Complexity of International Law for Cyber Operations

Nazli Choucri

Professor
Political Science Department
Massachusetts Institute of Technology

Gaurav Agarwal

Alumnus
Sloan School of Management
Massachusetts Institute of Technology

November 8, 2021

Abstract

Policy documents are usually written in text form—word after word, sentence after sentence etc.—which often obscures some of their most critical features. Text cannot easily situate interconnections among elements, or identify feedback, nor reveal other embedded features. This paper presents a computational approach to International Law Applicable to Cyber Operations 2.0, Tallinn Manual, a seminal work of 600 pages at the intersection of law and cyberspace. The results identify the dominance of specific Rules, the centrality of select Rules, and Rules with autonomous standing, as well as the feedback structure that holds the system together. None of these features are evident from the text alone.

Keywords

Tallinn Manual 2.0, cyber operations, international law, law of war, network theory.

Citation: Choucri, N., & Agarwal, G. (2021). Complexity of international law for cyber operations. *Proceedings of the 2021 IEEE International Symposium on Technologies for Homeland Security (HST)*, 1–7.

Unique Resource Identifier: https://doi.org/10.1109/HST53381.2021.9619833

Version: Author's final manuscript.

Complexity of International Law for Cyber Operations

1 Introduction

The international community is now on the verge of a major challenge: How to frame the relationship between international law and cyberspace. One analyst observes that there is a "simple choice," that is, between "[m]ore global law and a less global internet" [1]. Another reminds us that the most "important point" is that "all ground occupied by international law is shared by others who are not lawyers" [2]. Noteworthy in this connection are the multifaceted arguments for "mapping an emergent jurisprudence" [3], supported by the illustration of ways that "scholars are using complexity theory to make sense of law" [3]. See, for example [4].

Informed by complexity theory, this paper presents a computational analysis of *International Law Applicable to Cyber Operation*, *Tallinn Manual 2.0* [5] and illustrates new ways of analyzing policy documents in order to (a) extend the conventional sequential representation of policy, (b) create transparency in the system, for the "whole" and for its "parts," (c) clarify diverse interconnections among policy components, and (d) help identify embedded policy feedback, as well as (e) explore contingencies such as, "what if…?" Although complexity theory is well recognized in the scientific community [6–11], as is the development of complexity science, there are few directives for exploring its relevance to law and order for cyberspace.

The text of *Tallinn Manual 2.0* [5] serves as the "raw data" for our investigation. A policy document of nearly 600 pages, this text-as-conduit imposes a powerful sequential logic in an otherwise complex and interconnected set of policy directives. Developed at the NATO Cooperative Cyber Defense Center of Excellence, *Tallinn Manual 2.0* is viewed as "a reflection of the law as it existed at the point of the Manual's adoption" [5]. It extends and supersedes the legal principles put forth in *International Law Applicable to Cyber Warfare* [12] to include "the public international law governing operations during peacetime" [5].

2 Method of Inquiry

Our approach consists of a chain of computational moves, each intended to generate specific outputs and, jointly, designed to identify different properties of the legal corpus.

2.1 From Policy Text to System Structure

The first step is to construct a system structure for the *Tallinn Manual 2.0* that mirrors the organization of the policy text. The structure is generated from the text in the form of a Design

Structure Matrix (DSM), also known as a Dependency Structure Matrix. First proposed in 1962 [13], DSM is an information exchange method for representing interactions among the elements of a system. Browning and collaborators [14, 15] illustrate various DSM applications, and highlight their use in the areas of engineering design, engineering management, management/organization science, and systems engineering.

When completed, the system structure provides the venue through which the incidence or occurrence of *Rules*, and their connection to other *Rules*—as stated in the text—are recorded. When completed, the result is a 154 by 154 matrix (rows and columns), This approach is "low risk," as it is anchored in the organization of the *Tallinn Manual 2.*0 and built on its most basic element, the *Rule.*

2.2 From System Structure to Base Metrics

Next is to generate metrics for the basic elements. We begin with a binary metric ("yes/no,"), whether a *Rule* commentary or footnote (in a row) refers to another *Rule* (in a column). The result is a system structure "populated" by empirically derived observations. This structure, the *reference* (or base case) DSM, is the most elemental representation *Tallinn Manual 2.0* for both structure and content.

2.3 From System Structure to Summed Frequency Metrics

If we record the frequency with which a *Rule* (in a row) refers to another *Rule* (in a column) in its commentary, including the footnotes, the entry in each cell shows the summed incidence of relationships at the cell level. Appendix 1 presents *Tallinn Manual 2.0* in DSM form by *Rule* frequency. By replacing the numeric value in a cell in Appendix 1 with a binary measure (i.e., "1" as incident and "0" for blank cell) generates the *reference* (or base case) DSM. The system structure (154 by 154) of *Tallinn Manual 2.0* remains unchanged. By definition, we would expect the numeric in the DSM cells and the characteristic features of the network forms to signal different features of the system when compared to the base case.

2.4 From Metrics to Network Models

So far, we focused on foundational tasks to enable the construction of network models for more nuanced and informative analysis. We begin with the binary-form DSM to generate the reference network model in order to provide a "neutral" (binary) view of the system structure. Then we replace the binary form with summed incidences to generate a content-rich DSM and allow for more detailed investigations.

The remainder of this paper turns to network analyses, results, and attendant implications.

3 Base Case – Reference System

Derived from binary DSM, Fig. 1 displays the reference case for the network architecture of *Tallinn Manual 2.0*. Each *Rule* is shown as a node (with the edge or interface connecting any two *Rules*). This Figure includes all *Rules* listed sequentially in *Tallinn Manual 2.0* and identifies the *Part* in which each *Rule* is situated. Note that all *Rules* are displayed as identical in size—all are shown to be "equal" in the system structure. Further, all connections (i.e. interfaces or edges) between *Rules* are also displayed as "equal."

While minimalist in content, the base network model signals notable features of *International Law for Cyber Operations* that cannot be observed in text form. These include:

1. *Asymmetry of content disitribution* throughout the policy document;
2. *Rule density* signaled by the *Part* with the most *Rules* and least connections to other *Parts,* (such as in *Part* I and *Part* IV);
3. *Rule influence* indicated by the dominance of *Rules* referenced in other *Rules*, and
4. *Stand-alone* or autonomous *Rules*, i.e., those that remain unconnected to any other *Rule*.

At the same time, Figure 1 shows a network distinguished by what is known as a "display of affinity." Note, for example, the discernable clustering of *Rules* in *Part* I on *International Law*, situated on one side of the network, and a similarly notable clustering of *Rules* in *Part* IV on *Law of Armed Conflict* situated on the opposite side. We return to these, and related issues, later on.

We now turn to introduce a major departure from the reference network model (Figure 1) by weighing the edges—the interface connecting any two *Rules*—with the number of references made by a *row Rule* to a *column Rule* (Figure 2). The results draw attention to three notable network features: the (a) direction of arrows, (b) source and destination, and (c) width of connection, that is, edge or interface. Even the most cursory view reveals the variability across the system structure.

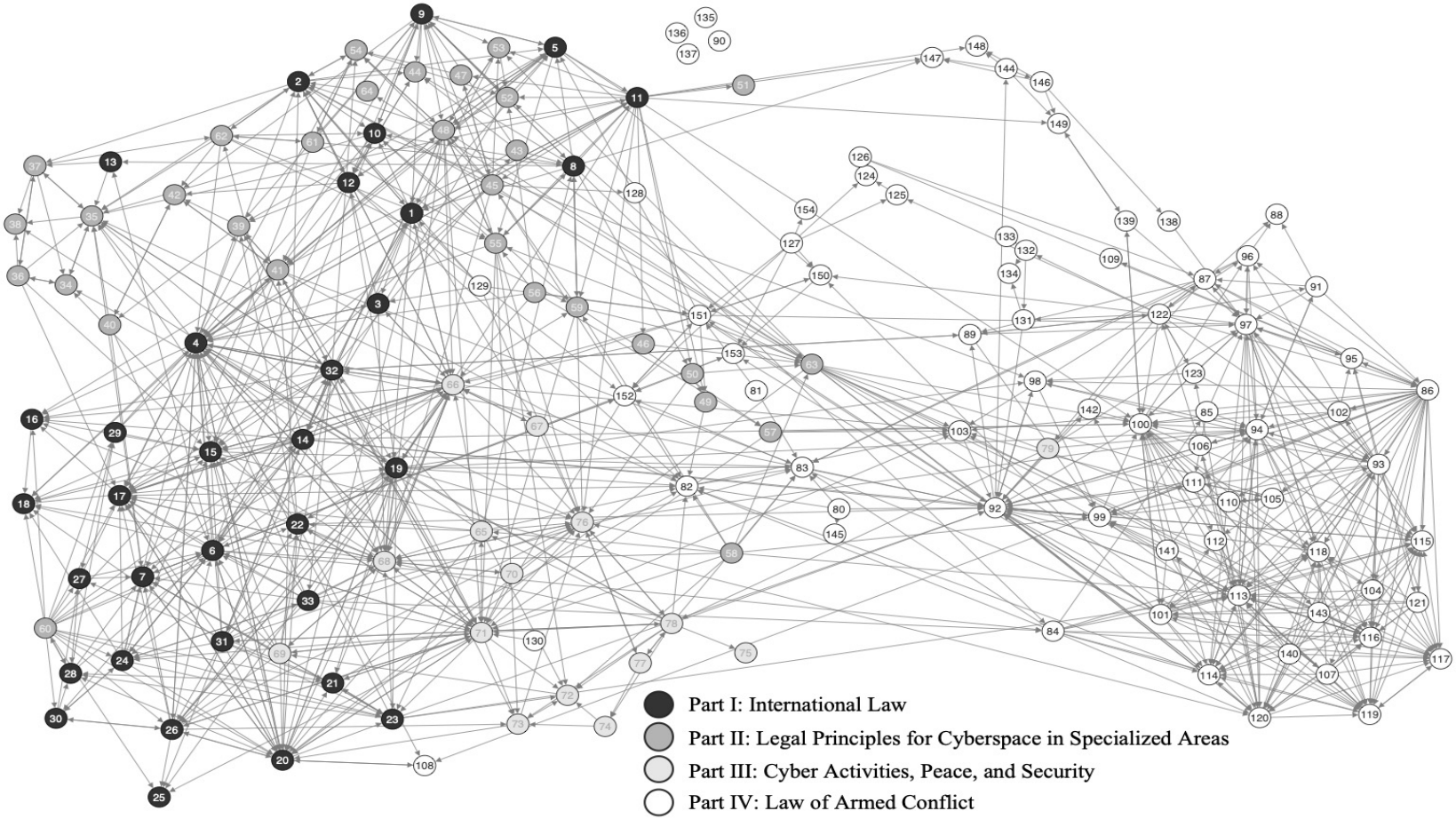


Figure 1 Network model of *Tallinn Manual 2.0*—reference case.

Source: Based on *reference* (or base case), i.e. binary, version of Design Structure Matrix of *Tallinn Manual 2.0* [5] in Appendix 1.
Note: Each node represents an individual *Rule* (with *Rule* number), identified by Part.
Arrow indicates that a *source Rule* (node) refers to *target Rule* (node) at the head of the arrow.
Rule, *Chapter,* and *Part* labels in this figure and all the figures that follow are direct quotes from [5].

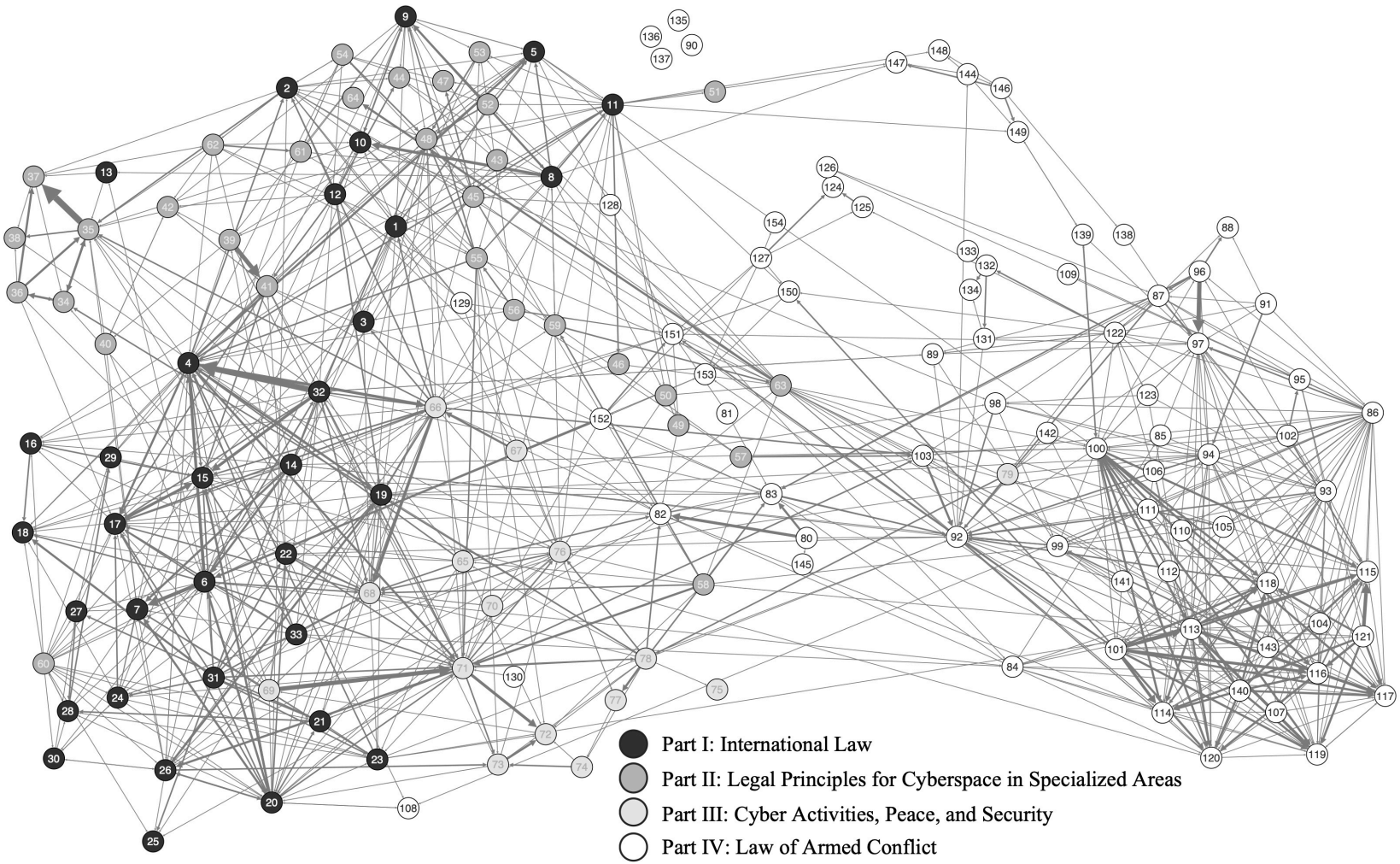


Figure 2 Network model of *Tallinn Manual 2.0*—with weighted edges signalling intensity of connectivity.

Source: Based on Design Structure Matrix of *Tallinn Manual 2.0* [5] in Appendix 1.
Note: Each node represents an individual *Rule* (with *Rule* number), identified by Part.
Arrow width indicates the frequency with which *source Rule (*node) refers to *target Rule* (node) at the head of the arrow.

4 Rule Centrality

The *degree of centrality* in a network model is determined by the node eigenvector that, itself, is shaped by the eigenvector of the *Rules* to which it is connected. In other words, the network model of *Rule* centrality is derived from the "neighborhood" to signal system-wide salience of individual Rules. The results, in Fig. 3, show a network model of the *Tallinn Manual 2.0* that clearly differs from the view in Fig. 2**.** With no change in the relative location of the *Parts,* or the overall system structure, the centrality measure reveals the *intensity* of connectivity and some notable features thereof.

First, the greatest concentration of high centrality nodes (five of the top ten) is located in *Part* I on *International Law*.

Second, although *Part* III—*Cyber Activities, Peace, and Security*—shows considerably fewer high-centrality *Rules* than *Part* I, some of its *Rules* attain especially high centrality scores. *Rule* 68 on "prohibition of threat of use of force" tops the list; *Rule* 66 on "intervention by states" ranks third; *Rule* 71 on "*self-defence against armed attack*" and *Rule* 76 on role of UN Security Council rank fifth and sixth respectively.

Third, only one high centrality *Rule* (of the top ten) is situated in *Part* IV on the "*law of armed conflict*," namely, *Rule* 92 in Chapter 17 on "*conduct of hostilities.*" This *Rule* defines cyberattack as a cyber action that causes injury or death. It is also the sole *Rule* of salience connecting "display affinity" of *Parts* I-III on the one hand, to *Part* IV on the other.

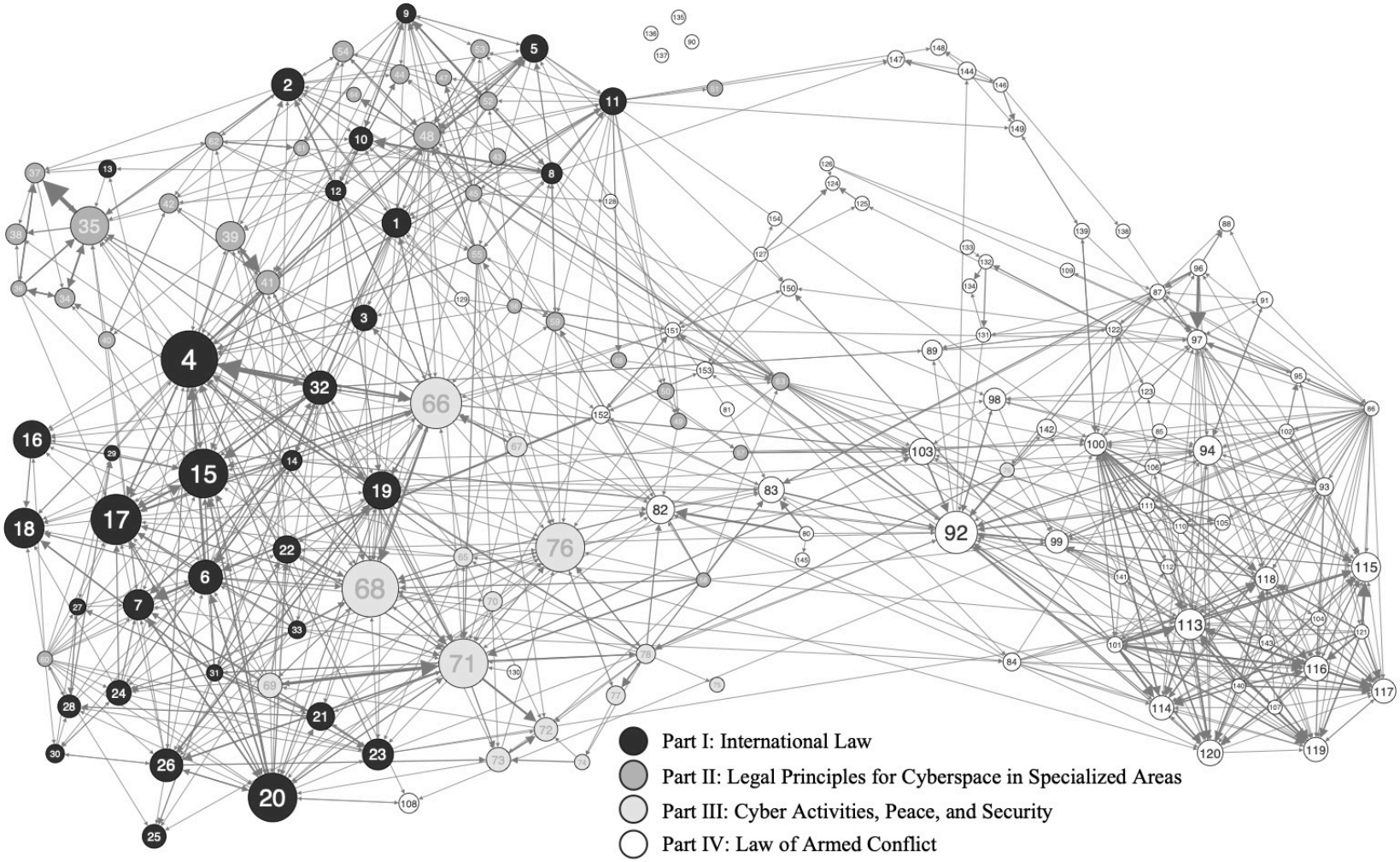


Figure 3. ***Rules-salience*** **(eigenvalue centrality) of the reference case for** ***Tallinn Manual 2.0.***

Source: Based on Design Structure Matrix (DSM) of *Tallinn Manual 2. 0* [5] in Appendix 1.
Note: Each node represents an individual *Rule* (with *Rule* number), identified by *Part*. Node size represents eigenvector centrality. Eigenvector centrality score is based on *reference* (or base case), i.e. binary, DSM of *Tallinn Manual 2. 0* [5] in Appendix 1.
Arrow width indicates the frequency with which *source Rule (*node) refers to *target Rule* (node) at the head of the arrow

5 Feedback

In its various forms, feedback reflects the complexity of order and disorder, "which gives it [the complex system] adaptive power" [8]. Especially compelling is the view of first order direct feedback (Fig. 4). Jointly, the arrowhead, source, destination, and weight provide a stark view of network structure systemwide. The Figure reveals only the direct feedback between nodes (*Rules*) and across *Parts*—all others can be identified at close observation of previous Figures. Several features of Fig. 4 are especially revealing:

One, is the apparent bifurcation between the high-density relationships among *Rules* (nodes) in *Part* IV on the *Law of Cyber Arm Conflict* and *Part* I on International Law, on the one hand, and the relatively sparse Rule direct feedback dependencies within *Parts* II and III, on the other – as signaled earlier.

Two, is the related feature of no-feedback connection between the *Rules* in *Part* IV and *Parts* II and III—more an affirmation of the power of international law, perhaps, than of its diffusion systemwide. It may also be due to the unchartered character of the cyber domain and its situational logic in war and peace.

Three, are the instances of direct feedback between *Parts* I and II (twelve loops); *Parts* I and III (sixteen loops); and *Parts* I and IV (only three loops)—all are further indication of the salience of international law on the overall system structure.

Four, is the very "thin" direct feedback connecting all *Parts* of *Tallinn Manual 2.0.* It consists of rather muted feedback connecting *Part* I and P*art* IV (via three feedback loops), and *Parts* II and *Part* III (only one direct feedback link).

Five, is the distinctive role of *Rule* 92—the only *Rule* of high salience in *Part* IV—and the one node of direct feedback between Rules in *Part* IV.

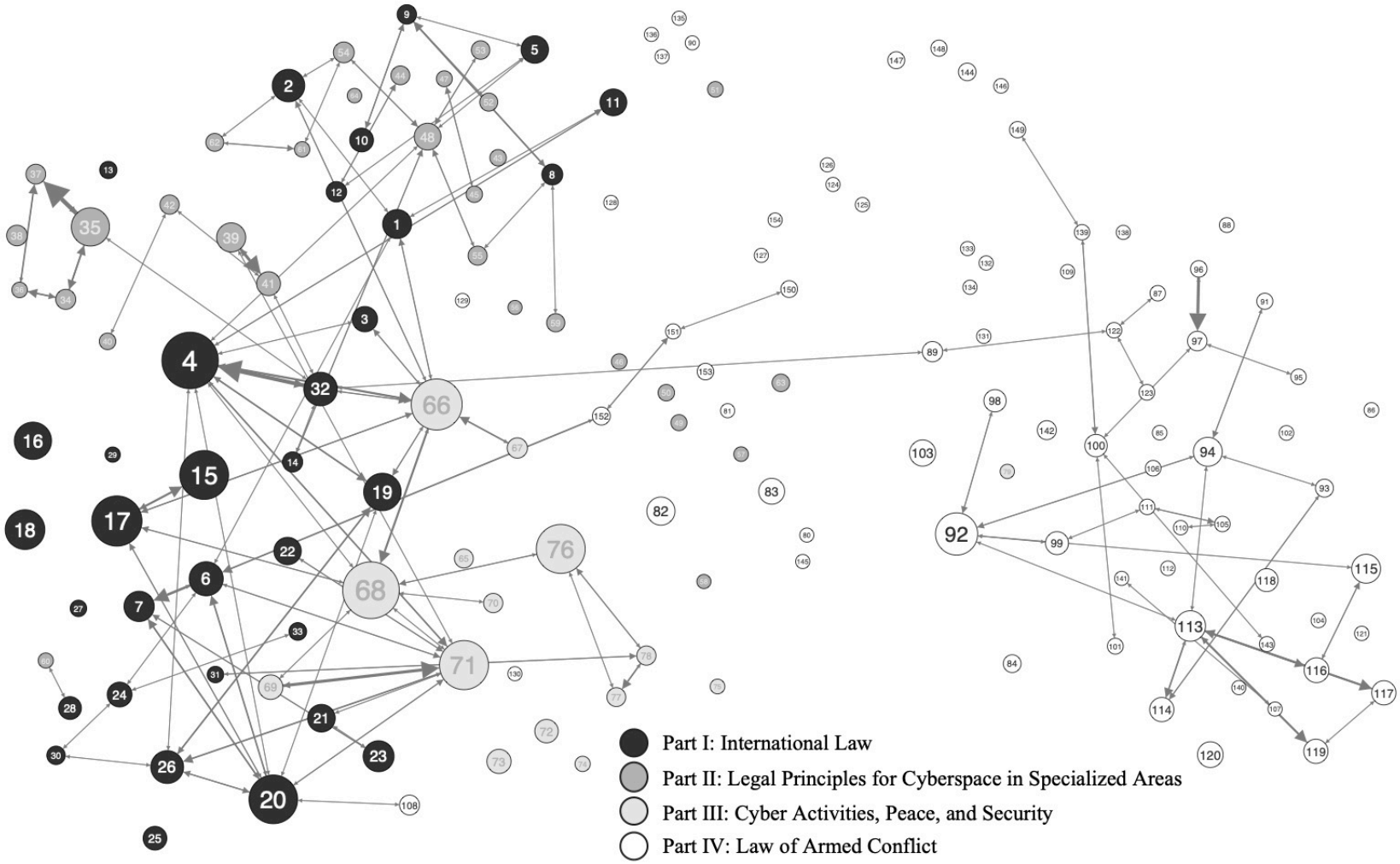


Figure. 4 First-order feedback in *Tallinn Manual 2.0*.

Source: Based on Fig. 3 on *Rules* centrality (eigenvector) of *Tallinn Manual 2.0* [5].
Note: Each node represents an individual *Rule* (with *Rule* number), identified by *Part*. Node size represents eigenvector centrality. Eigenvector centrality score is based on *reference* (or base case), i.e. binary, Design Structure Matrix (DSM) of *Tallinn Manual 2. 0* [5] in Appendix 1. Arrow width indicates the frequency with which *source Rule (*node) refers to *target Rule* (node) at the head of the arrow.

6 End Note

The logic of *International Law for Cyber Operations* assumes the absence of any significant difference between the structure of the international system and its *legal* principles on the one hand, and the *networked* system of cyberspace and its *operational* principles, on the other. Until very recently cyberspace has been a matter of *low* politics in international relations. Now that cyberspace has been catapulted to the highest levels of *high* politics, the international community is faced with a common dilemma: how to manage the cyber domain in a world where sovereignty is no longer the sole operating authority system.

Legal systems are structured to resist pressures for rapid change. All matters "cyber" transcend any efforts to limit the rates of change for any aspect thereof. *International Law for Cyber Operations* was not designed to "fit" the characteristic features of cyberspace, rather to develop legal bases for its management in relations between states – during war and during peace. While states are increasingly able to control Internet access and content transmission, the principle of sovereignty is yet to be fully aligned with the extent to which global communication networks and cross-border information flows are managed, largely by non-state entities buttressed by norms and procedures framed specifically to enable and facilitate the performance of a global cyber system.

References

[1] Kohl, Uta. (2007). *Jurisdiction and the Internet: A Study of Regulatory Competence over Online Activity*. Cambridge University Press.

[2] Lowe, Vaughan. (2007). *International Law*. Oxford University Press.

[3] Johnson, David R., and David G. Post. (1997). The Rise of Law on the Global Network. In *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, edited by Brian Kahin and Charles R. Nesson, 3–47. MIT Press.

[4] Ruhl, J. B., Katz, Daniel Martin, and Bommarito II, Michael J.. (2017). Harnessing Legal Complexity. *Science* 355(6332): 1377 LP-1378.

[5] Murray, Jamie, Webb, Thomas, and Wheatley, Steven. (2019). *Complexity Theory and Law: Mapping an Emergent Jurisprudence*. Routledge.

[6] Schmitt, Michael N.. ed. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

[7] Schmitt, Michael N.. ed. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge University Press.

[8] Benham-Hutchins, Marge, and Clancy, Thomas. R. (2010). Social Networks as Embedded Complex Adaptive Systems. *Journal of Nursing Administration* 40(9): 352–356.

[9] Paley, John, and Eva, Gail. (2011). Complexity Theory as an Approach to Explanation in Healthcare: A Critical Discussion. *Int J Nurs Stud 48*(2):269–279.

[10] Johnson, Neil F. (2007). *Simply Complexity: A Clear Guide to Complexity Theory*. Oneworld.

[11] Steward, Donald V. (1962). On an Approach to Techniques for the Analysis of the Structure of Large Systems of Equations. *SIAM Review* 4(4): 321–42.

[12] Browning, Tyson R. (2001). Applying the Design Structure Matrix to System Decomposition and Integration Problems: A Review and New Directions. *IEEE Transactions on Engineering Management* 48 (3): 292–306.

[13] Browning, Tyson R. (2016). Design Structure Matrix Extensions and Innovations: A Survey and New Opportunities. *IEEE Transactions on Engineering Management* 63 (1): 27–52.

[14] Girvan, Michelle, and Newman, M. E. J.. (2002). Community Structure in Social and Biological Networks. *PNAS* 99(12):7821–7826.

[15] Koniaris, Marios, Anagnostopoulos, Ioannis, and Vassiliou, Yannis. (2018). Network Analysis in the Legal Domain: A Complex Model for European Union Legal Sources. *Journal of Complex Networks* 6(2):243–268.

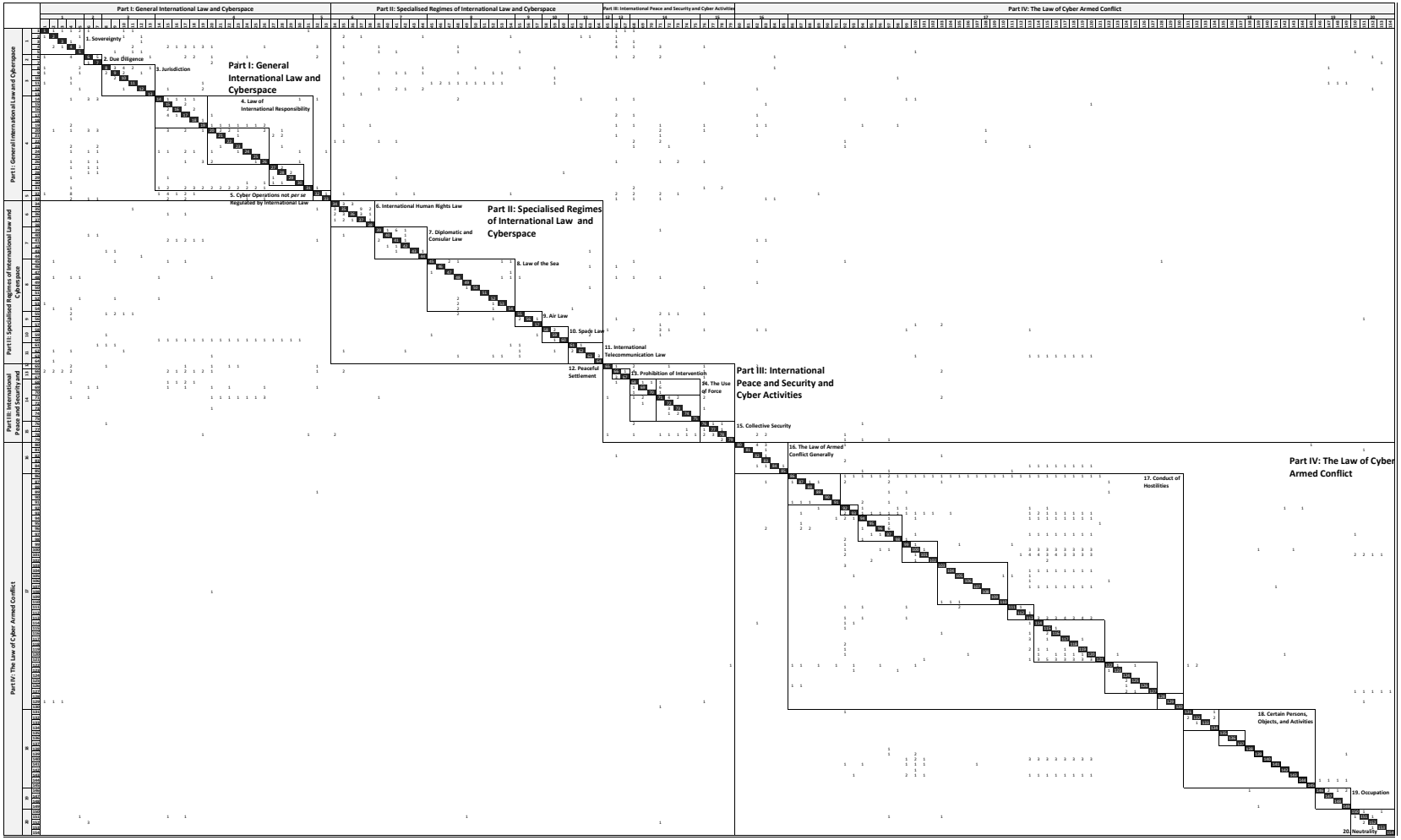
[16] Bastian, Mathieu, Heymann, Sebastien, and Jacomy, Mathieu. (2009). Gephi: An Open Source Software for Exploring and Manipulating Networks. *Proceedings of the Third International ICWSM Conference*, eds. Adar, Eytan, Hurst, Matthew, Finin, Tim, Glance, Natalie, Nicolov, Nicolas, and Tseng, Belle, 361–362. AAAI Press.

[17] Axelrod, Robert, and Michael D. Cohen. 2000. *Harnessing Complexity Organizational Implications of a Scientific Frontier*. New York: Free Press.

[18] Roscini, Marco. 2014. *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press.

[19] US Department of Defense. 2016. *Law of War Manual.* Washington DC: Office of General Counsel, US Department of Defense.

Appendix I. Design Structure Matrix (DSM) of Summed Frequency of Rule References By Cell of *Tallinn Manual 2.0*.



Source: Derived from the text in *Tallinn Manual 2.0 [5].*

Note: The cell at the *row-column* intersection records the frequency of a *row-Rule* reference to the intersecting *column-Rule* in its commentary, including footnotes. *Rule*, *Chapter*, and *Part* labels in this table, and in all the figures are direct quotes from [5]. Zoom in for a more detailed view.