some interesting observations related to certain clusters (see heatmaps of Huawei and Ericsson in Fig. 11 and Fig. 12 of Appendix 1).

When Huawei is removed from the collaboration-topic network, three notable shifts occur in the dynamics surrounding C1-silicon and optical photonic technologies. First, there is a 7% reduction in degree centrality, highlighting Huawei's direct collaborations and ties to this topic. When comparing the effects of removing Huawei from Cluster 1 with the effects of removing other industrial partners, it reveals that the impact of Huawei's absence is the greatest, showing its significant influence within this cluster in term of direct connections. However, unlike the significant lead of Huawei in RI and RS scores within Cluster 1, the gap in terms of degree centrality is less pronounced. Here, Teraxion Inc[14] emerges as a close second, with its impact on the degree centrality of C1 being 4.21%.

Second, the betweenness centrality of silicon and optical photonic technologies (C1) increases by 5.88%. Despite Huawei's absence from the collaboration-topic network, the increased betweenness centrality of C1 suggests that the network retains strong collaborative and informational flows in this area. This change demonstrates the network's robustness, showing that its functionality and contributions to C1 do not overly depend on Huawei. This dynamic is not unique to this topic. Similar patterns emerge for the following topics: Implementation and application of polar and LDPC codes in 5G wireless communication systems (C11), Optimization and management in next-generation small cell cellular networks (C12), Innovative strategies for massive data traffic and low latency in 5G networks (C13), 5G innovations: massive MIMO, mm wave communication, and wireless backhaul solutions (C17), Data center networking and optimization (C29), Resource management for next-generation wireless networks (C30).

Third, compared with Ericsson, the decrease in C1's degree centrality is relatively modest, only 1.05%, which is substantially less than the impact seen with Huawei's removal. However, in terms of betweenness centrality, Ericsson's removal results in a more notable increase of 6.10%, exceeding the impacts observed when Huawei was removed from the network. When comparing the impact of Huawei's removal with that of other companies, it becomes evident that Huawei does not exert the greatest influence on Cluster 1's betweenness centrality. For instance, IBM Canada surpasses both Huawei and Ericsson, with its removal leading to an even more significant impact of 10.52% on the betweenness centrality of C1. This suggest that even in the absence of these large players, the collaboration-topic network exhibits a high degree of robustness, i.e. Canada does not lose out in terms of research contribution to these topics.

Another research priority (C29 – Data center networking and optimization) of Huawei compared to Ericsson presents distinct patterns when either Huawei or Ericsson is removed. Huawei's removal results in a 13% decline in degree centrality of the topic, highlighting its substantial direct involvement with this topic. In contrast, Ericsson's removal leads to a smaller 6% decrease. Once again, the dynamics shift when considering betweenness centrality. Despite Huawei's stronger direct ties, its removal only increases the betweenness centrality of Data center networking and optimization (C29) by 8%. Conversely, the absence of Ericsson, with its fewer direct connections, results in a significant 16% drop in betweenness centrality of the topic. In practical terms, Huawei and the research topic (C29 – Data center networking and optimization) appear interchangeable in terms of their intermediary role in the collaboration-topic network, i.e. there is a high degree of robustness to the removal of Huawei (the topic occupies the void). The absence of Ericsson as a key integrator and intermediary of the network leaves a more fragmented collaboration-topic network, it has a greater impact on the network than the removal of any other industrial partner.

Huawei's removal yields a negligible impact on closeness centrality across various topics. This further suggests a high degree of redundancy in the connections within the research collaboration-topic network. Specifically, even in the absence of Huawei, multiple paths connecting these topics to other industrial partners and academics exist in the network. As a result, the average distance between nodes remains

[14] Teraxion Inc is a company specialized in photonic solutions.

relatively consistent, indicating that other nodes in the network effectively compensate for Huawei's absence.

Conclusion

The purpose of this paper is to explore the impact of geopolitical tensions on 5G technology research, with a particular focus on Huawei's role in Canadian academia. Amidst growing concerns about Huawei's involvement, we assess the robustness of Canada's 5G research network in response to growing geopolitical tensions related to Huawei. To achieve this objective, our evaluation focused on the robustness of two distinct networks: firstly, the business-academic network, and secondly, the collaboration-topics network.

In analyzing the business-academic network, we found that its robustness is low and decreasing over time. This means that the Canadian 5G research network is notably vulnerable to disruptions, especially when its key firms, the network's most central nodes, are targeted. These firms are essential in maintaining the network's structure, highlighting their irreplaceable role and the network's significant dependence on them. However, the dynamics shift when assessing the impact of Huawei alone on network robustness. By simulating geopolitical scenarios through the exclusion of Huawei, our analysis demonstrates that the network effectively endures this targeted disruption, thereby underscoring its sustained robustness even in the absence of Huawei's involvement.

First, our analysis reveals that the network retains its robustness, particularly in terms of its small-world properties, even when Huawei is removed. Despite Huawei being identified as the most central node, its exclusion has a minimal impact on these small-world characteristics. The network continues to maintain an optimal structure for knowledge diffusion within the Canadian 5G business-academic network. Second, the network maintains its robustness in terms of centralization even after the removal of Huawei, despite it being the most central node. Network centralization, which measures how much a network's activities are dominated by a few central players in the network, appears minimally affected by Huawei's absence. While its removal does lead to a slight decrease in centralization (in term of degree centrality), reflecting Huawei's role as a central hub, this change is consistent with the already observed decreasing trend in the network's centralization. Therefore, the ongoing shift towards a more distributed network structure seems to be occurring independently of Huawei's specific contribution.

These results imply that the structural properties of the network remain robust even without Huawei, indicating that Canada's research network does not depend solely on Huawei for optimal knowledge dissemination. Other players within the network can fill this gap, ensuring a continuous and effective flow of information.

In analyzing the robustness of the collaboration-topic network, especially in terms of research contributions to various 5G topics, we observed that the network consistently exhibits a high level of robustness, even in the absence of Huawei. These topics were identified by applying hierarchical clustering to summaries of NSERC projects. Our findings indicate that Huawei has specifically focused on silicon and optical photonic technologies (C1) in Canada, as evidenced by a large proportion of their projects being concentrated in this topic. Additionally, our analysis reveals that Huawei is the leading contributor to C1 in aspects of this topic that are unique to this cluster compared to others. This suggests that this topic is a primary research focus for Huawei within the Canadian context. However, when simulating Huawei's absence from the collaboration-topic network, we observed that even though the topic of silicon and optical photonic technologies loses direct connections due to Huawei's significant contributions, it remains robust. This is evidenced by the minor impact on the topic's degree centrality and a slight increase in its betweenness centrality, indicating robustness to such a disruption. Furthermore, this pattern of high robustness in the face of Huawei's removal is consistent across other topics within the network. Moreover, upon comparing the

impact of Huawei's removal on network robustness with the removal of other firms, we found that Huawei's absence does not stand out significantly. This suggests that the research network's topic-based robustness is not dependent on Huawei, indicating a broader robustness and diversity in contributions from various firms.

This study reveals that Canada's research ecosystem is robust and does not rely on a single player. Knowledge is transmitted between researchers and industry via multiple relationships. The majority of researchers maintain links with several players, ensuring the strength of the network even in the absence of a key player such as Huawei, whether in terms of knowledge transmission or contribution to 5G research. The study also shows that the robustness of this ecosystem can help policymakers assess the impact of geopolitical tensions on scientific collaboration and prevent these effects by promoting the construction of a robust research network.

There are some limitations on this study. First, one limitation pertains to the data extraction process. Since we extracted data from the MITACS and NSERC databases and extracted 5G publications from the Web of Science database, it's possible that some 5G projects were missed. A deeper involvement from experts could help future research incorporate more specific and pertinent keywords to identify 5G projects more precisely, thereby enhancing the accuracy and relevance of the selected articles. In addition, by excluding French abstracts due to our methodology's constraints in handling multilingual data we have deliberately limited our data. Future studies could employ a multilingual approach and compare their findings with ours to potentially enhance the comprehensiveness and applicability of the results.

Moreover, details regarding the technological and financial contributions made by industry partners to the 5G projects are not available in the NSERC database. The information is limited to funds from NSERC and does not include information about resources that the companies contributed in exchange. Future research could address this restriction by doing a thorough qualitative study that would yield more in-depth details on this aspect. Furthermore, in order to evaluate the strength of the Canadian research network, our analysis relied only on the NSERC funding network. Other databases that include patents, scientific articles, and other pertinent documents, could be incorporated into future studies to provide a more comprehensive analysis. One other limitation is the labeling procedure that is used after hierarchical clustering to identify each cluster. Although we read and interpreted the most representative documents of each cluster, some sub-themes may have been lost.

Also, in text mining techniques like hierarchical clustering, it is usually advisable to focus on particular parts of speech, as they are more likely to hold the substantive content of the text. The selection of words may also be tailored based on the objectives of the study and the characteristics of the corpus, depending on the task and the corpus involved. In our study, we chose to retain only nouns and adjectives to extract the most pertinent information regarding 5G topics. Future studies could include additional parts of speech (e.g., verbs) to determine whether the results regarding the impact of Huawei's removal from the studied networks remain consistent.

Reference

Azad, S. (2022). The West and the East on the Lookout: Tracking a Tangled Web of Sanctions-Busting. In East Asia and Iran Sanctions: Assistance, Abandonment, and Everything in Between (pp. 215-229). Cham: Springer International Publishing.

Bales, M. E., Dine, D. C., Merrill, J. A., Johnson, S. B., Bakken, S., & Weng, C. (2014). Associating co-authorship patterns with publications in high-impact journals. Journal of biomedical informatics, 52, 311-318

BBC. (2019, May 7). Huawei faces US charges: The short, medium and long story. https://www.bbc.com/news/world-us-canada-47046264

Benoit, K., Watanabe, K., Wang, H., Nulty, P., Obeng, A., Müller, S., & Matsuo, A. (2018). quanteda: An R package for the quantitative analysis of textual data. Journal of Open Source Software, 3(30), 774.

Beygelzimer, A., Grinstein, G., Linsker, R., & Rish, I. (2005). Improving network robustness by edge modification. Physica A: Statistical Mechanics and its Applications, 357(3-4), 593-612.

Bilal, K., Manzano, M., Erbad, A., Calle, E., & Khan, S. U. (2018). Robustness quantification of hierarchical complex networks under targeted failures. Computers & Electrical Engineering, 72, 112-124.

Bondi, M., & Scott, M. (Eds.). (2010). Keyness in texts (Vol. 41). John Benjamins Publishing.

Carchiolo, V., Grassia, M., Longheu, A., Malgeri, M., & Mangioni, G. (2019). Network robustness improvement via long-range links. Computational Social Networks, 6, 1-16.

Chen, H. (2023). A Lexical Network Approach to Second Language Development.

Chen, S., Ding, Y., Zhang, Y., Zhang, M., & Nie, R. (2022). Study on the robustness of China's oil import network. Energy, 239, 122139.

Council of Canadian Academies. 2018. Competing in a Global Innovation Economy: The Current State of R&D in Canada. Ottawa (ON): Expert Panel on the State of Science and Technology and Industrial Research and Development in Canada, Council of Canadian Academies

Cowan, R., & Jonard, N. (2004). Network structure and the diffusion of knowledge. Journal of economic Dynamics and Control, 28(8), 1557-1575.

Dekker, A. H., & Colbert, B. D. (2004, January). Network robustness and graph topology. In Proceedings of the 27th Australasian conference on Computer science-Volume 26 (pp. 359-368).

Duan, B., Liu, J., Zhou, M., & Ma, L. (2016). A comparative analysis of network robustness against different link attacks. Physica A: Statistical Mechanics and its Applications, 448, 144-153.

Durán-Muñoz, I. (2019). Adjectives and their keyness: a corpus-based analysis of tourism discourse in English. Corpora, 14(3), 351-378.

Ebadi, A., & Schiffauerova, A. (2015). On the relation between the small world structure and scientific activities. PloS one, 10(3), e0121129.

Fife, R., & Chase, S. (2021, July 12). Ottawa imposes national-security risk assessments for university researchers seeking federal funds. The Globe and Mail. https://www.theglobeandmail.com/politics/article-ottawa-imposes-national-security-risk-assessments-for-university/

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. Social networks, 1(3), 215-239.

Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Technological limitations and political responses. Development and change, 52(5), 1174-1195.

Hansen, D. L., Shneiderman, B., Smith, M. A., & Himelboim, I. (2020). Calculating and visualizing network metrics. Analyzing social media networks with NodeXL, 79-94.

Hertzberg, E., & Platt, B. (2022, May 19). Canada bans China's Huawei, ZTE from 5G networks. Financial Post. https://financialpost.com/telecom/canada-ban-huawei-5g

Hu, Q., Medina, A., Siciliano, M. D., & Wang, W. (2023). Network structures and network effects across management and policy contexts: A systematic review. Public Administration, 101(3), 953-972.

Humphries, M. D., Gurney, K., & Prescott, T. J. (2006). The brainstem reticular formation is a small-world, not scale-free, network. Proceedings of the Royal Society B: Biological Sciences, 273(1585), 503-511.
Iyer, S., Killingback, T., Sundaram, B., & Wang, Z. (2013). Attack robustness and centrality of complex networks. PloS one, 8(4), e59613.
Jacobi, C., Van Atteveldt, W., & Welbers, K. (2018). Quantitative analysis of large amounts of journalistic texts using topic modelling. In *Rethinking Research Methods in an Age of Digital Journalism* (pp. 89-106). Routledge.
Jaisal, E. K. (2020). The US, China and Huawei debate on 5G telecom technology: Global apprehensions and the Indian scenario. Open Political Science, 3(1), 66-72.
Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a security threat. NATO Cooperative Cyber Defence Center for Excellence (CCDCOE), 28, 1-26.
Kumar, S. (2019). Indian government tightens rules on academic collaboration with China. Science.
Lind, F., Eberl, J. M., Eisele, O., Heidenreich, T., Galyga, S., & Boomgaarden, H. G. (2022). Building the bridge: Topic modeling for comparative research. *Communication Methods and Measures*, *16*(2), 96-114.
Liu, J., Zhou, M., Wang, S., & Liu, P. (2017). A comparative study of network robustness measures. Frontiers of Computer Science, 11, 568-584.
Lordan, O., Sallan, J. M., Simo, P., & Gonzalez-Prieto, D. (2014). Robustness of the air transport network. Transportation Research Part E: Logistics and Transportation Review, 68, 155-163.
Louzada, V. H., Daolio, F., Herrmann, H. J., & Tomassini, M. (2015). Generating robust and efficient networks under targeted attacks (pp. 215-224). Springer International Publishing.
Luke, D. A., Wald, L. M., Carothers, B. J., Bach, L. E., & Harris, J. K. (2013). Network influences on dissemination of evidence-based guidelines in state tobacco control programs. Health Education & Behavior, 40(1_suppl), 33S-42S.
Ma, L., Liu, J., & Duan, B. (2016). Evolution of network robustness under continuous topological changes. Physica A: Statistical Mechanics and its Applications, 451, 623-631.
Mao, Y. (2021, June). Analyzing the current status of global 5G research from the perspective of bibliometrics. In Journal of Physics: Conference Series (Vol. 1955, No. 1, p. 012050). IOP Publishing
Mendonça, S., Damásio, B., de Freitas, L. C., Oliveira, L., Cichy, M., & Nicita, A. (2022). The rise of 5G technologies and systems: A quantitative analysis of knowledge production. Telecommunications Policy, 46(4), 102327.
Mervis, J. (2023, February 17). Canada moves to ban funding for 'risky' foreign collaborations. Science. https://www.science.org/content/article/canada-moves-ban-funding-risky-foreign-collaborations
Ministry of Foreign Afairs. (2019). Approach to matters relating to China (Skr. 2019/20:18). Government ofces of Sweden.
Moore, J. M., Small, M., & Yan, G. (2021). Inclusivity enhances robustness and efficiency of social networks. Physica A: Statistical Mechanics and its Applications, 563, 125490.
Morales, F. G., Paiva, M. H., & Bustos-Jiménez, J. A. (2018). Measuring and improving network robustness: A Chilean case study. IEEE Communications Letters, 23(1), 44-47.
Nguyen, N. K. K., Nguyen, Q., Pham, H. H., Le, T. T., Nguyen, T. M., Cassi, D., ... & Bellingeri, M. (2022). Predicting the robustness of large real-world social networks using a machine learning model. Complexity, 2022.
Nguyen, Q., Vu, T. V., Dinh, H. D., Cassi, D., Scotognella, F., Alfieri, R., & Bellingeri, M. (2021). Modularity affects the robustness of scale-free model and real-world social networks under betweenness and degree-based node attack. Applied Network Science, 6(1), 1-21.
Owens, B. (2022, August 3). Huawei ban adds to concerns of a chill effect in research over national security rules. University Affairs. https://www.universityaffairs.ca/news/news-article/huawei-ban-adds-to-concerns-of-a-chill-effect-in-research-over-national-security-rules/
Papadopoulos, G. D., Magafas, L., Demertzis, K., & Antoniou, I. (2023). Analyzing Global Geopolitical Stability in Terms of World Trade Network Analysis. Information, 14(8), 442.

Parinov, S. (2021). Citation contexts as a data source for evaluation of scholarly consumption. *Scientometrics*, *126*(11), 9249-9265.
Parsons, C. (2020). Huawei and 5G: clarifying the Canadian equities and charting a strategic path forward. In Huawei and 5G: clarifying the Canadian equities and charting a strategic path forward: Parsons, Christopher. [Toronto]: Munk School of Global Affairs & Public Policy, University of Toronto.
Rotolo, T., & Frickel, S. (2019). When disasters strike environmental science: a case–control study of changes in scientific collaboration networks. Scientometrics, 120(1), 301-317.
Roul, R. K., Sahoo, J. K., & Arora, K. (2017, December). Modified TF-IDF term weighting strategies for text categorization. In 2017 14th IEEE India council international conference (INDICON) (pp. 1-6). IEEE.
Rueda, D. F., Calle, E., & Marzo, J. L. (2017). Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements. Journal of Network and Systems Management, 25, 269-289
Sawai, H. (2013). A small-world network immune from random failures and resilient to targeted attacks. Procedia Computer Science, 18, 976-985.
Schneider, C. M., Moreira, A. A., Andrade Jr, J. S., Havlin, S., & Herrmann, H. J. (2011). Mitigation of malicious attacks on networks. Proceedings of the National Academy of Sciences, 108(10), 3838-3841.
Telesford, Q. K., Joyce, K. E., Hayasaka, S., Burdette, J. H., & Laurienti, P. J. (2011). The ubiquity of small-world networks.
The Globe and Mail. (2018, December 6). Huawei and Canada: The story so far of the Chinese company, Meng Wanzhou's case and a global political feud. The Globe and Mail. https://www.theglobeandmail.com/canada/article-huawei-canada-china-5g-network-explainer/
The Star. (2022, May 19). Timeline of Canada's decision to bar Huawei, ZTE from 5G networks. https://www.thestar.com/politics/timeline-of-canada-s-decision-to-bar-huawei-zte-from-5g-networks/article_7c2f7319-d9f6-5043-965c-7798ae38a161.html
Tunney, C., & Raycraft, R. (2022, May 19). Canada bans Chinese tech giant Huawei from 5G network. CBC News. Retrieved from https://www.cbc.ca/news/politics/huawei-5g-decision-1.6310839
U.S. Department of Commerce. (2020, August 17). Commerce Department further restricts Huawei access to U.S. technology and adds another 38 affiliates to the Entity List. https://2017-2021.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and.html
W. de Nooy, A. Mrvar, & V. Batagelj, (2005). Exploratory social network analysis with Pajek. New York: Cambridge University Press. 362 + xxvii PP. $39.99, ISBN: 0521841739.
Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world'networks. nature, 393(6684), 440-442.
Wei, N., Xie, W. J., & Zhou, W. X. (2022). Robustness of the international oil trade network under targeted attacks to economies. Energy, 251, 123939.
Wexler, B. (2022, June 28). McGill to maintain partnership with Huawei despite federal ban from 5G network. The Tribune. https://www.thetribune.ca/news/mcgill-to-maintain-partnership-with-huawei-despite-federal-ban-from-5g-network280622/
Wijffels, J., Straka, M., & Straková, J. (2019). Package 'udpipe'.
Wu, J., Barahona, M., Tan, Y. J., & Deng, H. Z. (2011). Spectral measure of structural robustness in complex networks. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 41(6), 1244-1252.
Xiaohong, W. A. N. G., Zhang, Y., Lizhi, W. A. N. G., Dawei, L. U., & Guoqi, Z. E. N. G. (2020). Robustness evaluation method for unmanned aerial vehicle swarms based on complex network theory. Chinese Journal of Aeronautics, 33(1), 352-364.
Xie, W. J., Wei, N., & Zhou, W. X. (2021). Evolving efficiency and robustness of the international oil trade network. Journal of Statistical Mechanics: Theory and Experiment, 2021(10), 103401.
Yang, Y., Li, Z., Chen, Y., Zhang, X., & Wang, S. (2015). Improving the robustness of complex networks with preserving community structure. PloS one, 10(2), e0116551.

Zare-Farashbandi, F., Geraei, E., & Siamaki, S. (2014). Study of co-authorship network of papers in the Journal of Research in Medical Sciences using social network analysis. Journal of research in medical sciences: the official journal of Isfahan University of Medical Sciences, 19(1), 41

Zhang, H. E., Wong, K. H., & Chang, V. (2021). Patent analysis in the 5G network. Journal of Global Information Management (JGIM), 29(6), 1-28.

Zhang, L., Zhao, Y., Chen, D., & Zhang, X. (2021). Analysis of network robustness in weighted and unweighted approaches: a case study of the air transport network in the belt and road region. Journal of Advanced Transportation, 2021, 1-13.

Zhang, Z. Z., Xu, W. J., Zeng, S. Y., & Lin, J. R. (2014). An effective method to improve the robustness of small-world networks under attack. Chinese Physics B, 23(8), 088902.

Appendix 1

Table 4 Hierarchical clustering results (topics)

Main theme	Clusters number	Clusters title	Clusters size
Location-based technologies	66	Advanced localization and tracking technologies in various environments	13
	65	Enhanced navigation and positioning through sensor integration in various environments	8
	47	Innovative technologies and strategies for enhanced indoor and outdoor wireless communication and contact tracing.	8
	64	Optimizing and analyzing Wi-Fi networks and technologies	6
	52	Wireless communication and control in residential and acoustic environments.	14
Millimeter-wave technologies	7	Millimeter-wave technology applications and developments in 5G and wireless communications	41
	2	Advancements and challenges in mm wave technologies for 5G and imaging application	20
Energy management and efficiency	60	Data-driven electric vehicle emission reduction and energy management.	21
	20	Smart grid technologies and energy management	41
	9	Energy-efficient resource allocation in advanced wireless networks	30
	4	Power management and energy efficiency in 5G wireless communication technologies	72
Iot and sensor networks	58	Wireless object monitoring, earthquake analysis, and motion sensing technologies for IoT and disaster mitigation	9
	45	Wireless sensor technologies for health and operational management in mining and oil industries.	21
	39	Agent-based decision making in stochastic game theoretical systems.	11
	38	Multi-agent scheduling and resource allocation in various industries, including healthcare, for enhanced efficiency and performance	8
	36	Wireless sensor networks in various applications and technologies	39
	25	Smart home and smart city technologies	18
	24	IoT communication and infrastructure research	17
Communication technologies and coding	44	Optimizing cable technologies for data transmission and grid monitoring	7
	42	Exploring coding theories and 3D technologies in network and multimedia applications	9
	41	Advancements and applications of coding and information theory in communication networks	11
	11	Implementation and application of polar and LDPC codes in 5G wireless communication systems	11
Edge and cloud computing	27	Mobile edge computing and mobile cloud applications	28
	26	Edge computing and deep learning for IoT and 5G networks	13

	21	Cloud computing, resource management, and privacy in fog networks	30

Table 5 (continued)

Main theme	Clusters number	Clusters title	Clusters size
Electromagnetic technologies	6	Advancements and applications of electromagnetic metamaterials in communication and processing technologies	58
	3	Advancements and challenges in electromagnetic metasurface-enhanced antenna arrays for communication systems.	63
Multimedia and content delivery	28	Multimodal media and communication technologies	37
	23	Multimedia content and video technology advancements	21
Network management and optimization	63	Optimizing 5G connectivity and network management through artificial intelligence.	6
	62	Optimizing network traffic management and operations in cellular networks	11
	61	Modeling and optimization in real-time software systems	48
	33	Quality of service and quality of experience in next-generation networks and service architectures	36
	32	Wireless mesh network performance and multicast optimization	11
	30	Resource management for next-generation wireless networks	31
	29	Data center networking and optimization	7
	14	Optimization of machine communications and node management in network layers	19
	13	Innovative strategies for massive data traffic and low latency in 5G networks	34
	12	Optimization and management in next-generation small cell cellular networks	35
	10	Optimizing cooperative diversity in wireless relay networks	41
	8	Access and management of dynamic spectrum in cognitive radio networks	21
	40	Technological approaches to sound and noise management in various applications and environments.	18
Professional development and skills	50	Professional skill development and training programs in emerging technologies.	5
Safety, security, and privacy	59	Enhancing cybersecurity through advanced messaging verification and low-latency communication infrastructure optimization	3
	51	Enhancing safety and reliability through technological solutions in various environments	16
	34	Blockchain security and IoT privacy in emerging networks	44
	22	Vehicular communication and safety technologies	34
	19	Quantum information science and technologies for enhanced secure communication and computation.	17
	5	Innovations and applications of silicon circuits and chips in communication and diagnostics.	24

Silicon and optical technologies	1	Advancements in silicon photonics and optical communication systems.	101

Table 6 (continued)

Main theme	**Clusters number**	**Clusters title**	**Clusters size**
Advanced wireless communication technologies	67	Advanced radio channel modeling and remote communication technologies.	22
	57	Advanced wireless communication technologies and protocols for 5G, IoT, and beyond, including VLC, MMW, and RFID applications, and hardware development for DSP, 5G, and AI systems	11
	18	Synchronization and estimation in wireless communication systems	7
	15	Adaptive transmission techniques and channel management in wireless communications.	17
	54	Advanced wireless communication and networking technologies with a focus on interface, database, and platform development.	14
	43	Innovative approaches to RFID and wireless communication identification and management	15
	46	Digital innovations and paradigm shift in wireless communications and technology applications	7
Interdisciplinary research	56	Advanced technologies converging in aerospace, healthcare, and entertainment domains	5
	55	Advanced technology applications for testing and monitoring in diverse industries	8
	53	Interdisciplinary research in hardware, software, and sensing applications	10
	35	Medical imaging and healthcare technology advancements	42
	31	Optimizing game server performance and latency in cloud-based multiplayer online gaming.	10
	37	Building construction and management technologies and methods	13
	48	Human-interactive robotic systems and applications	9
	49	Electrical and thermal management in various technological applications	15
Mimo	16	Advancing 5G technologies: SDN, massive MIMO and full duplexing collaboration	54
	17	5G innovations: massive MIMO, mm wave communication, and wireless backhaul solutions	22

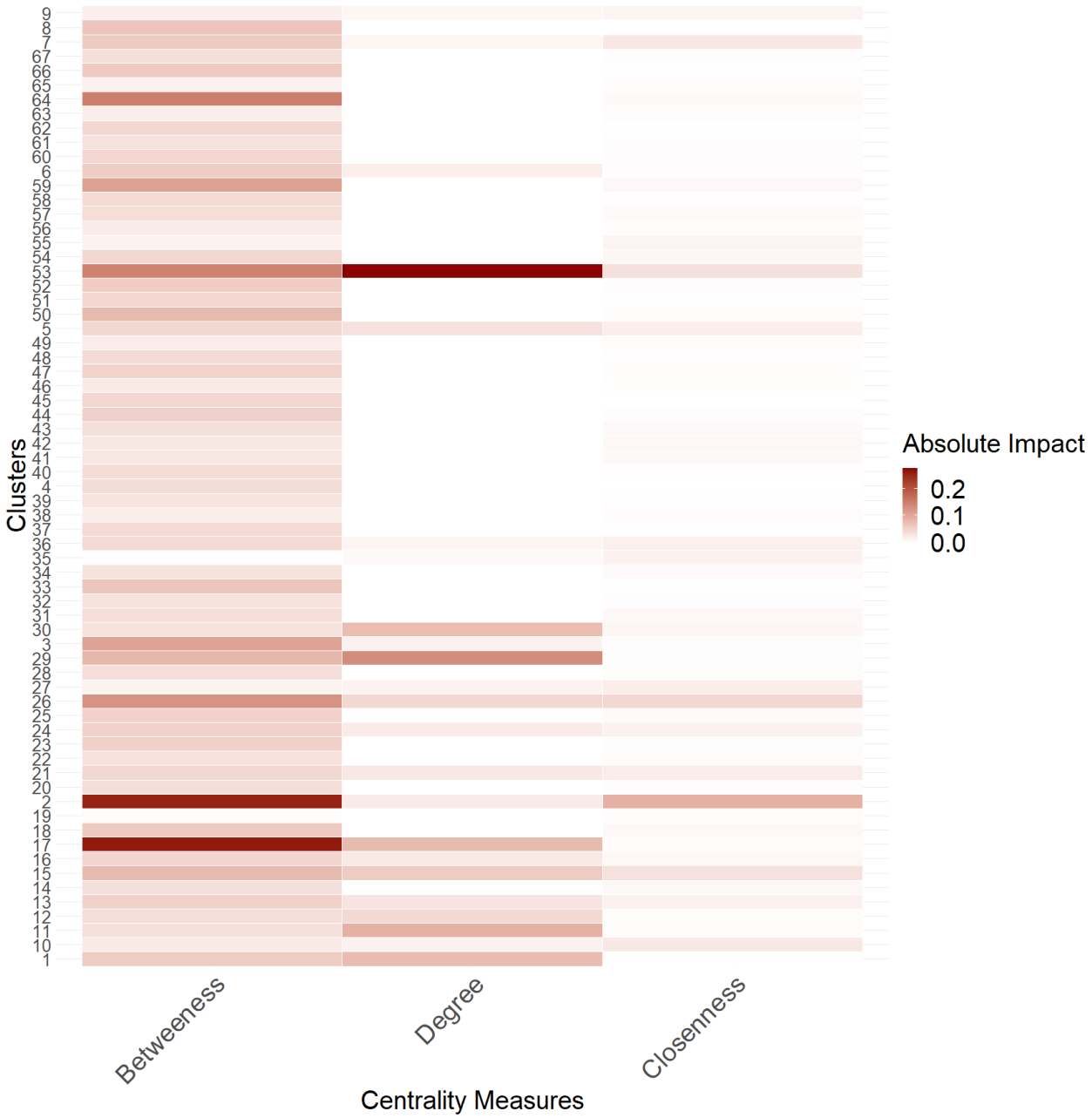


Fig. 11 Impact of Huawei's removal on clusters centrality measures

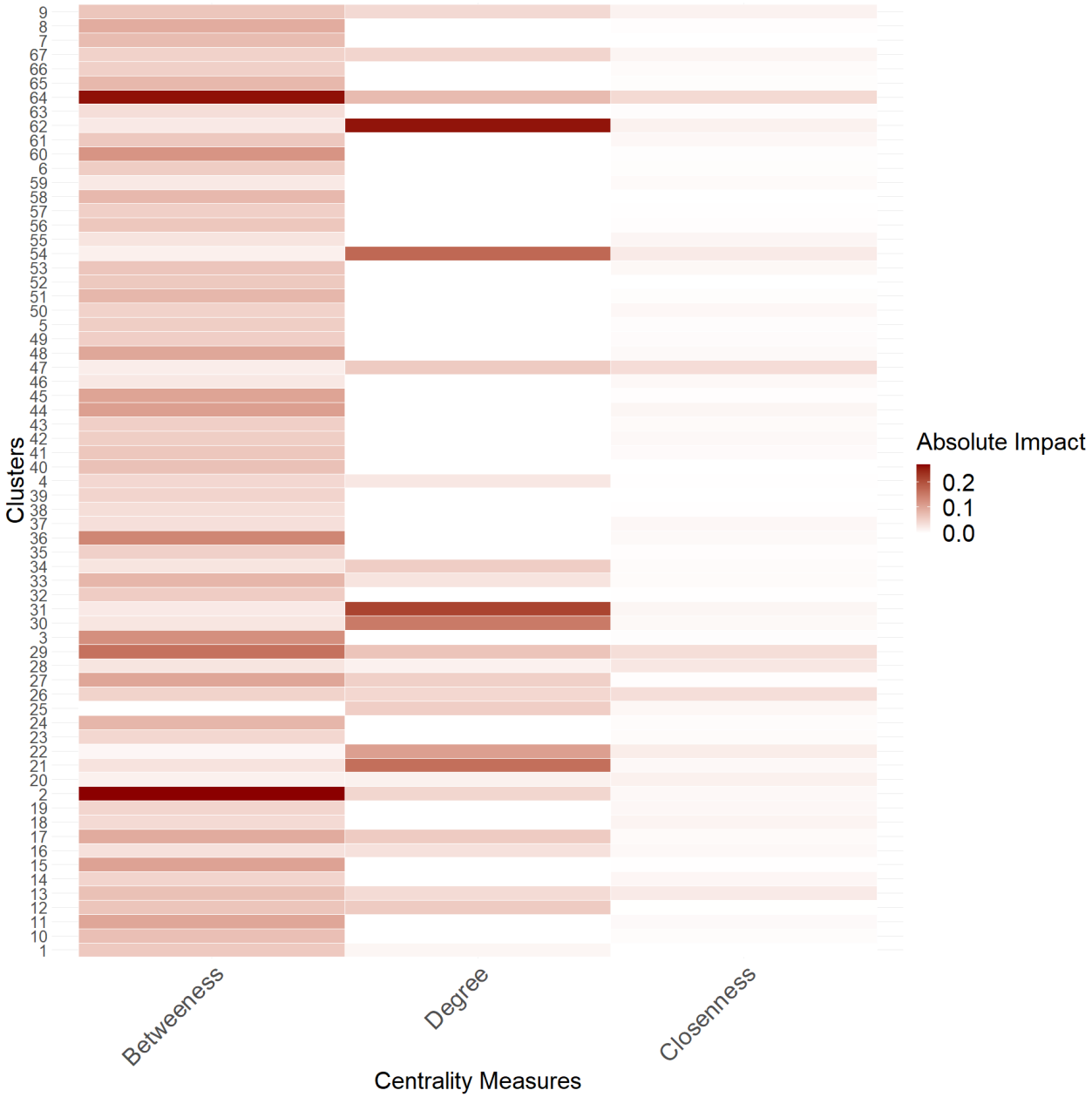


Fig. 12 Impact of Ericsson's removal on clusters centrality measures