Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

Network modelling as a tool for cyber diplomacy

Robert Collett

To cite this article: Robert Collett (2024) Network modelling as a tool for cyber diplomacy, Journal of Cyber Policy, 9:3, 377-398, DOI: 10.1080/23738871.2024.2433773

To link to this article: https://doi.org/10.1080/23738871.2024.2433773

Published online: 10 Dec 2024.

JOURNAL OF CYBER POLICY
2024, VOL. 9, NO. 3, 377–398
https://doi.org/10.1080/23738871.2024.2433773

Routledge
Taylor & Francis Group

Network modelling as a tool for cyber diplomacy

Robert Collett

Robert Collett, Developing Capacity, London

ABSTRACT

Visual representations of votes at the UN can assist cyber diplomacy practitioners, researchers and stakeholders in communicating and interpreting voting behaviour. The colour-coded maps that were first used to represent key votes now struggle to capture the complexity and nuances of the cumulative voting record. This article critically examines visualisation methods that have been used in the past. It introduces the advantages of a network model approach and demonstrates how it can be used to visualise a series of diplomacy votes at the UN. Finally, it describes how community detection algorithms can be applied to the network models to identify and better understand middle ground countries in cyber diplomacy.

ARTICLE HISTORY
Received 16 January 2024
Revised 6 August 2024
Accepted 3 October 2024

KEYWORDS
Cybersecurity; cyber diplomacy; United Nations

Introduction

Borrowing from Ernest Hemingway, the transformative power of the internet and associated technologies came to diplomacy at first slowly and then all at once. By the mid-1990s diplomats were observing they still operated in offices run on paper, while modem-connected computers had become ubiquitous in their own homes and on the desks of their private sector peers (Greenhouse 1995). The UK claimed to be the first diplomatic service to catch up, when in 2000 it unshackled its Windows-based IT system and gave staff the ability to email outside government networks and surf the net from a secured network (Select Committee on Foreign Affairs 2001). However, no sooner had its staff gained access to these technologies than they were grappling with the policy consequences of their abuse and deciding how the traditional tools of diplomacy could be deployed to protect them.

At the turn of the millennium, the health of the global email system was deteriorating as increasing volumes of spam clogged its arteries. Domestic legislation and a new generation of spam filters were vital to stemming the problem, but diplomacy also played a role. Amid several international initiatives, the UK convened agencies from 27 governments, plus private sector partners to agree the London Action Plan for spam enforcement cooperation in 2004. 20 years later this community, now renamed the Unsolicited Communications Enforcement Network (UCENet), still helps foster international cooperation to protect email and messaging systems.

CONTACT Robert Collett Robert.Collett@cybercapacity.org
The online version of this article contains colour figures and the print version contains greyscale versions

The early years of cyber diplomacy were marked by uncertainty about what role governments could, should or would play in cyberspace. At one extreme, cyberlibertarians proclaimed that those 'weary giants of flesh and steel … have no sovereignty where we gather' (Barlow 1996). At the other, China was building what *Wired* magazine dubbed a Great Firewall to tightly police the digital realm (Barme 1997). Despite this uncertainty, governments agreed that the UN's convening power could help the world navigate the new policy issues of a digital era.

Multiple tracks of cyber diplomacy negotiations at the UN have generated a growing voting record that should help us map the contours of this new diplomatic landscape, but the methods traditionally used to visualise country voting behaviour have struggled. In particular, colour-coded geographical maps can be misleading and are ill-suited to displaying the volume of voting data the field now has.

Here, we propose using network modelling to visualise and analyse voting records related to cyber diplomacy at the UN. We describe the context of 10 UN votes used in our sample dataset, our methodology and the results of applying a network modelling approach. We provide a practical example of how those results can be used to identify a set of middle ground countries in cyber diplomacy. To triangulate these results, we compare the middle ground identified by a network community detection algorithm with a set of 30 swing states identified by earlier research. We conclude by identifying some practical applications of the network modelling approach and suggestions for future research.

Contested votes in three tracks of cyber diplomacy at the UN

Cyber diplomacy emerged in the past two decades as a means by which states and non-state actors could address issues arising from cyberspace – the networked information systems that include the internet, telecommunications infrastructure and computer systems (Renard 2014, 23–24; Attatfa, Renaud, and Paoli 2020, 60; Barrinha and Renard 2020, 759,764; NIST n.d.).[1]

Where the borders of the cyber diplomacy field should be drawn is not settled (Berthelsen and Nellerod 2021, 20), but it has been described as encompassing, *inter alia*: stability and security in cyberspace; international cooperation to counter cybercrime; and internet governance (Cyber Risk GmbH 2019; Painter 2018; Riordan 2019; United States Department of State 2011). This is not an exhaustive list of issues addressed by cyber diplomacy, but they are significant for this paper because they have each been addressed in negotiations within the UN system that resulted in contested votes, which can be visualised and analysed with network modelling techniques.

The first track of negotiations in the UN system of which this paper makes use for voting data has its origin in a 1998 proposal by Russia for a UN treaty to ban electronic and information weapons. The UN's First Committee (Disarmament and International Security) agreed to create a Group of Government Experts (GGE)[2] in 2004 that went on to reach landmark agreements that international law applies in cyberspace and states should apply non-binding, voluntary norms of responsible behaviour.

The GGE process operated through consensus until 2017, when, for the first time, a round failed to agree a final report. Posited causes of the breakdown include differences over precisely how international law should be applied in cyberspace, but also deeper

ideological attitudes towards internet openness and fundamental freedoms (Henriksen 2019). Attempts to restart negotiations started a chain of contested votes in the UN First Committee between 2018 and 2023 which provide one of the paper's three sources of voting data.

The seven votes this paper uses from the UN First Committee track can be divided into two phases. In the first phase, the United States and Russia championed alternative proposals for how negotiations should be restarted, with the former advocating for a continuation of the GGE and the latter proposing a new Open-Ended Working Group (OEWG)[3] in which all states could participate. Although these were presented as competing alternatives, states effectively declined to choose between them, with both resolutions[4] receiving majority support when they were voted upon in 2018. As a result, both proposed bodies – an OEWG and a new GGE[5] – commenced their work in 2019 despite the risk of duplicating effort and additional cost.

In 2020, Russia tabled a resolution (A/RES/75/240) to reconvene the OEWG for a second four-year round (2021–2025). It was opposed by the United States but comfortably passed.

In the second phase of First Committee voting, member states addressed the question of what should follow the OEWG when it concluded in 2025. In 2022, and again in 2023, the United States and Russia championed competing resolutions with alternative options. The United States advocated for a permanent, inclusive and action-oriented programme of action. Russia proposed a state-centric dialogue that would include elaborating additional legally binding obligations. As before, the First Committee declined the invitation to make a choice between the alternatives. Each time competing resolutions[6] were presented, in 2022 and again in 2023, they secured majority support from UN members.

The second track of negotiations in the UN system upon which this paper draws has been convened under a different pillar of the UN: its Third Committee pertaining to the rule of law. As in the first track of negotiations, it was a Russian proposal in the late 1990s that required a first vote at the UN on cybercrime cooperation. In 1998 and 1999, Russia co-authored resolutions for an Ad Hoc Committee[7] to elaborate an international convention on countering cybercrime (A/RES/73/187 and A/RES/74/247), which critics said was both unnecessary and a threat to human rights (Association for Progressive Communications 2019). Both resolutions were contested but received majority support when voted upon. The Ad Hoc Committee held its first meeting in February 2022 and is due to propose a draft convention to the UN General Assembly in 2024.

The third track of negotiations the paper draws upon occurs at the International Telecommunication Union – an organisation within the UN system that has a mandate to address technical and development issues affecting the stability of cyberspace. In 2012, negotiations over the ITU's mandate led to the earliest vote in this paper's dataset and the first efforts to visualise how countries had voted on an issue within the purview of cyber diplomacy.

The vote in 2012 occurred at the World Conference on International Telecommunications (WCIT). Government representatives had convened to negotiate amendments to a technical treaty governing global standards for telecommunications services, but the vote took on totemic importance for the future of internet governance.

The US claimed the proposed changes to the International Telecommunication Regulations[8] (ITR) posed an existential threat to the multi-stakeholder model of internet

governance and thereby the internet itself (Eckebrecht 2021). 'Father of the Internet' Vint Cerf wrote in the *New York Times* that the internet stood at a crossroads and the amendments had the 'potential to put government handcuffs on the Net' (Cerf 2012). Google launched an online petition opposing the discussion of the internet at the conference (BBC News 2012).

After intense negotiations, the final vote on the amended ITR revealed a divide in international opinion: 89 ITU members voted for the new regulations and 55 refused to sign. 49 UN member states were ineligible to vote for reasons such as unpaid ITU membership fees. The result was a *de facto* deadlock and the anomalous outcome that two versions of the treaty were considered to be operative by two groups of ITU member states (Housen-Couriel 2014, 97). In a *Techdirt* article we will return to later, editor Mike Masnick observed that 'The real story here is a world in which there are two competing visions for the future of the internet – one driven by countries who believe the internet should be more open and free – and one driven by the opposite' (Masnick 2012).

The substantive choices dividing countries in each track were specific to each sub-field of cyber diplomacy, but they shared commonalities. In each track, a similar set of countries championed the competing options, with the United States and the EU among the advocates on one side and Russia and China among those on the other. And common points of disagreement arose across all three tracks, including what role non-state actor 'stakeholders' should have and how much importance should be afforded to protecting human rights and fundamental freedoms (Kim 2014).

How visualising voting behaviour can assist diplomacy

The outcomes of the negotiations described above have consequences for us all. Whether agreement can be reached and what is agreed upon will affect the online services and content users will be able to access and how citizens will be protected from risks ranging from conflict through to the invasion of privacy. Visualisations can play a modest, but not insignificant, supporting role in this diplomacy.

One of the earliest contributions visualising voting behaviour made to cyber diplomacy was explaining, and drawing attention to, what Dietrich and Pawlak (2022) called 'a world divided'. Communicating the extent of the division was a priority around the WCIT 2012 vote and Masnick chose to include a striking red and black map of the vote within his *Techdirt* article because it helped achieve that. The map was also a useful tool for training and briefing cyber diplomats new to the policy area.[9]

Having raised awareness of an issue, one of the next priorities in any diplomatic endeavour is to identify countries with which a productive dialogue can be held to better understand and potentially influence their position. From such dialogues, there is the potential to identify areas of common concern from which conversations and the path to agreement might begin (Riordan 2019, 75). Visualising voting records can assist with this too.

The *TechDirt* map of the WCIT 2012 vote showed, in grey, that a quarter of countries were ineligible to vote and therefore, how they would have voted if they could, had still to be discovered. Later voting visualisations by Dietrich and Pawlak (2022) highlighted that a large group of 74 countries had voting records on cybercrime in the Third Committee negotiations that they classified as neither convergent nor divergent with the EU's.

They used a variety of visualisation methods, which we discuss in the next section, to support their recommendation that the EU's diplomacy focus upon swing states. Diplomats can also use such visualisations as an aid to tracking how the voting behaviour of swing states, or middle ground countries, is changing (or not) over time.

Clarifying terminology: middle ground countries and swing states

We make frequent use of the terms 'middle ground country' and 'swing states' in the following sections of the paper and therefore clarify here what we mean by them.

The term 'middle ground' has different, context-dependent meanings. Most commonly in the literature, when countries are described as middle ground it is to convey that a state's *policy position* is between those of two sides or is yet to be determined.[10] However, 'middle ground' can also be used in the context of *voting records* to describe voting behaviour that is not aligned, or convergent, with either side. At its simplest, if one side voted in favour of a proposal and the other voted against it then those abstaining or not voting could be described as being in a middle ground between the two.

This paper is concerned with visualising and analysing voting records as networks and we therefore use middle ground in the context of voting behaviour relationships. This paper does not attempt to determine the extent to which countries with middle ground voting records hold middle ground policy positions. However, we believe that is an important question for future research and one that we believe network visualisations and analysis can help answer.

A related concept that this paper makes use of is the swing state. Swing states are countries with a mixed political orientation that might shift their position within a diplomatic process and thereby decisively influence its trajectory (Kliman and Fontaine 2012). In addition to Dietrich and Pawlak's work, swing states have been referenced in research on internet governance, stability and security in cyberspace, cybercrime and cyber capacity-building (Klimburg and Zylberberg 2015, 46; Schia 2016, 98–99; Yoo 2018; Homburger 2019, 236; Hurel 2022).

The fact that swing states have a mixed political orientation and that each side would want them to shift their position implies that they have middle ground voting record. This paper makes use of that implied characteristic by triangulating a set of potential middle ground countries identified through network analysis with a list of 30 swing states within internet governance negotiations proposed in 2014 by Morgus and Maurer.

Limitations of existing approaches to visualising cyber diplomacy voting behaviour

As mentioned earlier, one of the first efforts to visualise where countries stood in cyber diplomacy negotiations was a simple map by an anonymous source illustrating how members voted on a revision to the ITR at WCIT (*Country Positions on ITR Proposed at WCIT 2012)*. The map was used in news coverage and post-conference reports at the time, including in *Techdirt*, and has since been referenced in books and articles (Al-Begain et al. 2018; Center for International Media Assistance 2013; Masnick 2012). The map shows the 89 countries that agreed to sign new internet regulations in black and the 55 who joined the United States in refusing to sign in red. Grey was used to indicate

the 49 countries that were ineligible to vote for reasons such as unpaid dues, incorrect credentials or absence.

The WCIT 2012 map powerfully conveys a divided global community but has three shortcomings relevant here. First, it could lead the viewer to overestimate the extent of polarisation by reducing the national positions of countries that were eligible to vote to one of two polar camps: red or black. In the context of electoral vote maps, it has been shown that reducing political complexity to a dichotomised map leads people to overestimate the extent of polarisation (Furrer et al. 2023). Second, the map Figure 1 suffers from the area-size bias, in which geographically larger countries are perceived as more dominant (Schiewe 2019). The third shortcoming is that the WCIT 2012 map in Figure 1 only captures a single moment in time. It would be more useful to have a visualisation that could represent multiple votes and changes in a country's position over time. Despite these shortcomings, the research for this paper found only one prior effort to present alternatives.

Dietrich and Pawlak's 2022 article 'Tracking UN Voting Patterns on Cybercrime' contains several alternative methods for visualising UN voting records. The authors are particularly interested in how strongly countries converged with the EU on four cybercrime votes at the UN and which states moved closer to the EU's voting position over time. To illustrate the strength of convergence they use a divergent bar chart, arranged in a circular layout by region. As examples, Chile's score of +4 indicates it voted identically to the EU four times, while Serbia's score of -3 shows it voted three times the opposite way to the EU and missed one vote (Figure 2).

To visualise the change in national voting behaviour over time, relative to the EU, Dietrich and Pawlak use a diagrammatic cartogram (Figure 3). Every country in the cartogram is equally sized, mitigating the area-size bias problem with geographic maps. However, their chart still only contains two contrasting colours to distinguish between diverging and converging countries. The chart could be altered to illustrate the strength

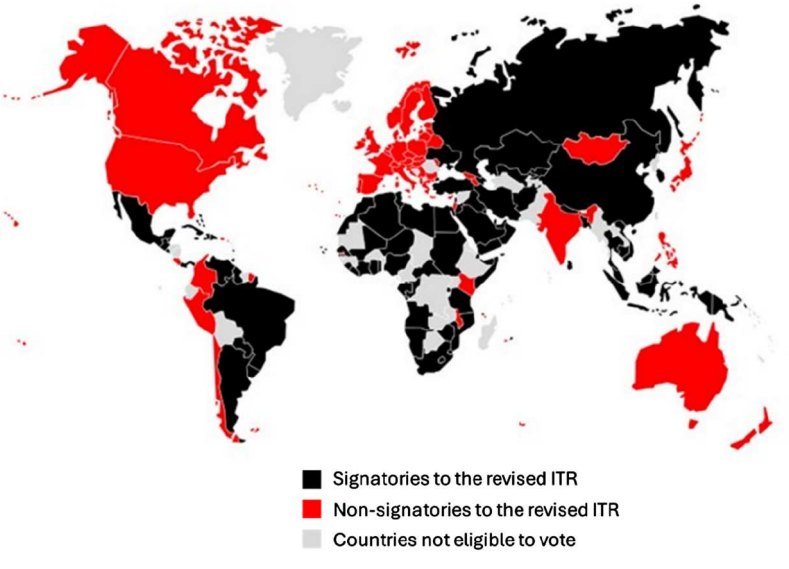

Figure 1. Map of the WCIT 2012 vote on revised International Telecommunication Regulations.[24]

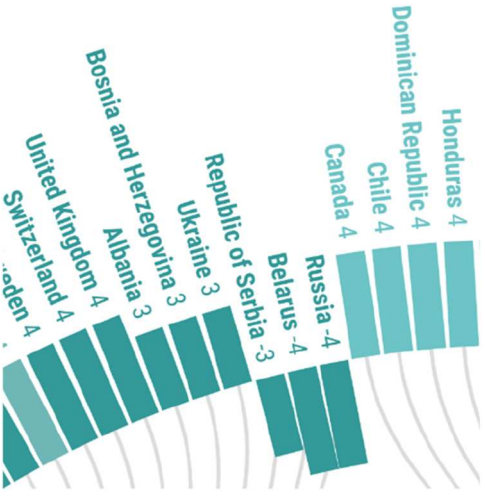

Figure 2. Section of the Convergence Across Resolution Votes chart in Dietrich and Pawlak's 'Tracking UN Voting Patterns on Cybercrime' (2022).

Figure 3. Diagrammatic cartogram illustrating divergence or convergence with the EU over time, from Dietrich and Pawlak's 'Tracking UN Voting Patterns on Cybercrime' (2022).

of divergence or divergence by varying the size of country shapes or adding more colour shades. However, even with these changes a static diagrammatic cartogram will face inherent challenges conveying the dynamic changes in time series data (Calvo, Cucchietti, and Pérez-Montoro 2023). Therefore, the opportunity remains to explore an alternative approach.

Methodology

This paper proposes representing cyber diplomacy votes at the UN as a dynamic network. Network diagrams have been used to model UN voting records before (Ha et al. 2015), but the technique has not been applied in the field of cyber diplomacy and prior work has concentrated on static rather than dynamic networks (Magu and Mateos 2018, 1182). This paper also differs from most previous network modelling of UN voting behaviour in including abstentions and countries not casting a vote when calculating the similarity of voting records (1177).

The dataset used in this paper consists of 10 votes at the UN or its agencies between 2012 and 2023: the WCIT 2012 vote on the final draft ITR, six votes in UN First Committee and two votes in the UN Third Committee.[11]

Methodology for generating a network layout

The paper's dynamic network model was constructed using a similarity metric termed here the Adjusted Voting Record Alignment Score (AVRAS). For each vote in the dataset, an AVRAS was calculated for every dyad of two UN member states. The score represents the degree of voting record alignment between the two countries in the dyad up to and including the vote for which the score is being calculated. It is an adjusted score because it takes account of the fact that there were more Russian-backed than American-backed resolutions in our dataset. The adjustment is made such that a country that consistently votes with Russia on Russian-backed resolutions and with the United States on American-backed resolutions should have the same AVRAS score for its dyad with Russia as it has for its dyad with the United States.[12]

The model's AVRAS similarity metric was calculated in five steps. First, all possible pairings of UN member states were generated, creating 18,528 dyads (Afghanistan-Angola; Afghanistan-Albania; etc.). Every dyad was then assigned a binary value for each voting event to record whether the two countries' voting behaviour aligned (1) or diverged (0) in that vote. In the third step, the voting events were placed in sequential order, earliest to most recent, and the binary values for individual votes were tallied into a cumulative count that represented the voting record thus far after each vote. Fourth, the cumulative count was adjusted to reflect the number of Russian-backed and United States-backed votes up to that point. This was done by dividing the number of times a dyad's votes had aligned in Russian-backed resolutions by the total number of votes that had been held on Russian-backed resolutions and adding this to a value that was calculated in a like manner for United States-backed resolutions. In the fifth and final step, the scores were normalised, so that the maximum AVRAS score a dyad could have after any vote was 1.0.

The formula for the AVRAS between countries i and j after a voting event is represented mathematically as $AVRAS_{ij} = \frac{1}{N}\left(\frac{A_{ijR}}{R} + \frac{A_{ijU}}{U}\right)$. In this formula, R and U represent the number of Russian and United States-backed resolutions in the dataset up to and including the voting event for which the AVRAS is being calculated. A_{ijR} and A_{ijU} represent the number of times that countries i and j aligned in their voting behaviour during the votes held thus far on Russian-backed and United-Stated backed resolutions respectively. The variable N is a normalising factor. When the voting record contained resolutions only backed by one of Russia or the United States, as it did early on, N was set to 1. When the voting record contained resolutions backed by both Russia and the United States, N was increased to 2 so that AVRAS was normalised to a maximum of 1.0.

The next stage in the modelling process was to construct a network graph layout, where each of the 193 countries in the dataset was represented as a node. Nodes were positioned relative to each other in the layout based on the degree of their relative voting alignment, using the AVRAS scores as edge weights. The Force Atlas 2 algorithm was used to generate the layout by applying two forces: one to attract nodes towards each other in proportion to the strength of their voting alignment; and an independent repulsive force to maintain space between nodes. The result is that countries will be positioned close to each if their voting behaviours closely aligned and distanced from each if they did not. Force Atlas 2 was chosen as the network layout algorithm because it retains relational information within the layout and would be relatively accessible to cyber diplomacy practitioners through the open source Gephi software (Bastian, Heymann, and Jacomy 2009; Jacomy et al. 2014).

Methodology for identifying the middle ground countries

This paper applies two statistical methods to identify the middle ground in cyber diplomacy, one simple and the other more sophisticated. The first, simple, statistical method tracks how often each country voted in alignment with the United States as compared with Russia – the two pole countries in the network. We generate a single metric, called the Pole Alignment Tally (PAT), by subtracting the number of times a country voted in alignment with Russia from the number of times it voted with the United States. If a country's action in a vote was in alignment with neither then their PAT would be unchanged after that vote. This results in a linear PAT scale from 10 (alignment in all 10 votes with the United States) to −10 (alignment in all votes with Russia).

The second statistical method we use to identify potential middle ground countries applies an algorithm for community detection within networks. The Leiden algorithm detects communities within a network by seeking to maximise the density of connections within communities while minimising the density of connections between them. We tested a range of resolution settings and found that 0.53 was the optimum with our dataset.[13,14] If a community detected by the algorithm had two or fewer members it was merged with the nearest neighbouring community.

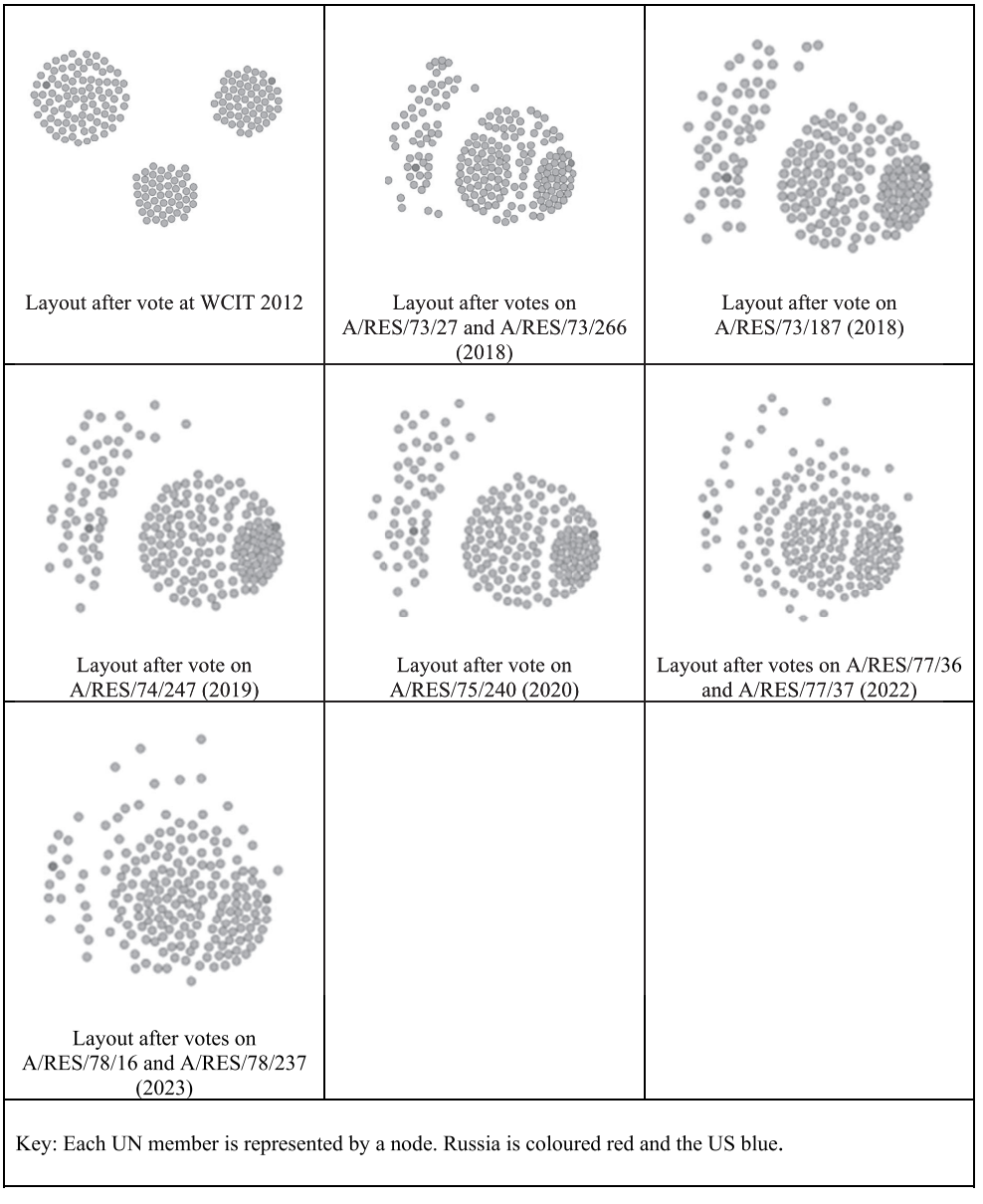

Figure 4. Network representation of UN member voting alignment after 10 cyber diplomacy votes.

Results

Figure 4 illustrates the evolution of the network after each voting event in the dataset. The network has been oriented so that the nodes representing Russia and the US colour-coded red and blue respectively, align along the same plane of the y-axis.

Figure 5 shows the network layout after all 10 votes, colour-coded using the Pole Alignment Tally. Nodes are coloured shades of red for those countries that voted more frequently in alignment with Russia than the United States and blue for the opposite. White nodes

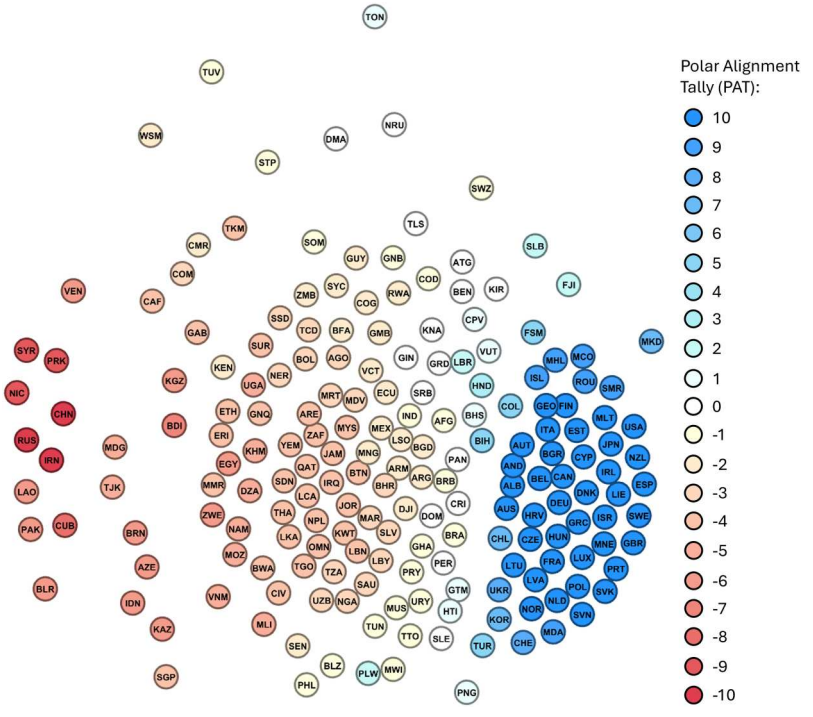

Figure 5. Network representation of UN member voting alignment with Russia and the US after 10 cyber diplomacy votes, coloured using the Polar Alignment Tally.

represent countries that did not vote more frequently with one than the other. The nodes are labelled with the ISO 3166 alpha-3 code to indicate which country they represent.

The final step in the methodology applied the Leiden algorithm to detect communities within the network layout after 10 votes. The algorithm detected seven communities, which are colour-coded in Figure 6.[15]

The table in Figure 7 lists the countries within each community detected by the algorithm and orders the countries within the communities by PAT score so that information from both statistical methods is displayed. Additionally, the 30 swing states identified by Maurer and Morgus are highlighted in bold, as these will be referred to in the next section where we interpret the results (Maurer and Morgus 2014, 7).

Interpreting the results

Having generated a set of network layout visualisations from UN voting recordings we can now consider their utility for identifying middle ground in cyber diplomacy negotiations at the UN. This will expose some of the strengths and weaknesses of network layouts as a way to visualise the field's growing UN voting record.

Turning first to Figure 4, we can identify several useful features of a network layout approach. The first is that clusters of nodes – representing groups of countries with similar voting records – can be identified by simple visual inspection. However, as the number of votes increases so does the complexity of the network and it becomes increasingly difficult to determine objectively by eye where one cluster ends and the next begins.

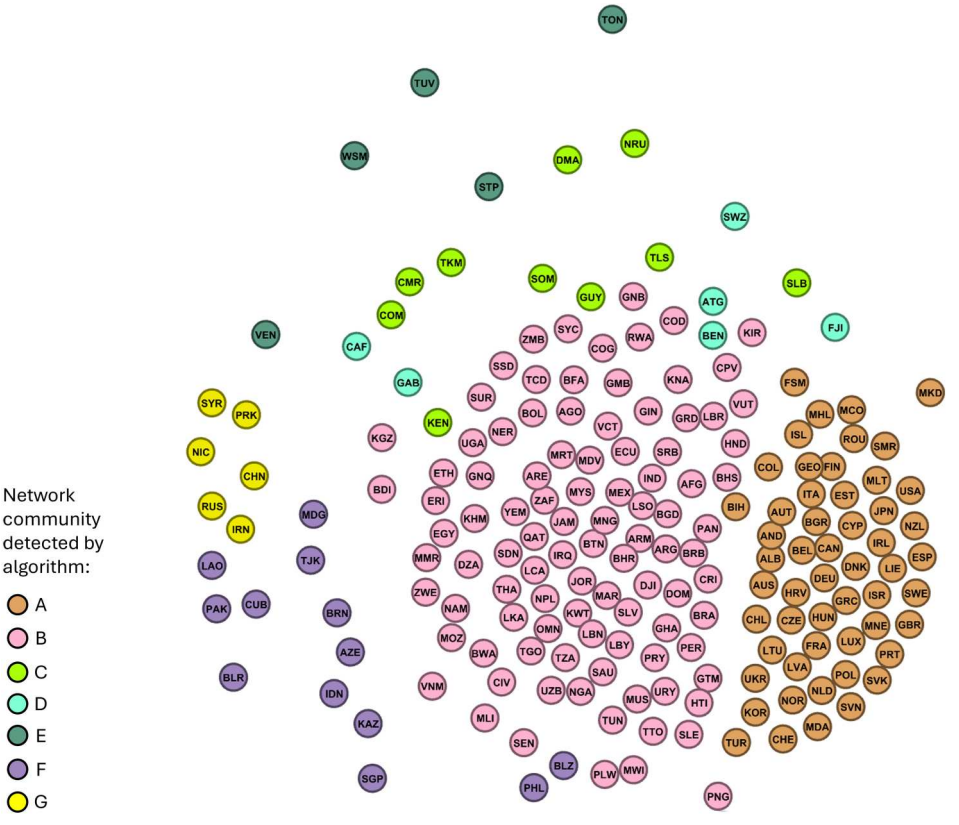

Figure 6. Communities within the network model detected by the Leiden algorithm.

Visual inspection alone is not a reliable way to identify clusters, and additional steps of analysis and colour-coding, such as those used to generate Figures 5 and 6, become necessary.

The second useful feature of the layouts is that the two poles in our network – Russia and the United States – are placed on opposite sides. This provides a visual representation of their divergent voting records and helps convey the concept of a middle ground of countries between the two. However, there is a risk that the user misinterprets this feature of the layout as meaning that the position of the nodes represents a measure of their national policy position. For example, they might wrongly infer that a country node is positioned to the left because it favours a state-centric internet governance model and to the right if it prefers a multi-stakeholder model. To avoid such confusion, network layouts are better suited to contexts where there is an opportunity to explain how the position of country nodes is determined solely by voting record alignment with other countries. That alignment will often reflect a similarity in policy positions on the issues being voted upon, but other factors also influence voting behaviour and sometimes they will better explain alignment. We return to this later when considering the position of Singapore in the network.

The third useful feature is that voting behaviour that metaphorically sets a country apart from most others at the vote will physically set their node apart from others in

PAT	Communities in the network as detected by algorithm
	Community A
10	**ALB Albania**, AND Andorra, AUS Australia, AUT Austria, BEL Belgium, BGR Bulgaria, CAN Canada, CYP Cyprus, CZE Czech Republic, DEU Germany, DNK Denmark, ESP Spain, EST Estonia, FIN Finland, FRA France, GBR United Kingdom, **GEO Georgia**, GRC Greece, HRV Croatia, HUN Hungary, IRL Ireland, ISR Israel, ITA Italy, JPN Japan, LIE Liechtenstein, LTU Lithuania, LUX Luxembourg, LVA Latvia, MLT Malta, MNE Montenegro, NLD Netherlands The, NOR Norway, NZL New Zealand, POL Poland, PRT Portugal, SVK Slovakia, SVN Slovenia, SWE Sweden, USA United States
9	ISL Iceland, MCO Monaco, **MDA Moldova**, MHL Marshall Islands, ROU Romania, SMR San Marino
8	CHE Switzerland, UKR Ukraine
7	CHL Chile, **KOR South Korea**, MKD Macedonia
5	BIH Bosnia and Herzegovina, **COL Colombia**, FSM Micronesia, **TUR Turkey**
3	HND Honduras
	Community B
2	LBR Liberia, PLW Palau
1	BHS Bahamas The, CPV Cape Verde, GTM Guatemala, HTI Haiti, VUT Vanuatu, PNG Papua New Guinea
0	**CRI Costa Rica**, **DOM Dominican Republic**, GIN Guinea, GRD Grenada, KIR Kiribati, KNA St Kitts and Nevis, **PAN Panama**, **PER Peru**, SLE Sierra Leone, **SRB Serbia**
-1	AFG Afghanistan, **BRA Brazil**, BRB Barbados, COD DRC, **GHA Ghana**, GNB Guinea-Bissau, **IND India**, MUS Mauritius, MWI Malawi, PRY Paraguay, TTO Trinidad and Tobago, **TUN Tunisia**, **URY Uruguay**
-2	**ARG Argentina**, **ARM Armenia**, BFA Burkina Faso, BGD Bangladesh, COG Congo, DJI Djibouti, ECU Ecuador, GMB Gambia, LSO Lesotho, **MEX Mexico**, **MNG Mongolia**, RWA Rwanda, SEN Senegal, SYC Seychelles, VCT St Vincent, ZMB Zambia
-3	AGO Angola, BHR Bahrain, BOL Bolivia, LBY Libya, MAR Morocco, MDV Maldives, MRT Mauritania, NER Niger, NGA Nigeria, SAU Saudi Arabia, SLV El Salvador, SSD South Sudan, TCD Chad, TZA Tanzania, UZB Uzbekistan
-4	ARE United Arab Emirates, BTN Bhutan, **BWA Botswana**, CIV Cote d'Ivoire, ERI Eritrea, ETH Ethiopia, GNQ Equatorial Guinea, IRQ Iraq, **JAM Jamaica**, JOR Jordan, KWT Kuwait, LBN Lebanon, LCA St Lucia, LKA Sri Lanka, MMR Myanmar, **MYS Malaysia**, NPL Nepal, OMN Oman, QAT Qatar, SDN Sudan, SUR Suriname, TGO Togo, THA Thailand, YEM Yemen, **ZAF South Africa**
-5	DZA Algeria, KHM Cambodia, MLI Mali, MOZ Mozambique, **NAM Namibia**, UGA Uganda, VNM Vietnam
-6	EGY Egypt, KGZ Kyrgyzstan, ZWE Zimbabwe
-7	BDI Burundi

Figure 7. Communities in the network as detected by the Leiden algorithm.

the network layout.[16] This is most obvious in the case of Tonga's node, which is at the top of the layout in Figures 5 and 6, with the label TON. Tonga only voted three times in the 10 votes in our dataset and on two of those occasions it voted 'No' when the majority voted 'Yes'. As a consequence, Tonga has relatively few connections to other countries in terms of aligned voting behaviour. These connections are what pull nodes towards each other when applying the Force Atlas 2 network layout algorithm, and without them, Tonga's node is pushed out towards the edge of the layout in an isolated position. This visual

Community C	
2	SLB Solomon Islands
0	DMA Dominica, NRU Nauru, TLS East Timor
-1	SOM Somalia
-2	CMR Cameroon, GUY Guyana, **KEN Kenya**
-3	COM Comoros
-4	TKM Turkmenistan
Community D	
2	FJI Fiji
0	BEN Benin, ATG Antigua and Barbuda
-1	SWZ Eswatini
-4	GAB Gabon, CAF Central African Republic
Community E	
1	TON Tonga
-1	STP Sao Tome and Principe, TUV Tuvalu
-2	WSM Samoa
-6	VEN Venezuela
Community F	
-1	BLZ Belize, **PHL Philippines**
-4	SGP Singapore
-5	MDG Madagascar, TJK Tajikistan
-6	AZE Azerbaijan, **BLR Belarus**, BRN Brunei, **IDN Indonesia**, KAZ Kazakhstan, LAO Laos, PAK Pakistan
-8	CUB Cuba
Community G	
-9	NIC Nicaragua, PRK North Korea, SYR Syria
-10	CHN China, IRN Iran, RUS Russia
Key: **Bold** highlighting indicates countries identified as swing states in internet governance diplomacy by Maurer and Morgus.	

Figure 7. Continued.

distinction between tight clusters of like-voting countries at one end and isolated nodes like Tonga's at the other helps the user visualise one of the dynamics of cyber diplomacy.

Having explored some of the benefits of raw network layouts to visualise voting records we can explore how these layouts can help us identify the middle ground in cyber diplomacy when we apply colour coding based on statistical analysis of the voting record. The first, simple statistic we use to colour-code the network is the custom Pole Alignment Tally (Figure 5). This helps highlight a difference at the poles of

the network: only two countries (Iran and China) had a voting record that perfectly aligned with Russia's across all 10 votes, while 38 countries fully aligned with the United States.[17] The middle ground countries must, by definition, lie somewhere between these two poles, but where precisely does it start and end? One way to answer that question would be to ask another: if a country wanted to be in the cyber diplomacy middle ground what PAT score would it have?

A country that wanted to be in the cyber diplomacy middle ground would likely aim for a 'balanced' voting record and there are several ways it might interpret what that meant, each associated with its own PAT score range. We consider three of them here. Under one strict interpretation, to have a balanced voting record is to vote no more frequently for the resolutions backed by one pole than the other. That would result in a PAT score of 0, which 15 countries have after the 10 votes we consider.[18] An alternative strict interpretation would be that a balanced voting record is achieved by voting in support of all resolutions that were tabled, even when – or especially when – that meant voting for competing resolutions.[19] That would result in a PAT score after 10 votes of −4, because Russia backed seven resolutions in our dataset and the United States just three. In our study, 29 countries ended with a PAT score −4 and of these 18 did so because they voted 'Yes' in all 10 votes.[20]

We have considered two strict interpretations of a 'balanced' voting record that result in a single PAT score, but we can also imagine countries having looser interpretations of what being balanced means that would result in a potential range of PAT scores. A country might, for example, consider that they could achieve balance in their voting record by never voting against a resolution or ensuring that a vote against one pole's resolution was later counterbalanced by a vote against a resolution proposed by the other pole. A country following one of these looser interpretations would have a PAT score between −7 and 3. If we use PAT scores alone to identify the middle ground, that would mean it potentially contains up to 132 countries – the number with PAT scores in that range.[21] It is possible that two thirds of UN members are in the cyber diplomacy middle ground, but it would be useful to triangulate that with another approach. For this, we can turn to the results of the community detection algorithm.

As described in the results section, our method for applying the Leiden algorithm detected six communities within the network after 10 votes. Two of these – A and G – we call the polar communities because they contain the two poles in the network, the United States and Russia. Community A contains 54 countries, including the United States. Community G contains six countries, including Russia. That leaves 133 countries in the four other communities the algorithm detected – a number only one away from the 132 with a PAT score in the range −7 to 3. We can now consider whether each of the other algorithmically-detected communities (B through F) should be considered part of the middle ground or whether any would be better described as satellites of a polar community.

Community B occupies the central area in the network layout after 10 votes and therefore has the strongest claim to be within the cyber diplomacy middle ground. It contains 99 countries, all of which have PAT scores between −7 and 3, which we earlier identified as the range that a country seeking a balanced voting record would be within.[22]

Communities C, D and E are positioned at the top of the network in more isolated positions. This reflects their relative disengagement from voting: 19 of the 21 countries

in these communities missed at least four votes.[23] An inspection of country voting records suggests the algorithm is distinguishing between these less engaged communities based upon recent voting behaviour. The members of Community E missed all four votes in 2022 and 2023. Those in Community D cast more votes in 2022 than 2023, while those in Community C cast more votes in 2023 than 2022. We might describe these three communities as the less engaged middle ground in cyber diplomacy at the UN.

The last non-polar community detected by the algorithm is F, which might be best described as a borderline community of the middle ground. Some of its constituent countries – Laos, Pakistan, Belarus and Cuba – have nodes that are placed in close proximity to Russia within the network layout. Others, including Singapore, the Philippines and Belize have nodes that are closer to the edge of Community B. A grouping of countries based on their public policy positions would be unlikely to put Belarus and Singapore together, but an advantage of the community detection algorithm is that it identify similarities in UN voting records we might not have noticed or considered otherwise. It is therefore worth examining what the countries within Community F have in common and what they do not.

A characteristic that Community F countries have in common is that they all abstained, in 2022, on A/RES/77/37, backed by the US. This appears to have been a key factor in the algorithm grouping these countries as a community. However, we know from statements countries gave to explain their votes that the motives behind these abstentions can vary considerably. As an example, Singapore and Cuba are both in Community F and voted the same way in seven of the 10 votes we consider, including abstaining on the US resolutions in 2022 and 2023. Singapore has explained that its abstentions was a demonstration of neutrality on OEWG matters following Singaporean Ambassador Burhan Gafoor's appointed as the working group's Chair in 2021 (Ministry of Foreign Affairs Singapore 2022). In contrast, Cuba said its own abstentions were motivated, *inter alia*, by inclusion within the resolutions of a universal affirmation of the applicability of international law in cyberspace (United Nations 2023). On this important policy issue, Cuba resists the principle that international law is automatically applicable in cyberspace, while Singapore believes 'adherence to international law [in cyberspace] is essential' (United Nations 2021, 83). This illustrates how two countries with divergent positions on one of the key issues within a resolution can nonetheless both vote in the same way, and thereby be placed in the same voting community by the algorithm, because of factors unrelated to the substance of the resolution.

Returning to the question of how we categorise Community F, it cannot be neatly classified as either wholly in the middle ground or wholly out of it. Using purely statistical methods, it contains countries with PAT scores as far apart as −1 and −8. We therefore categorise it as a mixed community.

As a final triangulation check on the validity and utility of an algorithmic approach to detecting communities in the cyber diplomacy voting network, we can compare our results to the swing states identified by Maurer and Morgus (2014). We would expect to find the swing states within the middle ground communities identified by the algorithm. In Figure 7, we can see that 24 of their 30 swing states (highlighted in bold) are in Communities B, C and F, which we defined as either middle ground or mixed. However, six are in A, which is a polar community. Either the algorithm is placing

swing state middle ground countries in polar communities or these countries are no longer swing states.

Examining the voting records of the six Maurer and Morgus swing states in Community A reveals that five have voted uniformly against the Russian-backed resolutions in our dataset since 2019. If these were swing states 10 years ago then it would be reasonable to conclude from this record that they have now 'swung' towards the US camp. This is most obvious in the cases of Albania and Georgia, which have voted in alignment with the US in all 10 votes we consider. The one country that continues to exhibit middle ground characteristics among the six is Colombia. Colombia does show signs of a shift in voting behaviour: it voted for the Russian-backed resolution in 2018, but voted against, or abstained on, every Russian-backed resolution since then, while consistently supporting those backed by the US. However, in 2022 and 2023, Colombia abstained on the Russian-backed resolutions and that could be consistent with a middle ground position during this period.

Regarding the presence of former swing states in Community A, we conclude that the community detection algorithm has helpfully identified the shift of five swing states away from the middle ground and that it is too soon to reach a conclusion on the sixth, Colombia. This is further evidence that a network analysis can lead to useful insights for cyber diplomacy and points to potential future research examining what influenced former swing states to shift their position and which countries are the new swing states.

Conclusion

Network modelling offers distinct advantages over the alternatives previously used for visualising and analysing country voting records at the UN, especially colour-coded geographical maps. It is better able to handle large voting records, avoids the problem of area-size bias, reduces the risk that users overestimate the extent of polarisation and visually conveys the concept of middle ground countries. Network visualisations can also be created that are dynamic, rather than static, to illustrate changes in voting behaviour over time.

Generating network layouts from multiple votes, we found that it soon became difficult to identify clusters of like-voting countries by eye with confidence. However, the application of simple and more advanced statistical methods mitigated this limitation. The Leiden community detection algorithm proved especially useful for identifying the polar communities and middle ground countries in the network. The algorithm also detected communities with distinct features, such as lower engagement levels, which could inform both future research and projects aimed at increasing participation in cyber diplomacy negotiations. Measures of country engagement, such as the combined duration of country's interventions, could be used to adjust the node sizes and visually represent which countries were heard in negotiating sessions.

Another potential use for network models in cyber diplomacy research is as a tool to help identify factors that influence a country's voting behaviour. Network diagrams and algorithmic identification of like-voting communities provide visual and statistical cues that a country has changed its voting behaviour relative to other states, prompting investigation into the underlying drivers of such changes.

Finally, we encourage experimentation with different cyber diplomacy datasets. We chose to use voting records from three prominent tracks, but the methodology described here could be applied and adapted to any set of voting records or other types of connection between countries, such as membership of international organisations or the endorsement of international declarations.

As the terrain of cyber diplomacy continues to evolve, so too must its analytical toolkit. Network modelling is a powerful tool that can help us better understand the landscape and dynamics of cyber diplomacy with applications for researchers and practitioners alike.

Notes

1. Cyber diplomacy is now considered to be distinct from digital diplomacy – the use of modern communications channels to directly inform or influence foreign audiences – although the two were once conflated (Pahlavi 2003; Riordan 2019, 5; Attatfa, Renaud, and Paoli 2020, 61).
2. UN Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.
3. UN Open-Ended Working Groups on security of and in the use of ICTs.
4. A/RES/73/266 authored by the United States and A/RES/73/27 by Russia.
5. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.
6. The Russian-based proposal was presented in A/RES/75/240 in 2022 and A/RES/78/237 in 2023. The alternative supported by the United States was presented in A/RES/77/37 in 2022 and A/RES/78/16 in 2023.
7. The Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.
8. The International Telecommunication Regulations were agreed by ITU members in 1988 as a set of general principles for the provision and operation of international telecommunication services. The original ITR included no mention of the internet, which was in its infancy in 1988. The debate at WCIT 2012 centred around upon whether and how the ITR should be amended to include provisions directly affecting the internet. Five amendments in the final draft were particularly contentious: a right for States to access the internet, which might limit the application of international sanctions; extending the ITR's scope to internet service providers; adding a reference to security; encouraging member states to take measures against spam email, which was an extension of the ITR into the internet domain and, it was argued, set the dangerous precedent of empowering governments to decide which emails should be blocked based on their content; and a reference to the World Summit on the Information Society (WSIS) in 2003 that would implicitly reinforce that 'authority for internet-related public policy issues is the sovereign right of States' without a counterbalancing statement acknowledging the effectiveness of multi-stakeholder model of internet governance (Eckebrecht 2021, 19–21).
9. Author's own experience as a diplomat in the Cyber Policy Department of the UK Foreign Office.
10. For example, Van Raemdonck (2021) uses the term middle ground to describe South Africa's position on a new cybercrime treaty and that insight informs her paper's recommendations for the EU's digital dialogue with Africa (Van Raemdonck 2021, 35).
11. 2018, A/RES/73/266 – A First Committee resolution, backed by the United States, for another round of the UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace. 2018, A/RES/73/27 – A competing First Committee resolution, backed by Russia, that would expand these discussions to include all UN members through an Open-Ended Working Group (OEWG). 2018, A/RES/73/187 – A Third Committee resolution, backed by Russia, to seek member state views on cybercrime, with an eye to launching a process that could result in a cybercrime treaty. 2019, A/RES/74/247 – A Third

Committee resolution, backed by Russia, to create an open-ended Cybercrime Ad Hoc Committee. 2020, A/RES/75/240 – A First Committee resolution, backed by Russia, creating a follow-on OEWG, to run from 2021 to 2025. 2022, A/RES/77/37 – A First Committee resolution, backed by the United States, proposing a programme of action. 2023, A/C.1/78/L.11 – A First Committee resolution, backed by Russia, preparing the ground for a programme of action at the UN to follow on from the 2021–2025 OEWG institutional dialogue at the UN on security in the use of ICTs after the conclusion of 2021–2025 OEWG 2023, A/C.1/78/L.60/Rev.1 A competing First Committee resolution, backed by the United States, elaborating on a programme of action to follow the 2021–2025 OEWG.

12. Importantly, cyber diplomacy is more complex than a competition between American and Russian visions for cyberspace. However, for the purpose of introducing network modelling as a tool for cyber diplomacy and identifying communities within the network, it is helpful to account for the fact that Russia has authored more cyber diplomacy resolutions than the United States. This adjustment results in network layouts in which it is easier to visually identify communities of like-voting countries and, in which, countries that consistently for both American and Russian resolutions are positioned closer to the centre. The previous footnote describes which country backed each resolution in the First and Third Committees. The final draft ITR text at WCIT 2012 was backed by Russia and opposed by the United States.
13. The settings we used for the Leiden algorithm plugin within the Gephi package were: resolution 0.53; Constant Potts Model quality function; 10 iterations; 1 restart; make use of edge weights; and starting seed 0.
14. Setting the resolution when using the Leiden community detection algorithm is a subjective task guided by the number and size of the communities one wants to detect, the purpose of the analysis and knowledge of the context. If the resolution is set too low the algorithm just detects one community (i.e. the whole network) and if it is set too high it will treat every node as its own community. When selecting a resolution we optimized for two factors: detecting a small number of communities (<10) to allow a discussion of each within the length of this paper; and avoiding the inclusion of countries that might be trying to pursue a 'balanced', middle ground voting record in the polar communities, with Russia and the United States. We discuss what a 'balanced' voting record means when interpret the results, but in brief we looked at whether any countries with a PAT score between -6 and 3 were in the detected polar communities, and, if they were, whether they had voted in opposition to a resolution.
15. The algorithm also detected one other community, but as this contained only two countries it was merged with the nearest neighbouring community, as per our methodology.
16. This feature results from using a layout algorithm, Force Atlas 2, that mimics physical forces of attraction and repulsion. It would not necessarily be a feature of layouts generated by other algorithms.
17. For a list of the countries see those in Figure 7 with a PAT score of 10 or -10. In Figure 5 these countries are colour-coded with the darkest shades of blue and red respectively.
18. The nodes of these 15 countries are colour-coded white in Figure 5. They are listed in Figure 7 within communities B, C and D.
19. 47 countries voted three times in favour of competing resolutions in 2018, 2022 and 2023.
20. The 18 countries that voted in favour each time were Bhutan, Iraq, Jamaica, Jordan, Kuwait, Lebanon, Malaysia, Nepal, Oman, Qatar, South Africa, Sri Lanka, St Lucia, Sudan, Togo, Thailand, the United Arab Emirates and Yemen.
21. Of these 132, 100 countries achieved a PAT score between -6 and 3 while never voting against a resolution.
22. This does not mean that every country within Community B was seeking a balanced voting record, but it does mean that Community B does not contain any countries whose PAT scores would imply had an 'unbalanced' voting record.
23. The exceptions are Kenya and Guyana in Community C. These countries only missed two votes and one vote respectively. However, they both missed the vote on A/RES/77/37 and the fact that all other members of Community C also missed that vote appears to have been enough for the algorithm to group them with C rather than placing them in Community B.

24. Coloured versions of the following diagrams are available in the online version of this article

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Robert Collett is a researcher, adviser and trainer specialising in cybersecurity capacity-building. He is a Chatham House Associate Fellow and founder of Developing Capacity Ltd. From 2019 to 2020, he was the UK's first seconded senior adviser to the Global Forum of Cyber Expertise (GFCE). Prior to this he ran, and grew threefold, the UK's international cybersecurity capacity-building programmes. Robert has a 17-year track record leading programmes and policy initiatives as a UK diplomat, working at the intersection of foreign policy, security and development in Iraq, Afghanistan and Sierra Leone.

ORCID

Robert Collett http://orcid.org/0000-0002-8594-6035

References

Al-Begain, K., C. Turyagyenda, M. Zak, and W. Alosaimi. 2018. *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global.

Association for Progressive Communications. 2019. "Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online." Association for Progressive Communications. November 6. https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.

Attatfa, Amel, Karen Renaud, and Stefano De Paoli. 2020. "Cyber Diplomacy: A Systematic Literature Review." *Procedia Computer Science* 176:60–69. https://doi.org/10.1016/j.procs.2020.08.007.

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation. February 8. https://www.eff.org/cyberspace-independence.

Barme, Geremie R. 1997. "The Great Firewall of China." *Wired*, 1 June 1997. https://www.wired.com/1997/06/china-3/.

Barrinha, André, and Thomas Renard. 2020. "Power and Diplomacy in the Post-Liberal Cyberspace." *International Affairs* 96 (3): 749–766. https://doi.org/10.1093/ia/iiz274.

Bastian, Mathieu, Sebastien Heymann, and Mathieu Jacomy. 2009. "Gephi: An Open Source Software for Exploring and Manipulating Networks." *Proceedings of the International AAAI Conference on Web and Social Media* 3 (1): 361–362. https://doi.org/10.1609/icwsm.v3i1.13937.

BBC News. 2012. "Google Attacks UN's Internet Treaty Conference." November 21, sec. Technology. https://www.bbc.com/news/technology-20429625.

Berthelsen, Emilie, and Johan Nellerod. 2021. "Cyber Diplomacy at the United Nations: The Endeavours of the European Union and China to Determine Responsible State Behaviour in Cyberspace." https://doi.org/10.13140/RG.2.2.23752.80649

Calvo, Luz, Fernando Cucchietti, and Mario Pérez-Montoro. 2023. "Measuring the Effectiveness of Static Maps to Communicate Changes Over Time." *IEEE Transactions on Visualization and Computer Graphics* 29 (10): 4243–4255. https://doi.org/10.1109/TVCG.2022.3188940.

Center for International Media Assistance. 2013. "Governments, Gatekeepers, and Journalists." Center for International Media Assistance. https://www.cima.ned.org/wp-content/uploads/2015/02/WPFD-Summary-04-22-13-FINAL-for-website.docx.

Cerf, Vinton G. 2012. "Opinion | Keep the Internet Open." *The New York Times*, 24 May 2012, sec. Opinion. https://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html.

'Country Positions on ITR Proposed at WCIT 2012'. 2012. https://ipv.sx/wcit/.

Cyber Risk GmbH. 2019. "What Is Cyber Diplomacy?" The Cybersecurity Toolbox. 2019. https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html.

Dietrich, Christian, and Patryk Pawlak. 2022. "Tracking UN Voting Patterns on Cybercrime." Directions. 1 February 2022. https://directionsblog.eu/tracking-un-voting-patterns-on-cybercrime/.

Eckebrecht, Felicitas. 2021. "Much Ado about Nothing? The Controversy about the International Telecommunication Regulations and Internet Governance." SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.3796242

Furrer, Rémy A., Karen Schloss, Gary Lupyan, Paula M. Niedenthal, and Wood. Adrienne. 2023. "Red and Blue States: Dichotomized Maps Mislead and Reduce Perceived Voting Influence." *Cognitive Research: Principles and Implications* 8 (1): 11. https://doi.org/10.1186/s41235-023-00465-2.

Greenhouse, Steven. 1995. "The State Department: A Snail in Age of E-Mail." *The New York Times*, March 6. https://www.nytimes.com/1995/03/06/world/the-state-department-a-snail-in-age-of-e-mail.html.

Ha, Hyoji, Seongmin Mun, Oh-Hyun Kwon, and Kyungwon Lee. 2015. "Proximity Based Circular Visualization for Similarity Analysis of UNGA Voting Patterns." *In 2015 Big Data Visual Analytics (BDVA)*, 1–2. IEEE. https://doi.org/10.1109/BDVA.2015.7314300.

Henriksen, Anders. 2019. "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace." *Journal of Cybersecurity* 5 (1): 1–9. https://doi.org/10.1093/cybsec/tyy009.

Homburger, Zine. 2019. "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace." *Global Society* 33 (2): 224–42.

Housen-Couriel, Deborah. 2014. "The "Dubai Clash" at WCIT-12: Freedom of Information, Access Rights, and Cyber Security." Law and National Security: Institute for National Security Studies. https://www.jstor.org/stable/resrep08957.9.

Hurel, Louise Marie. 2022. "The Rocky Road to Cyber Norms at the United Nations." *Council on Foreign Relations* (blog). 6 September 2022. https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0.

Jacomy, Mathieu, Tommaso Venturini, Sebastien Heymann, and Mathieu Bastian. 2014. "ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software." *PLoS One* 9 (6): e98679. https://doi.org/10.1371/journal.pone.0098679.

Kim, Sangbae. 2014. "Cyber Security and Middle Power Diplomacy: A Network Perspective." *The Korean Journal of International Studies* 12 (2): 323. https://doi.org/10.14731/kjis.2014.12.12.2.323.

Klimburg, Alexander, and Hugo Zylberberg. 2015. "Cyber Security Capacity Building: Developing Access." NUPI Report 6. Norwegian Institute of International Affairs. https://www.nupi.no/publikasjoner/cristin-pub/cyber-security-capacity-building-developing-access.

Kliman, Daniel M., and Richard Fontaine. 2012. "Global Swing States: Brazil, India, Indonesia, Turkey and the Future of International Order." Center for a New American Security. https://www.jstor.org/stable/resrep06364.

Magu, Rijul, and Gonzalo Mateos. 2018. "United Nations General Assembly Vote Similarity Networks." In *Complex Networks & Their Applications VI*, edited by Chantal Cherifi, Hocine Cherifi, Márton Karsai, and Mirco Musolesi, 1174–1183. Studies in Computational Intelligence. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-72150-7_95.

Masnick, Mike. 2012. "Who Signed The ITU WCIT Treaty … And Who Didn't." Techdirt. December 14. https://www.techdirt.com/2012/12/14/who-signed-itu-wcit-treaty-who-didnt/.

Maurer, Tim, and Robert Morgus. 2014. 'Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate'. Centre for International Governance Innovation- Internet Governance Papers. https://www.cigionline.org/static/documents/no7_2.pdf.

Ministry of Foreign Affairs Singapore. 2022. "Singapore's Explanation of Vote at the 77th United Nations General Assembly First Committee." November 3. http://www.mfa.gov.sg/Overseas-Mission/New-York/Mission-Updates/First_committee/2022/11/20221103.

NIST. n.d. *Glossary - Cyberspace*. NIST Computer Security Resource Center. Accessed 27 November 2023. https://csrc.nist.gov/glossary/term/cyberspace.

Pahlavi, Pierre Cyril. 2003. *Cyberdiplomacy: Managing Security and Governance Online*. Cambridge: Polity Press. https://www.wiley.com/en-gb/Cyberdiplomacy%3A+Managing+Security+and+Governance+Online-p-9781509534074.

Painter, Chris. 2018. "Diplomacy in Cyberspace." *The Foreign Service Journal* 95 (5): 26–27. https://afsa.org/diplomacy-cyberspace

Renard, Thomas. 2014. "The Rise of Cyber-Diplomacy."

Riordan, Shaun. 2019. *Cyberdiplomacy: Managing Security and Governance Online*. Cambridge: Polity Press. https://www.wiley.com/en-gb/Cyberdiplomacy%3A+Managing+Security+and+Governance+Online-p-9781509534074.

Schia, Niels. 2016. "Cyber Security Capacity Building, Digitalization and the Global South." *European Cybersecurity Journal* 2 (January): 82–94.

Schiewe, Jochen. 2019. "Empirical Studies on the Visual Perception of Spatial Patterns in Choropleth Maps." *KN - Journal of Cartography and Geographic Information* 69 (3): 217–228. https://doi.org/10.1007/s42489-019-00026-y.

Select Committee on Foreign Affairs. 2001. "Written Evidence - Memorandum from the Foreign and Commonwealth Office on The FCOD's ICT (Appendix 6)." December 2001. https://publications.parliament.uk/pa/cm200102/cmselect/cmfaff/826/826ap07.htm.

United Nations. 2021. "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266." A/76/136. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

United Nations. 2023. "First Committee Coalesces Around UN Disarmament Machinery Drafts, But Differences Persist over "ICT" Security, Regional Disarmament in Mediterranean Region | Meetings Coverage and Press Releases." GA/DIS/3732. https://press.un.org/en/2023/gadis3732.doc.htm.

United States Department of State. 2011. International Cyber Diplomacy: Promoting Openness, Security and Prosperity in a Networked World." United States Department of State. 14 July 2011. https://2009-2017.state.gov/r/pa/pl/168689.htm.

Van Raemdonck, Nathalie. 2021. "Digital Dialogue: Africa as a Cyber Player." European Union Institute for Security Studies (EUISS). https://eucyberdirect.eu/wp-content/uploads/2021/01/digital-dialogue-africa-final.pdf.

Yoo, Joonkoo. 2018. "Recent Trend of Cyber Security Governance and Challenges". IF2017-77E. IFANS Focus. Institute of Foreign Affairs and National Security. https://www.ifans.go.kr/knda/com/fileupload/FileDownloadView.do?storgeId=c61b04e5-0182-4c75-ad21-828ecacfb855&uploadId=11965809541958586&fileSn=1.