Adelaide Baronchelli and Roberto Ricciuti*

# The Battlefield and the Wire: Linking Cyber and Material Conflicts, 2000–2014

https://doi.org/10.1515/peps-2025-0050
Received July 9, 2025; accepted July 14, 2025; published online August 15, 2025

**Abstract:** This paper describes how cyber and material conflicts overlaps in the international system. Given countries' international alliances and conflicts, as well as their technical abilities, we want to uncover whether or not countries engage in cross-domain operations. Combining a dataset collecting information on cyber interactions between rival states and ICEWS data, we analyze cyber conflict among states and contextualize it into the system of international relations using social network analysis and the tool of multiplex networks from 2000 to 2014. We find support for our hypothesis that cross-domain operations are relatively rare. Furthermore, we find that: (a) the use of cyber tools is less frequent than the use of physical force; (b) there are some localized conflictual relations in the physical world, a circumstance that does not occur in the virtual world; (c) Russia seems to balance material aggressions and cyber-attacks, whereas the US prefer material conflict, and China is more active in the cyber realm.

**Keywords:** cyber conflict; material conflict; cross-domain operations; multiplex networks; social network analysis

**JEL Classification:** D74; C45

## 1 Introduction

This paper describes how cyber incidents and material conflicts interact in the international system. We try to answer the following research questions: Do countries engage in cross-domain operations?[1] Given their international alliances and conflicts, does the cyber world reflect the material relations among countries?

1 As in Katagiri (2022), we define cross-domain operation as an operation in which an attack in a domain is related to attack in another domain.

***Corresponding author: Roberto Ricciuti**, Department of Economics, University of Verona, Via Cantarane 24, 37129 Verona, Italy; and CESifo, Munich, Germany, E-mail: roberto.ricciuti@univr.it. https://orcid.org/0000-0001-8251-0423
**Adelaide Baronchelli,** University of Turin, Torino, Italy. https://orcid.org/0000-0002-5889-951X

Valeriano and Maness (2014) developed a dataset that collects information on cyber interactions between rival states over the period 2000–2014. Using this data, we analyze cyber conflict among states and contextualize it into the system of international relations using social network analysis and the tool of multi-layer networks. Since it is hard to establish causality as a condition for the operation, we only require correlation to be present for the definition to be valid.

Although the dataset has been subsequently updated, we focus on these earlier data to single out a period of initial use of the cybercapacity, when cyber conflict remained strategically limited despite advances in material and organizational capabilities (Valeriano et al. 2018). Although its operational requirements are relatively low, its strategic potential remains in the hands of established powers (Slayton 2017; Pytlak and Mitchell 2018). Capable state actors appear restrained in their exercise of power in cyberspace, with sustained interactions below the threshold of armed conflict, against the expectations of the early literature (Fischerkeller and Harknett 2019).

The incorporation of social network analysis (SNA) into the study of international relations (IR) marks a significant methodological and theoretical development. Traditional IR approaches often relied on dyadic analyses – focusing on bilateral conflicts, alliances, or trade – or systemic models that treated states as independent and interchangeable units. In contrast, SNA explicitly maps and quantifies relational structures among multiple actors, offering a means to investigate how patterns of connections shape international outcomes beyond what dyadic or aggregate models can capture (Maoz 2010; Hafner-Burton and Montgomery 2006).

Early applications of network concepts in IR trace back to studies of alliance structures during the Cold War, but formal network measures such as centrality, density, and clustering rose to prominence in the 1990s and early 2000s. Maoz (2010) systematically applied SNA to examine international alliances and conflicts from 1816 to 2001, demonstrating that structures such as clusters, hubs, and bridges within networks influence state behavior. His subsequent works (Maoz 2011; Maoz et al. 2007) demonstrated how states within dense conflict networks exhibited greater propensity for militarized disputes, and how voting in the UN General Assembly reflected broader community structures (Maoz and Joy 2008).[2]

Recently, several studies have advanced both empirical application and methodology. Kacziba (2021) provides a comprehensive methodological review of the

2 The application of network analysis extended beyond war and peace to governance and economics. Hafner-Burton and Montgomery (2006) showed how the structure of the preferential trade agreement network shapes states' bargaining power and economic integration. Kahler (2009) argued that global governance increasingly operates through networked modes of organization, involving states, international organizations, and NGOs that can be empirically studied via SNA.

network paradigm in IR, outlining its applications across geopolitics and geo-economics and cautioning scholars about limits related to data and inference. A study by Ben-Itzhak (2025) on international cooperation in outer space analyzed bilateral and multilateral cooperation networks from 1958 to 2023 using SNA, identifying temporal shifts in centrality and structural density that mirror geopolitical changes in space policy (Ben-Itzhak 2025).

Security dynamics and conflict diffusion have also benefited from network-based insight. Cranmer et al. (2014) demonstrated that conflict spreads through mechanisms like triadic closure, while Maoz (2011) suggested that the democratic peace might be partly explained by democracies' shared embedding in cooperative networks. Methodologically, the field continues to evolve with models like exponential random graph models (ERGMs) applied by Ward et al (2011) for alliance formation, and Boermans and Ward's (2014) work on institutional co-membership using network brokerage measures.

This paper applies multiplex (or multilayer) network analysis to study cyber and material conflict jointly. Multiplex networks (a system of multiple networks with different types of links but share a common set of nodes, Interdonato et al. 2020; Kivelä et al. 2014) are uniquely suited to address the (possible) interdependence between these two manifestations of conflict. The concept of a multiplex network fits well with the international system since it can be interpreted as a network where the world's nations interact along many dimensions (Maoz 2010): conflicts, alliances, diplomatic ties, and commercial links.

The paper is organized as follows: Section 2 reviews the literature on cyber conflict between states and spells out our hypotheses on the relationship between the latter and material conflict, while Section 3 introduces the multiplex network analysis and the data. Section 4 presents the results, and Section 5 concludes.

## 2 Literature and Hypothesis: The Relationship Between Cyber and Material Conflict

The existing literature on cyber conflict is grouped into two broad areas: a group of studies focused on the implications of cyber activities for peacetime deterrence, and another strand of literature investigating the overlap between cyber and kinetic capabilities.

Within the first group, Libicki (2016) argues that traditional deterrence theories may not be effective in the context of cyber conflict, given the unique characteristics of the domain. He suggests that cyber conflict may require a new approach that emphasizes the importance of resilience and the ability to recover from attacks.

Libicki argues that the key to deterring cyber attacks is to make them less effective, by strengthening defenses and increasing resilience. Gartzke (2013) examines the role of attribution in deterring cyber attacks. He argues that attribution is a key factor in deterrence, as it enables states to identify and respond to attackers. Attribution is often difficult in the context of cyberconflict, as attackers can hide behind proxy servers and other means of obfuscation. Gartzke (2013) proposes several strategies for improving attribution, including improving the capabilities of cyber forensics and developing new technologies for tracking attackers.

Axelrod and Iliev (2014) argue that norms play an important role in shaping state behavior in cyberspace, and that the development of a normative framework for cyber activities is crucial for deterring malicious actors. They suggest that norms can be established through the development of international agreements and the creation of institutional structures that promote cooperation and coordination. Valeriano and Maness (2014) examine the relationship between cyber conflict and traditional deterrence theory. They argue that the principles of deterrence, such as the credibility of threats and the cost-benefit calculation of potential attackers, can still be applied to cyber conflict. However, traditional deterrence strategies may need to be adapted to the unique characteristics of the cyber domain, such as the rapid pace of technological change and the difficulty of attribution.

The second stream of the literature starts from the observation that cyber and kinetic capabilities have become increasingly intertwined in modern conflict and security, with potentially significant implications for international relations and military strategy. For example, Kello (2013) argues that cyber attacks are being used to support and enhance traditional military operations. He suggests that the distinction between cyber and kinetic capabilities is becoming blurred, and that it is important to consider them as part of a wider spectrum of military capabilities. Andress and Winterfeld (2013) focus on the role of cyber attacks in supporting kinetic operations. They maintain that cyber capabilities can be used to gain information, disrupt or destroy enemy systems, and support traditional military operations. They suggest that their integration is leading to a new form of "hybrid warfare," in which attacks can occur across multiple domains. As a result, a holistic approach to a military strategy that takes into account the full range of capabilities available is needed. A similar plea for new models and frameworks to effectively integrate cyber capabilities into traditional military operations is advanced by Axelrod (2014), emphasizing the unique characteristics of the cyber domain, such as the difficulty of attribution and the speed of attacks.

Libicki (2016) focuses on the potential implications of cyber capabilities for deterrence and strategic stability. He argues that the former has the potential to upset existing power balances, and may lead to new forms of strategic competition and instability. The potential risks of integrating cyber and kinetic capabilities

within military operations are analyzed Kostyuk (2021), arguing that the increased use of cyber capabilities may create new vulnerabilities and risks, particularly if cyber attacks are used to target critical infrastructure or other sensitive systems. However, the disruptive potential of cyber capabilities has not come to fruition. Gartzke and Lindsay (2015) clarify that cyberspace is not offense-dominant because of technical characteristics that undermine deterrence and defense, as often believed. They claim that deception is a double-edged sword: covert attackers must exercise restraint against complex targets to avoid compromises resulting in mission failure or retaliation. Moreover, defenders can also employ deceptive concealment and ruses to confuse or ensnare aggressors.[3] In Buchanan (2017), two nations that do not seek to harm each other but neither trusts the other, will find it prudent to penetrate each other's systems, in a new incarnation of the "security dilemma", with the risk of escalating tension. Based on experimental wargames involving rival states with power parity in militarized disputes and randomized cyber triggers and response options, Jensen et al. (2024) find that the availability of cyber response options reduces escalatory behavior via a substitution mechanism.

What good is cyber in war? Schulze (2020) observes that cyber technologies in war have some benefits, but many operational hurdles, for example, need highly-specialized training and preparation and are difficult to use together with other types of arms. Cyber operations are more like a specialized weapon for quick strikes rather than for lengthy and sustained campaigns. A similar line of reasoning was put forward by Iasiello (2013). In Gomez and Whyte (2022) the uncertainty due to an inherent information deficit about cyber operations, which is credited to be one of the causes for its limited role, is treated in a cognitive-cultural framework, in which the strategic culture is used as a basis for deriving strategic objectives and the means of achieving them.

Two recent papers are close to ours. First, Kostyuk and Zhukov (2019) present the first quantitative analysis of the relationship between cyber activities and physical violence during war. For both Ukraine and Syria, they find that cyber attacks have had little or no impact on fighting. In Ukraine, cyber activities failed to compel discernible changes in battlefield behavior. For Syria the results are similar: the timing of cyber actions is independent of fighting on the ground. Second, Katagiri (2022) investigates five theories as to why most cyberattacks do not take place simultaneously with military operations. Two theories emerge as the most convincing. First, state attackers decide strategically not to "cross the domain" for administrative reasons based on the internal division of labor. Second, although

**3** Gartzke and Lindsay (2015) make a parallel between the importance of deterrence in the nuclear era with the role of deception in a world that increasingly depends on technology to mediate interaction.

their cyber and military units are integrated, many cyber attackers have major technical difficulties with cross-domain operations. The other three arguments – fear of war escalation, international law as it applies online, and cyberspace conduct norms – appear less convincing.

Starting from this review of the literature, we can state the following hypothesis to test:

**Hypothesis 1:** Cross-domain operations are infrequent.

# 3 Methodology and Data

In this work, we use SNA and, specifically, the concept of multiplex networks to represent the relationship between cyber and material conflicts in the international system.[4] A multiplex network is defined as a triple, $G_e = (N, E, C)$, where $N$ is the node set, $C$ is the color set (which is used for labeling the type of edge), and $E$ is the edge set (Kivelä et al. 2014). We interpret the nodes as countries in the international system, and the edges as the relations that connect them, which differ in type and are represented by different colors. In other words, according to this perspective, the same nodes (i.e. countries) can have different types of relations (i.e. cyber or material conflicts).

Multiplex networks allow us to describe how countries interact on the material conflict level as well as on the cyber level. Furthermore, this perspective also shows how each level contributes to the whole network. To do so, we adopt three different approaches. First, we describe the network structure, highlighting similarities and differences between the two layers. Secondly, we single out the most central actors in the network. In this part, using different measures of multi-layer centrality, we question whether top players in the realm of material conflict are the same in cyber conflict. Finally, we correlate the two layers to show how much they overlap.

To single out the most important countries in the network, we go beyond the single-layer idea of degree centrality, and, following Dickison et al. (2016), we use the concept of neighborhood and exclusive neighborhood centrality. The key issue in analyzing centralities in multiplex networks lies in the fact that an actor can be connected to different nodes depending on the layer. Thus, the neighborhood centrality of an actor $a$ is the number of actors that are connected to $a$ on a specific layer

**4** In the context of a single-layer network, Baronchelli (2018) shows that the level of cohesion in the network is low and the number of countries which does not make use of cyber tactics is high; Russia is emerging as the major offender while the US is the most attacked country; and that geography is a driving factor in influencing links formation.

or set of layers. In a network of two layers like the one we analyze in this work, the difference between the concept of degree and neighborhood is not evident since they coincide on the single layer.[5] However, the idea of neighborhood centrality can be extended to that of exclusive neighborhood centrality, which counts the exclusive neighbors of an actor *a*, i.e. those actors connected to *a* only on a specific layer.

Closely related to these concepts, the relevance of an actor is the ratio between the neighbors of an actor connected by edges belonging to a specific layer (or set of) and the total number of her neighbors. Finally, the exclusive relevance of an actor *a* is the ratio between the exclusive neighbors of an actor connected by edges belonging to a specific layer (or set of) and the total number of her neighbors. Overall, neighborhood and relevance describe *how much an actor exists on a layer while exclusive neighborhood and exclusive relevance* indicate *how much the general connectivity of an actor would be affected by removing a specific layer*.

To draw data about cyber conflict, we use data from The Dyadic Cyber Incidents Dataset (DCID) v. 1.5, by Maness et al. (2019). The DCID dataset collects information about cyber incidents between couples of rival states from 2000 to 2016. Here, cyber incidents are defined as individual operations launched against a target state by a rival country. Data about material conflicts are drawn from the Integrated Crisis Events Warning System (ICEWS, see Boschee et al. 2015) which reports several types of coded interactions between socio-political actors (i.e. cooperative or hostile actions between individuals, groups, sectors, and nation-states) until 2014. We select material conflictual events regarding the same couples of states as reported in the DCID. Events labeled as material conflicts report hostile interactions between two countries, including protests, exhibition of force posture, coercion, assault, fighting, and use of conventional mass violence.[6] As a result, we obtained information on conflicts – both cyber and material – between 70 pairs of rival countries. The list of involved countries is provided in Table A.1 in the Appendix.

The data collected are organized as multiplex networks where rival states become the $N$ set of nodes, $E$ is the set of edges connecting them, and $C$ is the two types of hostile interactions that connect rival states, i.e. cyber incidents (DCID) and material conflictual events (MAT). Hence, the $E^C$ edge is quantified as $(N, E^C)$. One layer in the network is characterized by the edge set $(N, E^{\text{DCID}})$, the other by the edge set $(N, E^{\text{MAT}})$. The original network is valued and directed: an edge between two nodes indicates the number of cyber incidents (layer DCID) or material conflict events (layer MAT) between countries over the period analyzed. To compute network

**5** The degree centrality of a country a describes the number of countries it is adjacent to. While the degree counts edges, the neighbourhood counts actors.

**6** More specifically, we select events labelled with the following cameo codes 141, 1411, 143, 145, 150, 154, 160, 161, 162, 163, 164, 170, 171, 1711, 172, 1721, 173, 174, 175, 180, 181, 1822, 183, 185, 186, 190, 193, 2041

statistics, however, we need to dichotomize the data, that is, we need to select a threshold value above which an edge between two nodes exists in the network. Here, we choose a simple threshold defining the existence of a link if there is at least one cyber incident or material conflict event between two countries.

# 4 Results

Table 1 shows network statistics for the two layers: DCID for the cyber conflicts and MAT for the material conflicts. Overall, the two networks have very low density values. Density indicates the ratio between the links in the network and all possible links.[7] In the network, about 1 % of all the potential links are present in the DCID layer, while there are only 3 % of the links in the MAT layer. This figure indicates that conflictual relations among states are quite rare. Trade networks or alliances networks have much higher density values (Maoz 2009). Another interesting feature of the network is reciprocity, which describes how an incident from country A to country B is matched by one from B to A.[8] In the network, the values are pretty high: about 60 % of the links are reciprocated in the DCID layer, while the figure is 80 % in the MAT layer. This is quite interesting: although conflictual relations between states are rare, they frequently bring about an action–reaction dynamic. When a state is

**Table 1:** Layer statistics.

| | DCID | MAT |
|---|---|---|
| Nodes | 26 | 59 |
| Edges | 42 | 110 |
| Components | 1 | 8 |
| Size of largest component | 26 | 44 |
| Density | 0.01 | 0.03 |
| Clustering coefficient | 0.03 | 0.11 |
| Average path length | 3.00 | 3.37 |
| Diameter | 6 | 8 |
| Reciprocity | 0.62 | 0.82 |

7 *Density* is defined as the ratio between the links in the network and all possible links and ranges between 0 (i.e. no linkages) to 1 (i.e. all possible linkages are present).

8 Formally, *Reciprocity* is computed as the number of reciprocated links divided by the total number of links and describes the extent to which an incident from country A to country B is matched by one from B to A.

attacked, it usually responds to the attack. The values for reciprocity, however, are lower in the DCID layer. This could be because not all countries have the capabilities to respond to a cyber attack.

However, two key differences exist between the cyber and material conflicts layer. First, the number of countries involved in the DCID layer is lower than in the MAT layer. The use of cyber tools is less frequent than the use of physical force. Once again, this could indicate that not all nations have yet acquired the technology needed to use cyber tactics. Another key difference lies in the number of components (see Figure 1). In a network, a component is a maximally connected sub-network. In the DCID layer, all the countries are grouped in one large component, while in the MAT layer, one large component is made of 44 countries and a few dyads and triads (components made of two or three nodes). The existence of these small components indicates that in the MAT layer there are a few localized conflictual relations. As shown in Figure 1, Venezuela and Colombia, for instance, are involved in a material conflict with each other but have no conflictual relations with other countries. Interestingly, this indicates that the use of cyber tools seems to be restricted to actors that play on a global scale and have conflictual relations with many other countries.

Table 2 shows the correlations between the two layers. The values for actors and edge overlap are pretty low. This indicates that the countries involved in material conflicts are different from those involved in cyber incidents. Interestingly, when we overlap the material conflict layer with the cyber layer, the correlation value is very high, while the same value when we overlap the DCID layer with the MAT level is low. Overall, the cyber layer is not essential for the general connectivity of the network, and it is an extension of the material layer. In other words, countries often choose

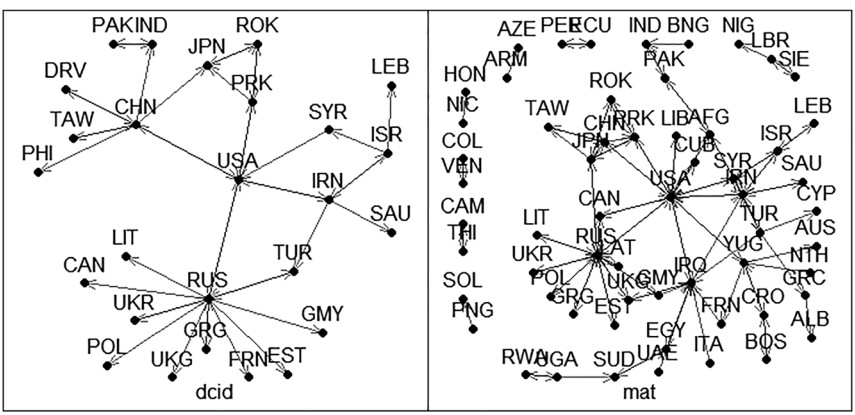


**Figure 1:** The network of cyber conflict and material conflicts.

**Table 2:** Layers overlapping.

| | Layer correlation |
|---|---|
| Actor overlap | 0.393 |
| Edge overlap | 0.299 |
| Mat – dcid overlap | 0.833 |
| Dcid – mat overlap | 0.319 |

material conflicts or pursue both cyber and material tactics. Rarely countries do pursue only cyber tactics. This evidence is consistent with Hypothesis 1.

Results about countries' out- and in-centralities shed light on this issue. Since our network is directed, we analyze both out- and in-connections. The firsts are the links that go from actor *a*, and they correspond to the incidents that have been initiated by actor *a*. The latter are the links that go to actor *a* and correspond to the incidents where actor *a* was attacked.

Table 3 describes the main attackers in the network, i.e. the nations that attacked the largest number of countries either in the cyber or material conflict realm. Results show that the three top offenders in the international system are Russia, the US, and China, which had conflicts with 13, 11, and 7 countries between 2000 and 2016, respectively. There are, however, key differences in how these three powers acted in the cyber and material conflict layers. Russia seems to balance material aggressions and cyber-attacks. When we observe its values of neighborhood centrality, it emerges that Russia entered into conflict with the same number of countries in both the cyber and material layers. Figure 1 shows that this country was involved in several conflicts with its geographical neighbors and that these conflicts were conducted with both physical and cyber tools. Figures for exclusive neighborhood centrality confirm this interpretation. Both the DCID and the MAT layer have only two exclusive neighbors. As a consequence, relevance and exclusive relevance values are identical. Russia gives the same weight to both cyber and material conflicts and it pursues its conflictual relations in the international context with both strategies. No strategy prevails over the other. This evidence for exclusive neighborhood centrality and exclusive relevance reinforces the results in Table 2 and provides further support for our hypothesis.

Conversely, the US has a distinct preference for material conflicts. Over the analyzed period, the US attacked 11 countries in the material conflict realms. Conversely, the number of countries attacked with cyber tools was just 4. The relevance of the MAT layer is maximal. Furthermore, figures for exclusive neighborhood centrality reveal that none of these countries was exclusive to the cyber level. This suggests that the USA uses cyber attacks to complement physical force.

**Table 3:** Top players in the network – out-connections.

| | Neighborhood | | | Exclusive neighborhood | | Relevance | | Exclusive relevance | |
|---|---|---|---|---|---|---|---|---|---|
| | Total | DCID | MAT | DCID | MAT | DCID | MAT | DCID | MAT |
| RUS | 13 | 11 | 11 | 2 | 2 | 0.846 | 0.846 | 0.154 | 0.154 |
| USA | 11 | 4 | 11 | 0 | 7 | 0.364 | 1 | 0 | 0.636 |
| CHN | 7 | 6 | 4 | 3 | 1 | 0.857 | 0.571 | 0.429 | 0.143 |
| TUR | 6 | 1 | 5 | 1 | 5 | 0.167 | 0.833 | 0.167 | 0.833 |
| IRN | 5 | 4 | 5 | 0 | 1 | 0.8 | 1 | 0 | 0.2 |
| JPN | 5 | 1 | 5 | 0 | 4 | 0.2 | 1 | 0 | 0.8 |
| IRQ | 4 | 0 | 4 | 0 | 4 | 0 | 1 | 0 | 1 |
| YUG | 4 | 0 | 4 | 0 | 4 | 0 | 1 | 0 | 1 |
| PRK | 3 | 3 | 3 | 0 | 0 | 1 | 1 | 0 | 0 |
| ISR | 3 | 3 | 3 | 0 | 0 | 1 | 1 | 0 | 0 |
| SYR | 3 | 1 | 3 | 0 | 2 | 0.333 | 1 | 0 | 0.667 |
| AFG | 3 | 0 | 3 | 0 | 3 | 0 | 1 | 0 | 1 |
| ROK | 2 | 2 | 2 | 0 | 0 | 1 | 1 | 0 | 0 |

On the opposite side, China is more active in the cyber realm. Out of 7 countries, it attacked over the period analyzed, six were attacked with cyber tools and three exclusively with these tools. China is the country with the highest exclusive relevance. Furthermore, looking closely at Figure 1, we also observe that the countries attacked by China are mainly its regional neighbors. Therefore, we conclude that, unlike Russia, China had conflictual relations with its neighbor mainly with cyber tools. Overall, however, China is an exception. The cyber layer's exclusive relevance is for most countries 0. Cyber tactics, when used, are applied with other more traditional forms of conflict.

Table 4 describes the main defendants in the network, i.e. the countries that were attacked by the largest number of states in the cyber or material conflict realm. Results show that the countries with the highest centralities are Russia and the US, which were attacked respectively by 12 and 11 countries over 2000–2016. Thus, the most important initiators of conflicts are also the ones that are attacked by the largest number of countries. Action–reaction dynamics prove to be important in conflict networks. However, both Russian and US enemies prefer material conflict strategies to attack their targets. Neighborhood centralities for the US and Russia are higher in the MAT layer than in the DCID layer. In other words, both countries have to defend themselves with fewer enemies in the cyber realm than in the material conflict realm. Furthermore, the exclusive relevance of the cyber level is 0 for the US and almost 0 for Russia. Attackers of Russia and the US choose both cyber and material conflict tactics and never cyber strategies alone.

**Table 4:** Top players in the network – in-connections.

| | Neighborhood | | | Exclusive neighborhood | | Relevance | | Exclusive relevance | |
|---|---|---|---|---|---|---|---|---|---|
| | Total | DCID | MAT | DCID | MAT | DCID | MAT | DCID | MAT |
| RUS | 12 | 4 | 11 | 1 | 8 | 0.333 | 0.917 | 0.083 | 0.667 |
| USA | 11 | 5 | 11 | 0 | 6 | 0.455 | 1 | 0 | 0.545 |
| IRQ | 8 | 0 | 8 | 0 | 8 | 0 | 1 | 0 | 1 |
| IRN | 6 | 2 | 6 | 0 | 4 | 0.333 | 1 | 0 | 0.667 |
| CHN | 4 | 3 | 3 | 1 | 1 | 0.750 | 0.750 | 0.250 | 0.250 |
| PRK | 4 | 2 | 4 | 0 | 2 | 0.500 | 1 | 0 | 0.500 |
| JPN | 4 | 3 | 4 | 0 | 1 | 0.750 | 1 | 0 | 0.250 |
| AFG | 3 | 0 | 3 | 0 | 3 | 0 | 1 | 0 | 1 |
| ISR | 3 | 1 | 3 | 0 | 2 | 0.333 | 1 | 0 | 0.667 |
| IND | 3 | 2 | 2 | 1 | 1 | 0.667 | 0.667 | 0.333 | 0.333 |
| TUR | 3 | 2 | 2 | 1 | 1 | 0.667 | 0.667 | 0.333 | 0.333 |
| SYR | 3 | 1 | 3 | 0 | 2 | 0.333 | 1 | 0 | 0.667 |

On the opposite side, China, India, and Turkey are attacked by a combination of cyber and material conflict tactics. Figures for neighborhood centrality and relevance show that these three countries have the same number of neighbors in both the MID and DCID layers. Furthermore, exclusive relevance values are equal: no layer prevails over the other.

# 5 Conclusions

The ability to conduct cyber attacks has improved significantly over the last two decades. The pervasiveness of digital networks is deemed to put the operations of several activities at risk and enhance the potential for attacks, even by countries with relatively minor military capabilities. Although this is a widespread view on cyber conflict, the reality seems far from this interpretation.

In this paper, we have formally addressed the relationship between cyber and material conflicts through a social network analysis technique known as multiplex networks. This methodology allows us to analyze the two features we are interested in jointly. We find support for the hypothesis derived from the literature: cross-domain operations are rare; therefore, the two modes of conflict tend to remain separated.

We also find some results that are worth highlighting. First, the use of cyber tools is less frequent than the use of physical force, which points toward the idea that

cyber conflict tools have not been widespread, and that the fear of retribution from another country may be very high, such as to avoid cyber attacks. Second, while in the cyber conflict layer all the countries are grouped in one large component, in the material conflict layer, there is one large component and a few very small components, meaning that there are some localized conflictual relations in the physical world. This indicates that the use of cyber tools seems restricted to actors that play on a global scale and have conflictual relations with many other countries. Third, when we look at global actors' conflict style, we find that Russia seems to balance material aggressions and cyber-attacks, whereas the US prefers material conflict, and China is more active in the cyber realm.

While our analysis captures correlations and structural co-occurrences across cyber and material conflict layers, establishing directionality or causal influence would require either temporal sequencing, dynamic multilayer models, all of which constitute promising avenues for future research.

# Appendix

See Table A1.

**Table A1:** List of rival countries.

| Country code 1 | Country name 1 | Country code 2 | Country name 2 |
|---|---|---|---|
| AFG | Afghanistan | IRN | Iran |
| AFG | Afghanistan | PAK | Pakistan |
| AFG | Afghanistan | USA | United States |
| ARM | Armenia | AZE | Azerbaijan |
| BNG | Bangladesh | IND | India |
| BOS | Bosnia and Herzegovina | CRO | Croatia |
| CAM | Cambodia | THI | Thailand |
| CAN | Canada | RUS | Russia |
| CAN | Canada | USA | United States |
| CHN | China | DRV | North Vietnam |
| CHN | China | IND | India |
| CHN | China | JPN | Japan |
| CHN | China | PHI | Philippines |
| CHN | China | PRK | North Korea |
| CHN | China | TAW | Taiwan |
| CHN | China | USA | United States |
| COL | Colombia | VEN | Venezuela |
| CRO | Croatia | BOS | Bosnia and Herzegovina |
| CRO | Croatia | YUG | Yugoslavia |
| CUB | Cuba | USA | United States |
| DRV | North Vietnam | CHN | China |

**Table A1:** (continued)

| Country code 1 | Country name 1 | Country code 2 | Country name 2 |
|---|---|---|---|
| ECU | Ecuador | PER | Peru |
| EGY | Egypt | IRQ | Iraq |
| EGY | Egypt | SUD | Sudan |
| EST | Estonia | RUS | Russia |
| FRN | France | IRQ | Iraq |
| GMY | Germany | IRQ | Iraq |
| GMY | Germany | RUS | Russia |
| GRC | Greece | ALB | Albania |
| GRG | Georgia | RUS | Russia |
| IND | India | PAK | Pakistan |
| IRN | Iran | AFG | Afghanistan |
| IRN | Iran | ISR | Israel |
| IRN | Iran | SAU | Saudi Arabia |
| IRN | Iran | TUR | Turkey |
| IRN | Iran | USA | United States |
| IRQ | Iraq | EGY | Egypt |
| IRQ | Iraq | IRN | Iran |
| IRQ | Iraq | UKG | United Kingdom |
| IRQ | Iraq | USA | United States |
| ISR | Israel | IRN | Iran |
| ISR | Israel | LEB | Lebanon |
| ISR | Israel | SYR | Syria |
| ITA | Italy | IRQ | Iraq |
| JPN | Japan | CHN | China |
| JPN | Japan | PRK | North Korea |
| JPN | Japan | ROK | South Korea |
| JPN | Japan | RUS | Russia |
| JPN | Japan | TAW | Taiwan |
| LAT | Latvia | RUS | Russia |
| LBR | Liberia | NIG | Nigeria |
| LBR | Liberia | SIE | Sierra Leone |
| LEB | Lebanon | ISR | Israel |
| LIB | Libya | USA | United States |
| LIT | Lithuania | RUS | Russia |
| NIC | Nicaragua | HON | Honduras |
| NTH | Netherlands | YUG | Yugoslavia |
| PAK | Pakistan | AFG | Afghanistan |
| PAK | Pakistan | IND | India |
| PER | Peru | | |

# References

Andress, J., and S. Winterfeld. 2013. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham: Elsevier.

Axelrod, R. 2014. "A Repertory of Cyber Analogies." In *Cyber Analogies*, edited by E. O. Goldman, and J. Arquilla. Monterey: Dept. of Defense Information Operations Center for Research.

Axelrod, R., and R. Iliev. 2014. "Timing of Cyber Conflict." *Proceedings of the National Academy of Sciences* 111 (4): 1298–303.

Baronchelli, A. 2018. "Conflict in Cyber-Space: The Network of Cyber Incidents, 2000–2014." *Peace Economics, Peace Science and Public Policy* 24 (4): 20180028.

Ben-Itzhak, S. 2025. "Network Analysis of International Cooperation in Space 1958-2023: Evidence of Space Blocs." *Journal of Peace Research* 62 (3): 517–34.

Boermans, M., and M. D. Ward. 2014. "Co-membership in International Organizations and the Structure of International Cooperation." *Political Science Research and Methods* 2 (2): 245–64.

Boschee, E., J. Lautenschlager, S. O'Brien, S. Shellman, J. Starz, and M. Ward. 2015. "BBN ACCENT Event Coding Evaluation (Updated). ICEWS Coded Event Data." *Harvard Dataverse*. https://doi.org/10.7910/DVN/28075.

Buchanan, B. 2017. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. London: Hurst & Company.

Cranmer, S. J., T. Heinrich, and B. A. Desmarais. 2014. "Reciprocity and the Structural Determinants of the International Conflict Network." *International Interactions* 40 (4): 576–601.

Dickison, ME, M Magnani, and L Rossi. 2016. "Multilayer Social Networks." Cambridge: Cambridge University Press.

Fischerkeller, M., and R. Harknett. 2019. "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation." *Cyber Defence Review*: 267–87.

Gartzke, E. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth." *International Security* 38 (2): 41–73.

Gartzke, E., and J. R. Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24 (2): 316–48.

Gomez, M. A., and C. Whyte. 2022. "Unpacking Strategic Behavior in Cyberspace: a schema-driven Approach." *Journal of Cybersecurity* 8 (1): tyac005.

Hafner-Burton, E. M., and A. H. Montgomery. 2006. "Power Positions: International Organizations, Social Networks, and Conflict." *Journal of Conflict Resolution* 50 (1): 3–27.

Iasiello, E. 2013. "Cyber Attack: a Dull Tool to Shape Foreign Policy." In *Proceedings of the 2013 Fifth International Conference on Cyber Conflict*, edited by K. Podins, J. Stinissen, and M. S. Maybaum, 451–70. Tallinn: IEEE.

Interdonato, R., M. Magnani, D. Perna, A. Tagarelli, and D. Vega. 2020. "Multilayer Network Simplification: Approaches, Models and Methods." *Computer Science Review* 36: 100246.

Jensen, B., B. Valeriano, and S. Whitt. 2024. "How Cyber Operations Can Reduce Escalation Pressures: Evidence from an Experimental Wargame Study." *Journal of Peace Research* 61 (1): 119–33.

Kacziba, P. 2021. "The Network Analysis of International Relations: Overview of an Emergent Methodology." *Journal of International Studies* 14 (3): 155–71.

Kahler, M. 2009. *Networked Politics: Agency, Power, and Governance*. Ithaca, NY: Cornell University Press.

Katagiri, N. 2022. "Two Explanations for the Paucity of Cyber-Military, Cross-Domain Operations." *Journal of Cybersecurity* 8 (1): tyac002.

Kello, L. 2013. "The Meaning of the Cyber Revolution." *International Security* 38 (2): 7–40.

Kivelä, M., A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter. 2014. "Multilayer Networks." *Journal of Complex Networks* 2 (3): 203–71.

Kostyuk, N. 2021. "Deterrence in the Cyber Realm: Public versus Private Cyber Capacity." *International Studies Quarterly* 65 (4): 1151–62.

Kostyuk, N., and Y. M. Zhukov. 2019. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63 (2): 317–47.

Libicki, M. C. 2016. *Cyberspace in Peace and War*. Arlington: RAND Corporation.

Maness, R. C., B. Valeriano, and B. Jensen. 2019. "Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 1.5." https://www.ryanmaness.com/_files/ugd/4b99a4_4c7971ea7791464a8ac551fff85fb1f1.pdf.

Maoz, Z. 2009. "The Effects of Strategic and Economic Interdependence on International Conflict Across Levels of Analysis." *American Journal of Political Science* 53 (1): 223–40.

Maoz, Z. 2010. *Networks of Nations: The Evolution, Structure, and Impact of International Networks, 1816–2001*. Cambridge: Cambridge University Press.

Maoz, Z. 2011. "The Democratic Networks: Connecting Democratic Peace and International Conflict." *International Studies Quarterly* 55 (1): 1–38.

Maoz, Z., and M. Joy. 2008. "Network Analyses of International Relations." In *The Oxford Handbook of Political Networks*, edited by J. N. Victor, A. H. Montgomery, and M. Lubell. Oxford: Oxford University Press.

Maoz, Z., L. G. Terris, R. D. Kuperman, and E. Shalam. 2007. "What is the Enemy of my Enemy? Causes and Consequences of Imbalanced International Relations, 1816–2001." *Journal of Politics* 69 (1): 100–15.

Pytlak, A., and G. E. Mitchell. 2018. "Power, Rivalry and Cyber Conflict: An Empirical Analysis." In *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, edited by K. Friis, and J. Ringsmose. London: Routledge.

Schulze, M. 2020. "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations." In *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*, edited by T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, and G. Visky. Tallinn: NATO CCDCOE Publications.

Slayton, R. 2017. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41: 72–109.

Valeriano, B., B. Jensen, and R. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press.

Valeriano, B., and R. C. Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11." *Journal of Peace Research* 51 (3): 347–60.

Ward, M. D., K. Stovel, and A. Sacks. 2011. "Network Analysis and Political Science." *Annual Review of Political Science* 14: 245–64.