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

July 9, 2022

Abstract

Policy documents are usually written in text form—word after word, sentence after sentence, page after page, section after section, chapter after chapter—which often masks some of their most critical features. The text form cannot easily show interconnections among elements, identify the relative salience of issues, or represent feedback dynamics, for example. These are "hidden" features that are difficult to situate. This paper presents a computational analysis of *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, a seminal work in International Law. *Tallinn Manual 2.0* is a seminal document for many reasons, including but not limited to, its (a) authoritative focus on cyber operations, (b) foundation in the fundamental legal principles of the international order and (c) direct relevance to theory, practice, and policy in international relations. The results identify the overwhelming dominance of specific *Rules*, the centrality of select Rules, the Rules with autonomous standing (that is, not connected to the rest of the corpus), and highlight different aspects of *Tallinn Manual 2.0*, notably situating authority, security of information -- the feedback structure that keeps the pieces together. This study serves as a "proof of concept" for the use of computational logics to enhance our understanding of policy documents.

Keywords

Tallinn Manual 2.0, visualization, design structure matrix, graph theory, network analysis, feedback, international law, cyber law.

Table of Contents

Complexity of International Law for Cyber Operations

1 Introduction

Despite major innovations in the construction and management of the Internet (the core of cyberspace)—or perhaps because of the remarkable expansion of its global reach—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].

For contextual purposes, these observations signal competing perspectives on international law. One view is that cyberspace requires a set of rules that are different from those that regulate interactions in the physical territorial domain—as argued, for example, by [3]. This view recognizes that rules are needed, but not those that govern the traditional international order defined by the state and its sovereignty; cyberspace is not bound by physical or geographical markers. The other view proceeds from the assumption that international law is applicable to all domains of state interaction in all known spaces—natural as well as built; it has a generic character. Therefore, it is also applicable to the cyber arena. In other words, when states interact, the rules of their interaction are governed by the international legal order.

Contentions aside, it is not too soon to appreciate the complexity associated with any legal order for the global system, especially when it encompasses cyberspace—a domain whose properties have no precedent and where multiple and diverse entities interact, often surrounded by uncertainty, ambiguity, and anonymity.

The physical layer of the Internet and its territoriality create an inevitable anchor to the state system. Today the ubiquity of cyberspace and its near total permeation throughout the traditional order—at all levels of analysis—makes it difficult to isolate cyber-specific elements. By the same token, it is especially difficult to retain a view of international relations that is devoid of the virtual—thus reinforcing the imperative of international law. Although complexity theory is well recognized in the scientific community [4], as is the development of complexity science, there are few directives for understanding its relevance to the broad area of international law for cyberspace. Especially noteworthy in this connection are the multifaceted arguments for "mapping an emergent jurisprudence" [5], supported by the illustration of ways that "scholars are using complexity theory to make sense of law" [5].

Our purpose in this paper is to explore and help “unravel” some of the complexity embedded in *Tallinn Manual 2.0* [6], a work recognized as seminal in both scale and scope. With complexity theory as our conceptual guide, we examine *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [6] through the lens of computational logic informed by complexity theory. *Tallinn Manual 2.0* extends and supersedes the legal principles put forth in *Tallinn Manual on the International Law Applicable to Cyber Warfare* [7] to include “the public international law governing operations during peacetime” [6].

Informed by complexity theory (or complexity science)—as a collection of theories and conceptual tools from diverse disciplines [8–9]—we view the *Tallinn Manual 2.0* as a legal corpus consisting of interconnections among different principles and directives. Despite the sequential text format and implied linearity, we consider this initiative a complex set of interconnected relationships. We shall return to these issues further along.

As with all legal and policy documents, *Tallinn Manual 2.0* is written in the text form—word after word, sentence after sentence, page after page, and chapter after chapter—which could well obscure critical features thereof. Text cannot reflect feedback relations, nor clearly delineate the relative salience of different features. This is not a critique of policy texts, or of law *per se;* it is an observation about the opportunity costs associated with tradition. The purpose of this paper is to bring such features to light and, in the process, contribute to greater understanding of the text and greater transparency for readers unfamiliar with complexity in discourse.

2 On *Tallinn Manual 2.0* and Computational Logic

Understanding the *Tallinn Manual 2.0* and its full implications amounts to a daunting challenge given its scale and scope. Although it does not carry the formal status of international law, it provides a formidable basis for exploring the properties of a legal order for cyber operations in times of war and peace. The text is clearly written, yet it is not easy for non-lawyers to track salient relationships, mutual dependencies, or reciprocal linkages among key elements, all of which are framed as *Rules*. Furthermore, as noted earlier, text-as-conduit imposes a sequential linear order on an otherwise complex system of interconnected logic. More important, however, is that text *alone* cannot do justice to what is clearly a major initiative in international law and increasingly relevant to state interactions in the cyber domain.

2.1 Context and Complexity

Tallinn Manual 2.0 is the product of a large-scale effort by a group of experts convened by the NATO Cooperative Cyber Defense Center of Excellence. It draws upon the corpus of international law established over a long period of time in an international context generally described as anarchic. The original *Tallinn Manual* was devoted to cyber operations during armed conflict. By contrast, *Tallinn Manual 2.0* is based on the assumption that states have to deal with cyber issues that lie below the use of force threshold on a daily basis [6]. *Tallinn Manual 2.0* extends the scope of the initial *Tallinn Manual* [7] regarding *jus ad bellum* and *jus in bello* in order to address cyber operations during times of peace. The logic of international law for cyber operations is issue-focused, but our method is generic and applicable to a wide range of issues.

Tallinn Manual 2.0 is not an official document or a study in the development of international law, nor does it represent the position of any country. It is "a reflection of the law as it existed at the point of the Manual's adoption" [6], created by international groups convened for its formulation. The intended audience consisted of state "legal advisors charged with providing international law advice to governmental decision makers, both civilian and military" [6]. For scholars of international relations, *Tallinn Manual 2.0* is especially important due to its (a) concerted focus on cyber operations, (b) relevance for theory, practice, and policy in international relations, and its (c) basis in sovereignty and security, traditional anchors in a complex world of chaos and conflict.

According to the General Editor, the "authority" of the *Manual* rests on the process of harnessing experiences recorded in major *international treaties* that span a wide range of issues, as well as a large body of *case law* [6]—all of which have evolved since the last decades of the nineteenth century. The extensive *Commentary* within the text, including footnotes, illustrates the nature of the discussion, contentions, and diverse points of view.

In a different context, Ruhl, Katz, and Bommarito [4] aptly note that legal systems are "locked in perpetual co-evolution with their regulatory targets." A somewhat loose analogy is found in international law, which is "locked in" co-evolution with the interests and activities of power relations and the changing configurations of states in the international system. Contentions aside, the fact remains that the *physical layer* of the Internet (the core of cyberspace) is embedded in the *territoriality* of the state and its sovereignty (the defining features of the international system).

2.2 Complexity Theory and Computational Logic

As noted in the Introduction, this paper is indebted to the properties of complexity science—in both conceptual and computational terms—for the analysis of the *Tallinn Manual 2.0*. Despite its salience in physics, mathematics, ecology, and social sciences—as well as its introduction to law [5]—there is no one definition of complexity science. But there is a general agreement that complexity "focuses on what new phenomena can emerge from a collection of relatively simple components" [10].

Here we highlight select elements of complexity science most relevant to the context at hand. Accordingly, a complex system consists of (i) a number of *interacting* elements (ii) linked to each other and constituting *networks* and (iii) influenced by "feedback," with (iv) conditions that could be "far from equilibrium" as well as (v) conditions supporting system stability, (v) and exhibits complicated order and disorder "which gives it [the complex system] adaptive power" [10]. These elements can best be viewed as propositions that frame the computational logic of this paper. Simply put, our logic consists of a chain of computational moves, each intended to generate specific outputs, and each designed to identify different properties of the text.

It is reasonable to ask: what is the added value of complexity—whether theory or science? Without referring prematurely to results, the answer at this point is as follows. At a minimum, the value of complexity coupled with computation—generic in frame and in form—is to (a) provide transparency of the system, of the "whole" and of its "parts," (b) generate new ways of analyzing system structure, (c) help extend conventional views surrounding the "as-is" system, and (d) explore contingencies such as, "what if…?"

What follows is a brief note on each segment of our computational logic. Each move is transformative, as follows: (a) from text to system structure, (b) from structure to system metrics, (c) from metrics to network models, and (d) from network models to motivations for further investigation. The process involves different methods based on different conceptual and operational assumptions. Jointly, they constitute a coherent computational logic.

2.2.1 From Text to System Structure

To begin, the text of the *Tallinn Manual 2.0* serves as the "raw data" for our investigation. While the text form may not do justice to what is clearly an effort of considerable complexity, the framework and organization of *Tallinn Manual 2.0* provide the basis—the essential information—for converting text into a structured representation of legal order. Put simply, the organization of the *Manual* is the anchor for a structured representation of the text form. The challenge is to remain as close to the "raw" text as possible, and to avoid introducing external or exogenous elements of any type.

In a document of nearly 600 pages, text-as-conduit imposes a form of sequential logic in an otherwise complex and interconnected set of directives. The *Manual* is organized into four *Parts*. *Part* I concerns *general international law* and begins with sovereignty to frame the basis of—and create foundations for—extending the application of international law to cyber operations. *Part* II focuses on and presents *specialized regimes of international law and cyberspace. Part* III addresses *international peace and security of cyber activities,* and *Part* IV focuses on the *law of armed conflict.* Each *Part* is divided into *Chapters* (some of which are further divided into *Sections*). Each *Chapter* consists of specific *Rules*, presented one after the other. It is at the level of *Rules* that the substantive materials are framed as explicit directives—points of law. Each *Rule* is followed by a detailed general *Commentar*y, designed to enrich our understanding by providing materials for contextual purposes on the one hand, and to help reflect on the whole content of the legal system (including differing views among legal scholars), on the other.

The first step for computational logic in this study is to construct the system structure or framework for the *Manual* in the form of a Design Structure Matrix (DSM), also known as a

Dependency Structure Matrix. First proposed by [11], a DSM is an information exchange method for representing interactions among the elements of a system. Browning [12–13] provides a survey of DSM applications, and highlights their use in the areas of engineering design, engineering management, management/organization science, and systems engineering.

For computational purposes, the system structure follows the organization of the *Manual* itself. Accordingly, it is a matrix of rows and columns consisting of 154 *Rules* organized into twenty *Chapter*s and four *Parts.* The matrix is important – even as an "empty" framework – as it becomes the venue through which the elements of the *Manual* are examined.

2.2.2 From System Structure to Metrics

For conceptual and computational purposes, the process of generating metrics focuses first and foremost on the most specific elements of *Tallinn Manual 2.0*, namely the *Rules* explicitly designated as such. As noted above, the structured matrix is designed to provide the venue through which the incidence or occurrence of *Rules*, and their connection to other *Rules*—as stated in the text—are recorded. This approach is "low risk" approach since it anchored in the organization of the *Manual.*

The *basic* metric is binary, in terms of "yes/no," and records if a *Rule* (in a row) refers to another *Rule* (in a column) in its commentary, including footnotes. This accounting creates a first order record of incidence, referred hereinafter as *Rules-incidence*. When viewed in matrix form this "mapping" of *Tallinn Manual 2.0* also shows the "white areas," namely those *Rules* in the matrix devoid of reference to, or from, any other *Rule*. When completed, the "mapping" process yields the basic *Rule-based* Design Structure Matrix (154 by 154) of the entire *Tallinn Manual 2.0,* where individual cell is "populated" by empirically derived observations. We consider the basic DSM as the *reference* case, the most elemental representation of structure and content of *Tallinn Manual 2.0*. The network view generated by the matrix of this basic metric—as we show later on in this paper—is by definition the *reference* view.

If we record the *frequency metric* with which a *Rule* (in a row) refers to another *Rule* (in a column) in its commentary, including the footnotes, the record in each cell shows *occurrences* of relationships at the cell level. The matrix generated by *Rule frequency* is a specific departure from the *basic metric* representation, or reference case, in matrix form. The DSM structure (154 by 154) for *Tallinn Manual 2.0* remains the same as the reference case. By definition, we expect the numeric in the DSM cells and the characteristic features of the network forms to signal fundamentally different properties compared to the reference case. For example, when we view *Tallinn Manual 2.0* at the *Chapter* level—a *Chapter* often includes several *Rules*—the DSM form and the network views follow, according to stated specifications.

2.2.3 From Metrics to Network Model

In the context of complexity, as in many other contexts, networks are increasingly used to address an ever-growing variety of relationships and attendant challenges. Networks have become commonplace in both qualitative and quantitative analyses of systems. Network theory, also called graph theory in mathematics, focuses on structures of symmetric or asymmetric relations among entities (or objects) in a system. In its most elemental definition, a network consists of items that are termed *nodes* or *vertices*, while the connections among them are termed *edges* or *interfaces.* The terms may vary by field, but the basics remain the same [14]. Recent studies of the European Union legal sources [15] introduce a "network-based approach to model law …" to examine the connections among and evolution of legal documents. Our purpose, however, is different: we focus on connections (as articulated) among *Rules*, and the linkages and lineages referenced therein. While we consider the features of the interfaces, their features are often more difficult to visualize than those of nodes.

Drawing on network theory and supporting tools, notably the *ForceAtlas* algorithm of Gephi 0.9.2 software [16], we generate a basic network model of the Design Structure Matrix for the reference case of the entire *Tallinn Manual 2.0*. The result is a spatially structured network, where nodes repulse each other like charged particles while edges attract their nodes like springs. Jointly they converge on a balanced state. Computationally, each node is based on the location of *other* nodes and depends only on the connections between nodes. A network provides a visual image of how a set of elements are connected to, or interact with, each other. The connections or interactions are useful in their own right, as they reveal the properties of a system. However, not all elements (nodes or vertices) are of the same importance in a complex system, nor are they of the same relevance to the structure of a complex system.

Central to all complex systems is the feature of "feedback"—as noted earlier. Again, feedback has become part of everyday discourse and is generally understood to be fundamental to systems of all types. Positive feedback reinforces and amplifies the system. Negative feedback prevents the system from losing its equilibrium or stability. Both serve as control mechanisms in a complex system. Less often considered is feedforward, whereby corrective action is taken in anticipation of disturbances before they occur. In addition, there is a role for "memory," that is, information embedded in the system (or in its nodes or, as relevant, its agents). We shall return to this feature of feedback later on in this paper.

2.3 Power of Perspective

It goes without saying that "what you see depends on how you look at it." With that in mind, we review briefly the computational logic, that is, *how* we look at *Tallinn Manual 2.0*, before we turn to the results, which focus on *what* we see. Recall that the text of *Tallinn Manual 2.0* provides all the information required to construct the structure of the entire *system* in matrix form. This matrix is the venue to record in binary form (i.e. yes/no) if a reference is made by a *Rule* (in a row) —in its commentary and footnotes—to another *Rule* (in a column). The record is entered in each cell, for each of the 154 *Rules*. When completed, the matrix contains only the most essential elements of the system, uninformed by added insight or information. This matrix serves as the reference case of the DSM mode. It carries all the input data to generate the baseline, or reference network model, for *Tallinn Manual 2.0*.

If we explore *Tallinn Manual 2.0* further, with more detailed analyses generating more differentiated results, *then* we obtain different perspectives. To avoid the “shifting sands” scenario, it is often useful to compare various perspective to the reference case. Such comparison, however, is not intended to imply that the reference case is “better” or more accurate than other cases. *Power of perspective* is the imperative that requires the analyst to share (and the reader to understand) the dependence of results on methods and assumptions.

3 Results of Computational Logic

What have we learned about *Tallinn Manual 2.0* in the course of our investigations? Is there value added? If so, what is it? If not, why not? What follows is a discussion of the results, revisiting the computational sequence introduced in the previous section.

In this section, we present first the results of the *Reference* case based on binary metrics (i.e. “yes/no”) of the reference DSM. Once completed, we depart from the binary metric, and replace the cells with the *numeric* measure of the incidences (i.e. number of times) a reference is made by a *Rule* (in a row)—in its commentary and footnotes—to another *Rule* (in a column). By definition, the latter is no longer the reference case, it is an entirely different case.

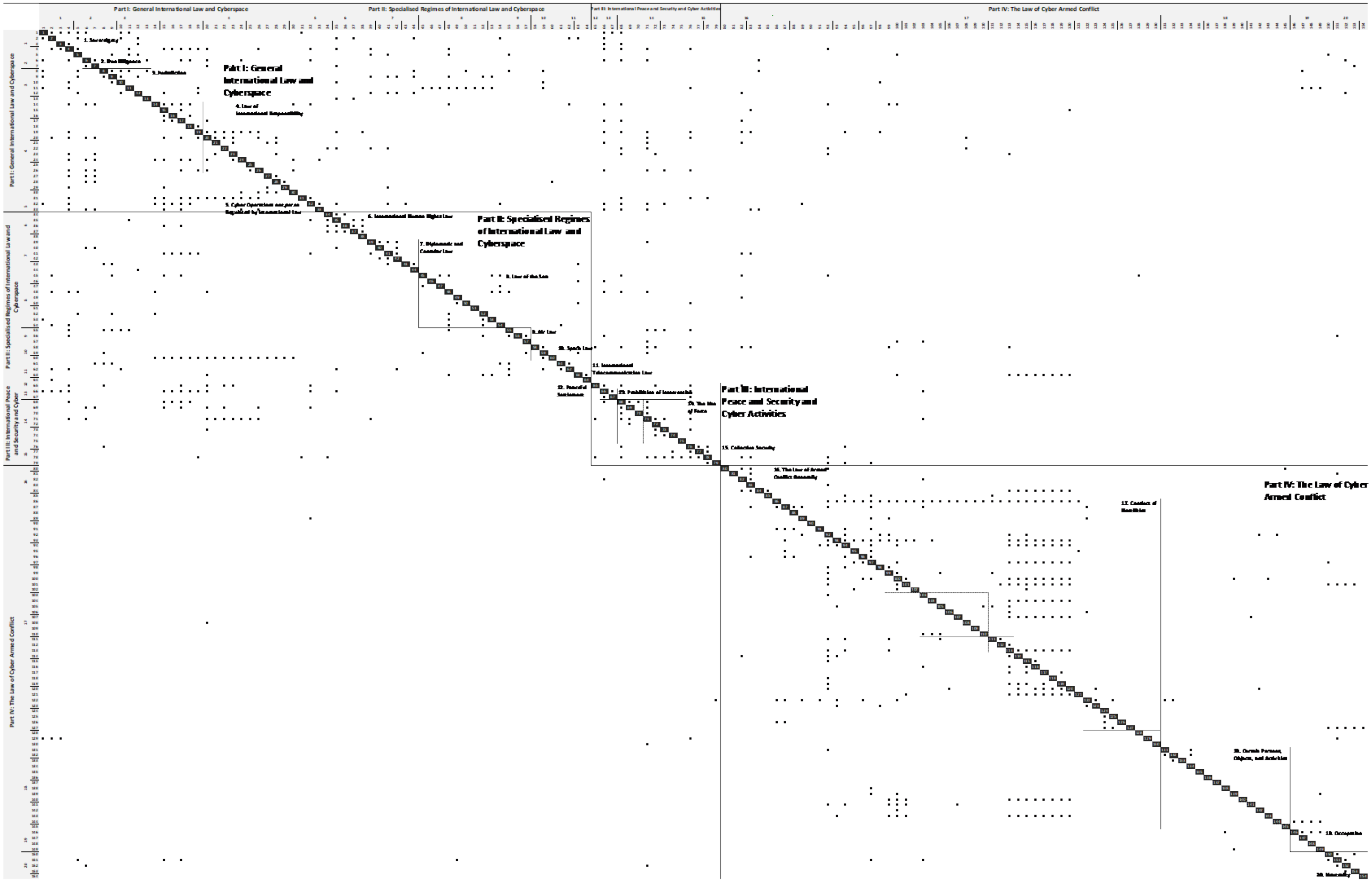
3.1 System Structure—Reference Case

We noted earlier that the organization of the *Tallinn Manual 2.0* provides the basis for the system *structure*, rendered in the rows and columns of a Design Structure Matrix. As noted is that the *Rule* is the most granular and fundamental feature of the *Tallinn Manual 2.0.*

3.1.1 Design Structure Matrix—Reference Case

The reference case for the DSM is presented in **Table 1**, a *matrix of incidence* (with “yes” records noted and “no” blank). The matrix shows the connections among all 154 *Rules* of the system—those readily discernable in the full text and in the table of contents. It also provides a comprehensive first-order view of the system as a whole. The size of a 154 by 154 matrix exceeds the bounds of conventional textual representation.

Table 1: *Incidence-view* (binary) by cell in DSM for *Rules* in *Tallinn Manual 2.0*


Part I: General International Law and Cyberspace
Part II: Specialised Regimes of International Law and Cyberspace
Part III: International Peace and Security and Cyber Activities
Part IV: The Law of Cyber Armed Conflict
1. Sovereignty
2. Due Diligence
3. Jurisdiction
Part I: General International Law and Cyberspace
4. Law of International Responsibility
5. Cyber Operations not per se Regulated by International Law
6. International Human Rights Law
Part II: Specialised Regimes of International Law and Cyberspace
7. Diplomatic and Consular Law
8. Law of the Sea
9. Air Law
10. Space Law
11. International Telecommunication Law
12. Peaceful Settlement
13. Prohibition of Intervention
14. The Use of Force
Part III: International Peace and Security and Cyber Activities
15. Collective Security
16. The Law of Armed Conflict Generally
17. Conduct of Hostilities
Part IV: The Law of Cyber Armed Conflict
18. Certain Persons, Objects, and Activities
19. Occupation
20. Neutrality

Source: Derived from the text in [6]. Rule, Chapter and Part titles are direct quotes from [6].

Note: Identifier ● indicates that a *row-Rule* refers to the *column-Rule* in its commentary, including footnotes. Zoom in for a more detailed view.

Despite its simplicity, the reference case status shows some less obvious or even entirely obscured features of the system as a whole. These include:

1. *Asymmetry of content*, that reflects the substantive structure of the entire legal system;
2. *Rule density*, that indicates the *Part* with the greatest number of *Rules* and least number of connections to other *Parts*, a feature most evident in *Part* IV;
3. *Rule influence*, that indicates *Rules* that are referred to by other *Rules*, and
4. *Stand-alone status*, which signals autonomous *Rules,* that is, those that remain unconnected to the whole or to its parts.

These features may be more evident in the network model than in the design structure matrix.

3.1.2 Network Model—Reference System

Derived from the data in **Table 1**, **Figure 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 architecture. Further, all *connections* (i.e. interfaces or edges) between *Rules* are also displayed as "equal."

At the same time, however, this Figure displays a system architecture distinguished by a "display of affinity" that is, perhaps, more readily observable in the network view than in the DSM matrix. 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, further along.

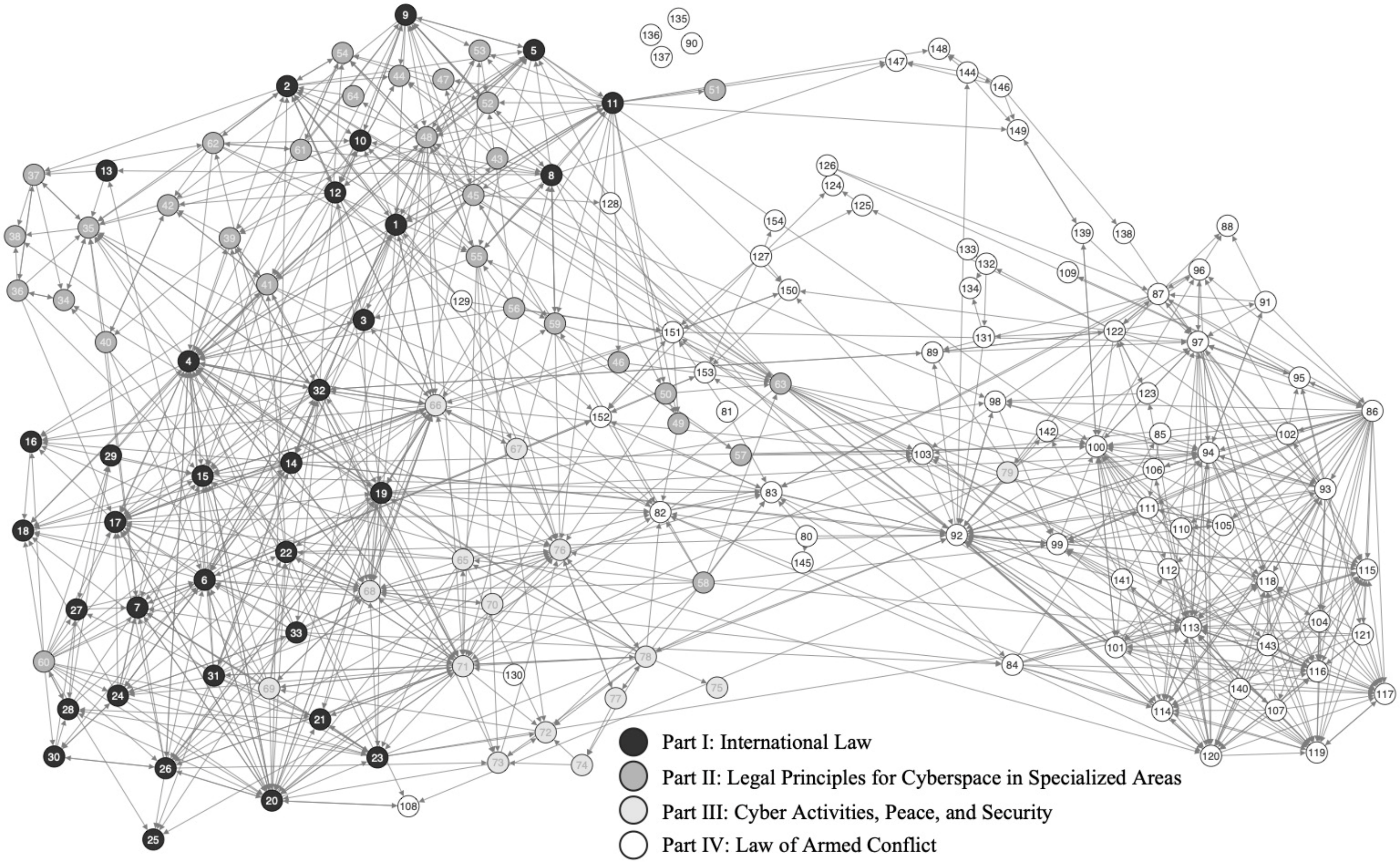

● Part I: International Law
● Part II: Legal Principles for Cyberspace in Specialized Areas
○ Part III: Cyber Activities, Peace, and Security
○ Part IV: Law of Armed Conflict

Figure 1. Network Model of *Tallinn Manual 2.0* – Reference Case.

Source: Based on *incidence* (binary) Design Structure Matrix in **Table 1** for text of *Tallinn Manual 2.0* [6].

Note: Each node represents an individual *Rule* (with rule number), identified by *Part*.

3.1.3 Rule Centrality View of the Reference System

If we differentiate among nodes by *degree of centrality*, that is, in terms of salience system-wide, we obtain a network view different from the reference model. *Rule* centrality is determined by the eigenvector centrality of one node based on the eigenvector centrality of the *Rules* to which it is connected. Put simply, centrality is a measure of the neighborhood. The results, in **Figure 2** show a network model of the *Tallinn Manual 2.0* clearly different from the view displayed earlier in **Figure 1**. With no change in the relative location of the *Parts*, the centrality measure reveals additional features of the reference case.

First, the greatest number of high centrality nodes are located in *Part* I on *International Law.* Of these, the most salient is *Rule* 4 in *Chapter* 1 on *State Sovereignty,* prohibiting the violation of state sovereignty via cyber venues. The other three nodes of high salience—*Rule* 15 (Collective Security), *Rule* 17 (Cyber Actions), and *Rule* 20 (Neutrality of Cyber Assets)—are all located in *Chapter* 4 on *International Responsibility*.

Second, although *Part* III—*Cyber Activities, Peace, and Security*—harbors considerably fewer high-salience *Rules* than *Part* I, four of its *Rules* show greater centrality than three of the four high-salience *Rules* in *Part* I. These *Part* III *Rules* are *Rule* 66 (prohibiting intervention in other states), *Rule* 68 (prohibiting the use of force against another states), *Rule* 71 (supporting self-defense), and *Rule* 76 (reiterating the United Nations' priority of using non-force measures).

Third, only one high-salience *Rule* is situated in *Part* IV on the *Law of Armed Conflict,* namely, *Rule* 92 defining a cyberattack as a cyber action that causes injury or death. At the same time, however, *Rule* 92 is distinctive not only for its salience but, perhaps more important, for its function as the sole *Rule* providing a strong connection between *Parts 1-III* and *Part* IV.

Fourth, by definition, the "stand-alone," or isolated, *Rules* of **Figure 1** retain that position in **Figure 2**. We shall return to these *Rules* later in this paper. Then, too, a casual glance at **Figure 2** will also draw attention to what seem to be a dual focus (or relative density) of relationships among *Rules*: one on the left of the figure, and one on the right. In this network model, the two segments are connected by a relatively large number of low centrality *Rules*, many of which appear to converge around *Rule* 92, which defines cyberattack as a cyber action that causes injury or death, located in *Chapter* 17 on "conduct of hostilities" of *Part* IV. Interestingly, the relative centrality of *Rule* 92 appears pivotal, *as if* connected much of *Part* I to *Part* IV. Further along we shall demonstrate the error of inferring this pivotal role.

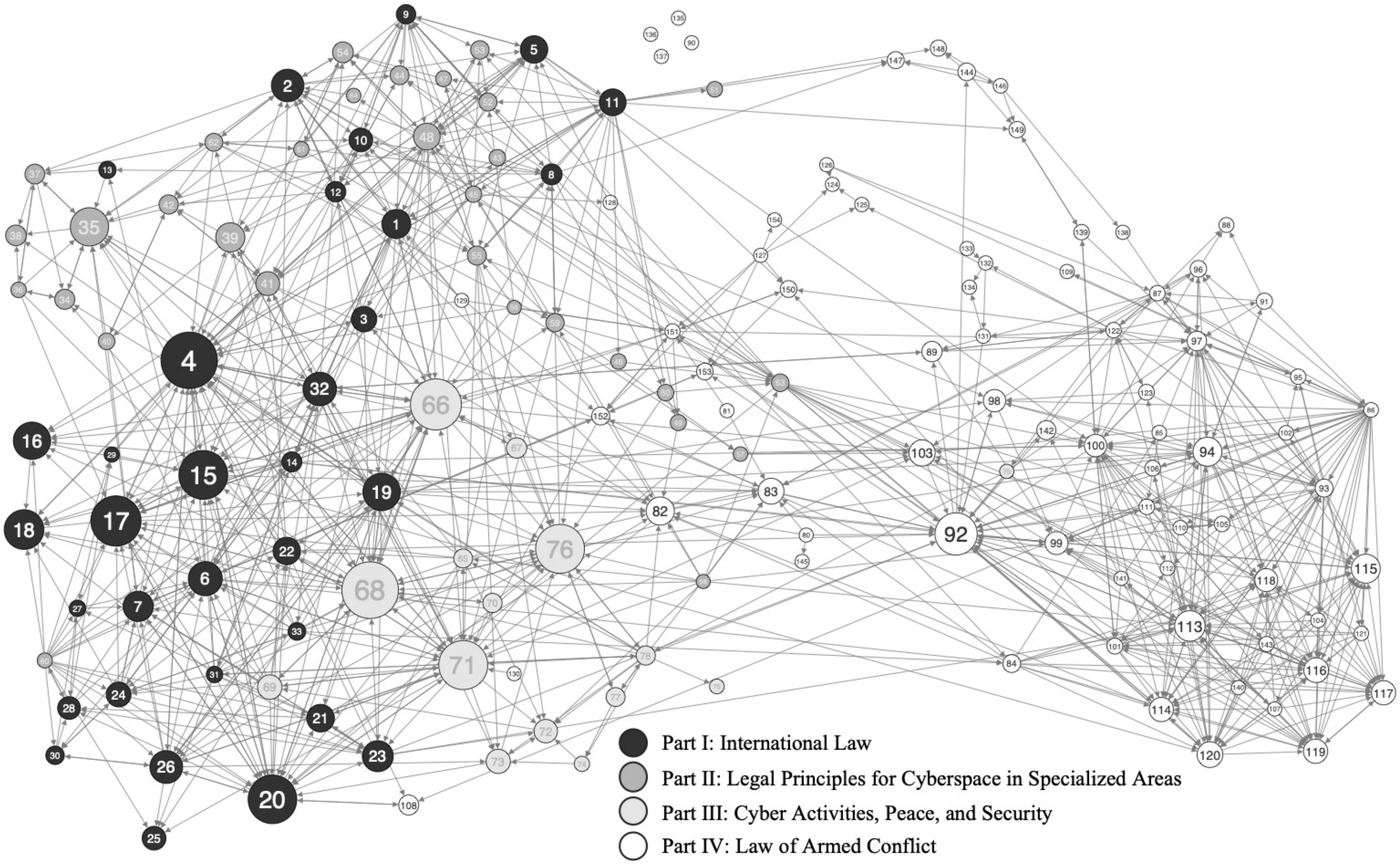

9
5
2
11
10
8
13
1
12
35
39
3
4
32
66
16
15
14
19
18
17
76
6
22
68
7
27
33
31
71
24
28
21
23
30
26
20
25
108
82
83
92
103
100
94
98
99
115
118
113
116
117
114
120
119
Part I: International Law
Part II: Legal Principles for Cyberspace in Specialized Areas
Part III: Cyber Activities, Peace, and Security
Part IV: Law of Armed Conflict

Figure 2. ***Rules-salience*** **(eigenvalue centrality) of the Reference System for** ***Tallinn Manual 2.0.***

Source: Based on *incidence (binary)* Design Structure Matrix in **Table 1** for text of *Tallinn Manual 2.0* [6]. Eigenvector centrality scores generated with Gephi 0.9.2 software [16].

Note: Each node represents an individual *Rule* (with rule number), identified by *Part.* Node size represents eigenvalue centrality score.

The *Rules* with the greatest centrality for the reference case—shown in the system-wide view of **Figure 2**— are listed in **Table 2**. From a computational perspective, *if Tallinn Manual 2.0* can be distilled to its most basic core, *then* this table provides an excellent perspective thereof. We do not expect legal scholars to support this characterization. Our purpose here, however, is to understand the content-architecture of the system as a whole, not to yield legal interpretation.

Table 2. Highest Centrality Rules of Tallinn Manual 2.0: Eigen Centrality

Rule*		Chapter*		Eigen centrality
68	Prohibition of threat or use of force	**14**	The use of force	1.000
4	Violation of sovereignty	**1**	Sovereignty	0.996
66	Intervention by States	**13**	Prohibition of intervention	0.868
17	Attribution of cyber operations by non-State actors	**4**	Law of international responsibility	0.849
71	Self-defence against armed attack	**14**	The use of force	0.822
76	United Nations Security Council	**15**	Collective security	0.819
15	Attribution of cyber operations by State organs	**4**	Law of international responsibility	0.817
20	Countermeasures (general principle)	**4**	Law of international responsibility	0.813
92	Definition of cyber attack	**17**	Conduct of hostilities	0.660
18	Responsibility in connection with cyber operations by other States	**4**	Law of international responsibility	0.602

Source: Based on computational analysis of text in *Tallinn Manual 2.0* [6].

Note: * Rule and Chapter titles are direct quotes from [6]. Eigen centrality values are generated with Gephi 0.9.2 software [16].

3.2 System Structure—*Rule* Frequency

We now introduce a major departure from the reference case of the binary DSM and network model by computing *Rule* frequency defined as the number of references made by a row *Rule* to a column *Rule.* The underlying question is this: Does this departure from the baseline case generate results other than those discussed above? If so, what are these differences? If not, why would it matter, one way or the other?

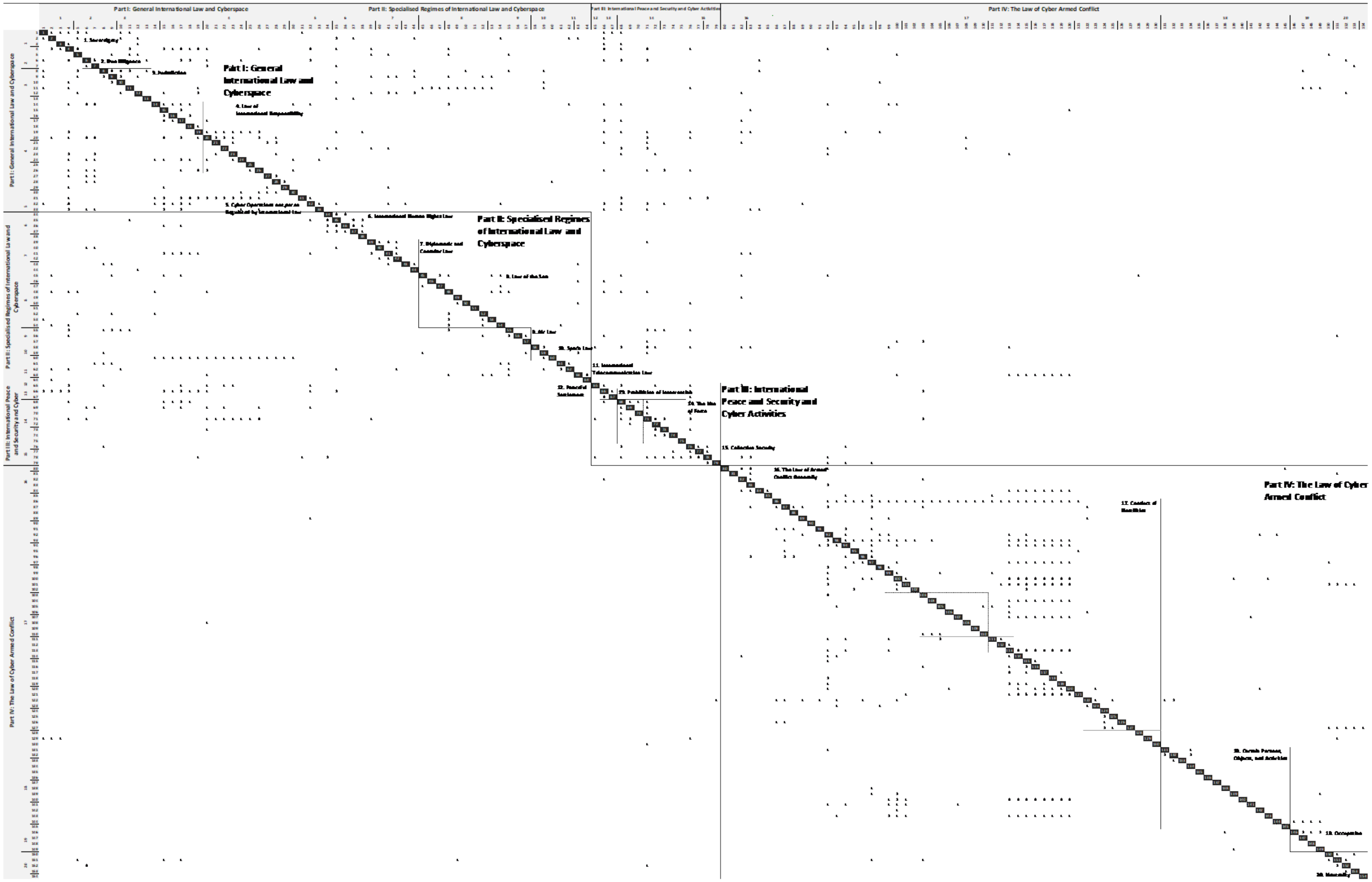
3.2.1 *Rule* Frequency: DSM and Network Model

Consistent with the computational logic, we begin by constructing the DSM based on frequency rather than binary records. The results are shown in **Table 3.** Even the most cursory view reveals the variability in the distribution of frequencies across individual cells. It does not alter the distribution of the "white areas" nor the diagonal.

Recall that **Figure 2** above indicates the relative salience of individual *Rules* and our discussion focused on the nodes. Recall also that the centrality value is based on "neighborhood" properties, not on features of an individual *Rule.* Thus, the "neighborhood" in the *frequency* network model is akin to that of the reference case. We now turn to *directionality* in order to explore the nature and types of relationships among *Rule*s. **Figure 3** draws attention to three network features that we have not yet addressed: (a) direction of arrows, (b) source and destination, and (c) width of connection, that is, edge or interface.

First, we focus on *Rules* that *influence* other *Rules* system-wide. Then, we turn to *Rules* that are *influenced* by other *Rules.* The valences, often obscurely rendered, do not easily signal the defining feature(s) of influence. Certainly, we would not expect all nodes to be directly connected to each other; nor do we expect all indirect connections to be routed in the same way. Jointly, however, these two perspectives may provide added insight into the underlying logic of *Tallinn Manual 2.0.*

Table 3. Summed *frequency* by cell in DSM for *Rules* in *Tallinn Manual 2.0*


Part I: General International Law and Cyberspace
Part II: Specialised Regimes of International Law and Cyberspace
Part III: International Peace and Security and Cyber Activities
Part IV: The Law of Cyber Armed Conflict
1. Sovereignty
2. Due Diligence
3. Jurisdiction
Part I: General International Law and Cyberspace
4. Law of International Responsibility
5. Cyber Operations not per se Regulated by International Law
6. International Human Rights Law
Part II: Specialised Regimes of International Law and Cyberspace
7. Diplomatic and Consular Law
8. Law of the Sea
9. Air Law
10. Space Law
11. International Telecommunication Law
12. Peaceful Settlement
13. Prohibition of Intervention
14. The Use of Force
Part III: International Peace and Security and Cyber Activities
15. Collective Security
16. The Law of Armed Conflict Generally
17. Conduct of Hostilities
Part IV: The Law of Cyber Armed Conflict
18. Certain Persons, Objects, and Activities
19. Occupation
20. Neutrality

Source: Derived from the text in [6]. Rule, Chapter and Part titles are direct quotes from [6].

Note: Metric in a cell at the *row-column* intersection indicates the frequency with which a *row-Rule* refers to the *column-Rule* in its commentary, including footnotes. Zoom in for a more detailed view.

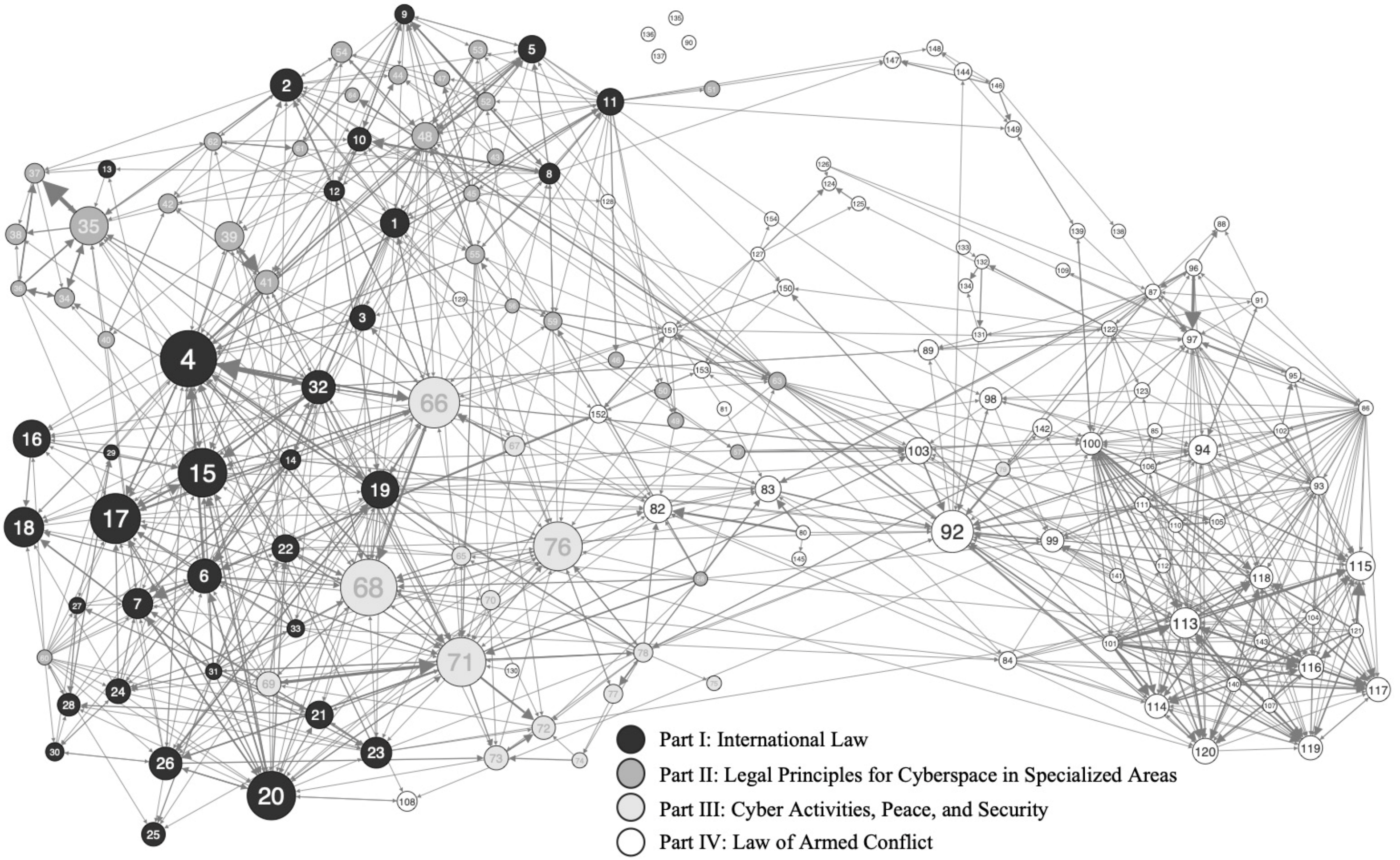


Figure 3. Edge Salience View of the *Tallinn Manual 2.0*.

Source: Based on *summed frequency by cell* Design Structure Matrix in **Table 3** for text of *Tallinn Manual 2.0.* Eigenvector centrality scores are calculated with Gephi 0.9.2 software [16].

Note: Node size represents eigenvalue centrality score. Arrow width indicates the frequency with which the source *Rule* (node) refers to the target *Rule* (node) at the head of the arrow.

3.2.2 *Rules* of Influence: Out Degree

"Out degree" refers to the *direction of influence* from a *Rule* to another *Rule* in the network, signaled by the arrowhead, or terminal point, and the weight or width of the interface or edge. **Figure 4** shows out degree networks and identifies *Rules* by their respective *Part*. Despite its complexity, this Figure retains some familiar features in a structure that appears to be far from volatile. The reader might find it useful to situate both arrowhead and terminal point and then focus on the width of the connections (edges).

Following the arrowheads in the **Figure 4**,**Table Table 4** shows the top ten *Rules* with the highest reference frequency to other *Rules* and the number of *different Rule*s referred. These are the *Rules* that influence, or shape, the influence-architecture of the system as a whole. Interestingly, Rule 101 on civilian and military uses in *Part* IV tops the list. However, it comes as no surprise that *Rule* IV on sovereignty in *Part* I also ranks high.

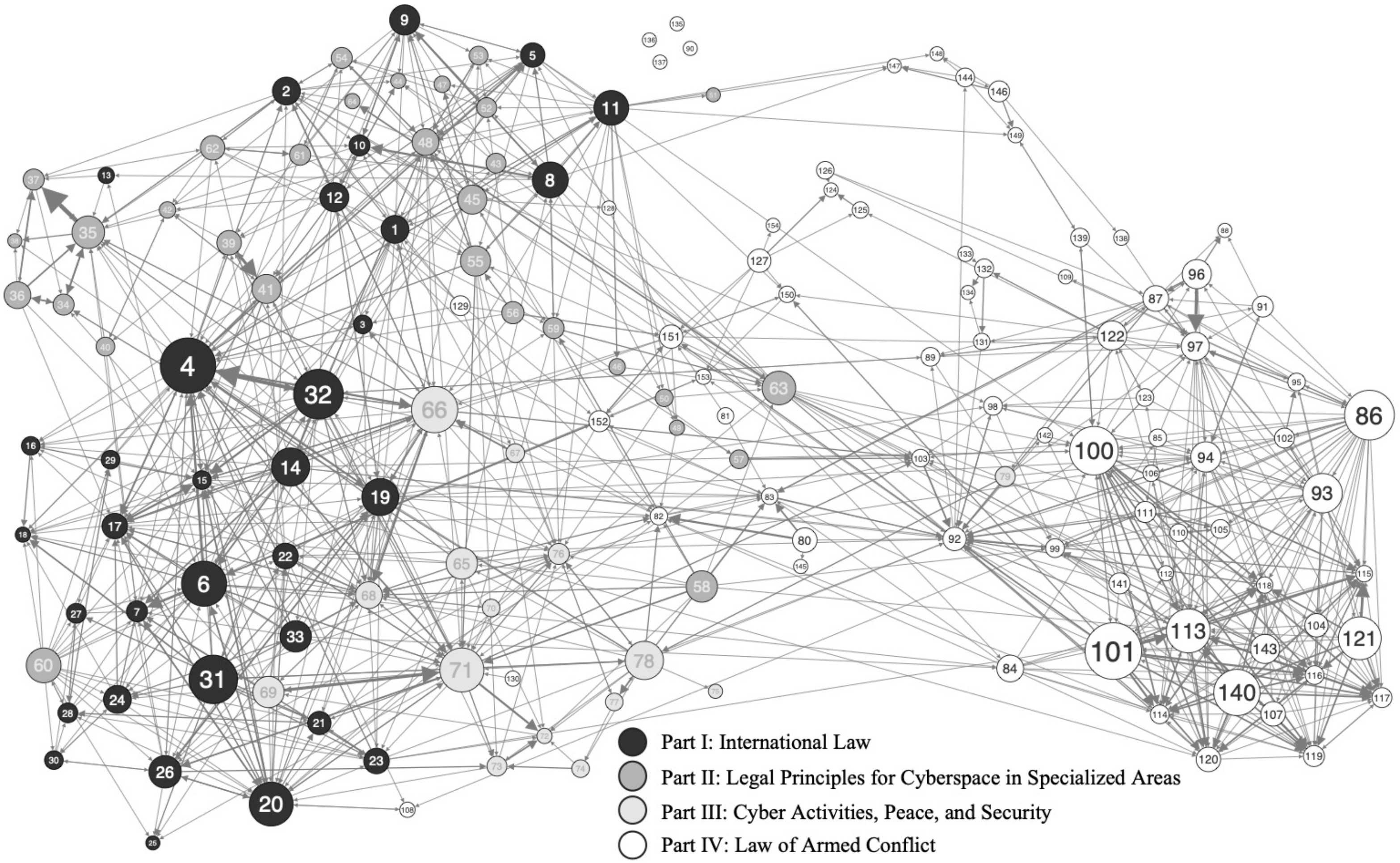


Figure 4. Out Degree Centrality View of *Tallinn Manual 2.0.*

Source: Based on *summed frequency by cell* Design Structure Matrix in **Table 3** for text of *Tallinn Manual 2.0* [6].

Note: Node size is based on frequency of references made by a *row-Rule* to a *column-Rule(s)* in its text commentary. Arrow width indicates the frequency with which the source *Rule* (node) refers to the target *Rule* (node) at the head of the arrow.

Table 4. Out Degree: *Rules* with Most References to Other *Rules* (ranked by frequency)

Rule*		***Chapter****		**Reference Frequency**	**Reference Count**
101	Objects used for civilian and military purposes	**17**	Conduct of hostilities	37	15
4	Violation of sovereignty	**1**	Sovereignty	36	20
32	Peacetime cyber espionage	**5**	Cyber operations not *per se* regulated by international law	31	17
86	Participation generally	**17**	Conduct of hostilities	31	30
31	General principle	**4**	Law of international responsibility	30	17
100	Civilian objects and military objectives	**17**	Conduct of hostilities	30	14
66	Intervention by States	**13**	Prohibition of intervention	28	16
140	Duty of care during attacks on dams, dykes, and nuclear electrical generating stations	**18**	Certain persons, objects, and activities	28	11
6	Due diligence (general principle)	**2**	Due diligence	27	15
20	Countermeasures (general principle)	**4**	Law of international responsibility	26	15
71	Self-defence against armed attack	**14**	The use of force	26	17
113	Proportionality	**17**	Conduct of hostilities	26	10

Source: Based on computational analysis of *Tallinn Manual 2.0* text [6]. * Rule and Chapter titles are direct quotes from [6].

Note: Reference frequency is the sum of numeric values in off-diagonal cells across a row of the DSM in **Table 3.** Reference count is the number of binary entries in off-diagonal cells across a row of the DSM in **Table 1.** *Example*: *Rule* 101 in *Chapter* 17, refers 37 times to other rules; references are from 15 *different* rules.

3.2.3 Rules Influenced: In Degree

Turning now to “in degree,” that is, the *Rules* situated at the end point of the arrow. These *Rules* are the most referred to by other *Rules*. **Figure 5** shows the in-degree network view. Recall that **Table 2** ranks *Rule* 4 on *sovereignty* as second in the ten most referred to *Rules* and also ranks second in **Table 4** on out degree. In **Table 5**, however, *Rule 4* heads the list on in degree. Earlier, we labelled these relationships as forms of influence. This may be accurate. Notably more significant is the reinforcement function embedded in, and represented by, both arrowhead and end point.

Given that the *Manual* is “meant to be a reflection of the law as it existed at the point of the Manual’s adoption …” (Schmitt 2017, 2), it is fair to say that it also represents the connections among laws. A review of **Figures 4** and **5** more than confirms this statement. Note that each link (i.e. interface or edge between *Rules* or nodes) connotes the direction of the connection.

The arrowheads—regretfully not easily discernable in print—signal source and destination. It should come as no surprise that the system as a whole is tightly linked. The connections reflect the recorded history as well as the operational “memory.”

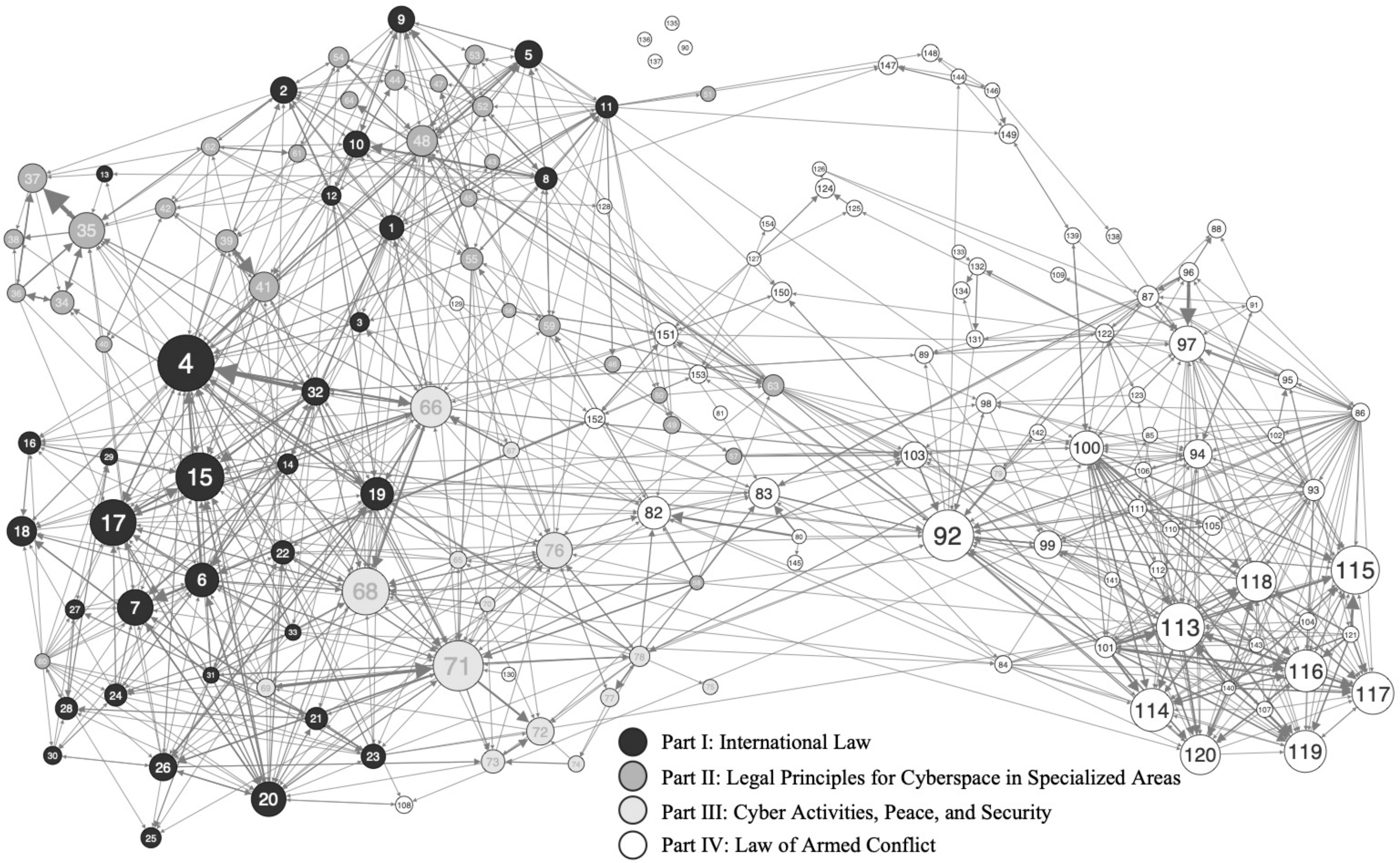


Figure 5. In Degree Centrality View of *Tallinn Manual 2.0.*

Source: Based on *summed frequency by cell* Design Structure Matrix in **Table 3** for text of *Tallinn Manual 2.0* [6].

Note: Node size is based on the total frequency of references made to a *column-Rule* in the commentary of *row-Rules.* Arrow width indicates the frequency with which source *Rule* (node) refers to target *Rule* (node) at the head of the arrow.

Table 5. In Degree: *Rules* Most Frequently Referred to by Other *Rules* (ranked by frequency)

*Rule**		*Chapter**		Reference Frequency	Reference Count
4	Violation of sovereignty	**1**	Sovereignty	41	25
92	Definition of cyber attack	**17**	Conduct of hostilities	36	27
71	Self-defence against armed attack	**14**	The use of force	35	21
15	Attribution of cyber operations by State organs	**4**	Law of international responsibility	33	19
113	Proportionality	**17**	Conduct of hostilities	33	23
115	Verification of targets	**17**	Conduct of hostilities	33	19
68	Prohibition of threat or use of force	**14**	The use of force	32	22
17	Attribution of cyber operations by non-State actors	**4**	Law of international responsibility	31	19
114	Constant care	**17**	Conduct of hostilities	28	16
116	Choice of means or methods	**17**	Conduct of hostilities	27	16
117	Precautions as to proportionality	**17**	Conduct of hostilities	27	16
119	Cancellation or suspension of attack	**17**	Conduct of hostilities	27	16

Source: Based on computational analysis for text of *Tallinn Manual 2.0* [6].* Rule and Chapter titles are direct quotes from [6].

Note: Reference frequency is the sum of numeric values in off-diagonal cells down a column of the DSM in **Table 3**. Reference count is the number of binary entries in off-diagonal cells down a column of the DSM in **Table 1**. For example: Rule 4, in Chapter 1, is referred to 41 times in the text commentary of 25 different Rules.

4 Cyber Actions and Responsibilities

Different levels of aggregation yield different information and provide different “lenses” through which to “read” the Manual. More specifically, for example, when the *Rule frequency* matrix in **Table 3** is aggregated at the *Chapter-level*, the system structure of *Manual* consists of a 20 by 20 matrix, (organized into four *Parts*). The results are shown in **Table 6,** the entries in the cells at the *row-column* intersection signal the *number* of references made by *Rules* in a *row-Chapter* to *Rules* in *column-Chapter.* So, too, entries in the diagonal cells signal the *sum* of *Rules within* a *Chapter* that refer to rules in the *same Chapter*. For example, the *Commentary* of *Rules* in *Chapter* 1 refers to *sovereignty* fourteen times in that same *Chapter*. This frequency may well be a form of design reinforcement to stress the power of sovereignty, in terms of principle and practice, as well as a driving force.

Particularly compelling in **Table 6** is the entry of 324 incidents situated at the intersection of rows and columns for *Chapter* 17 on the "Conduct of Hostilities". This entry refers to the number of different times that *Rules* between 86 and 130 are referenced *within Chapter* 17. It is the highest occurrence of self-reference in the entire *Tallinn Manual 2.0*. Legal scholars may argue that this density incidence provides the *raison d'etre* for the *Manual*. Others might consider it self-evident, in that the overall mission of the *Tallinn Manual 2.0* requires the contents of *Part* IV. Still, others might view the entire references-record in *Part* IV as a generative feature of state sovereignty, one that requires no particular justification.

This specific entry of 324 on the diagonal of Chapter 17 draws attention to an issue related to Chapter 4 whose entry on the diagonal in **Table 6** of 96 self-references is the second highest systemwide. Given that Chapter 17 is on *cyber action,* and Chapter 4 focuses on *international responsibility,* we find rather weak cross-reference between the two *Chapters.* Chapter 17 refer only once to Chapter 4 (by Rule 108); by contrast, Chapter 4 refers to Chapter 7 Rules eleven times. On balance, therefore, we obtain a bifurcated view of *Tallinn Manual 2.0.* A closer look is shown in **Figures 6 and 7.**

The network views in **Figure 6** present three perspectives on Chapter 17 – labelled (a), (b) and (c). This *Chapter* is the longest in *Manual*—spanning *Rules* 86 to 130 and accounting for 30% of the 150 *Rules* therein. The high density of dependencies (or edges) among *Rules* within the *Chapter 17* is evident. By contrast, *Chapter 17* references to *Rules* in other *Chapters* are considerably fewer, and mostly connected to *Part* IV. References made to Chapter 17 by other *Chapters* are still even fewer. All of this indicates that *Chapter 17* is largely self-contained and loosely connected to the rest of *Tallinn Manual 2.0.* Most important, however, it is also disconnected to Rules in *Chapter 4* addressing the *responsibility* of the State in the *conduct of hostilities.* **Figure 7** shows three perspectives for Chapter 4 as well. But the patterns of dependencies and concentration of Rules are very different than those in the previous **Figure 6**. The *Rules* of Part 1 "radiate" out to connect with the rest of the network.

Table 6. Structure of *Tallinn Manual 2.0* – Based on Frequency DSM in Table 3

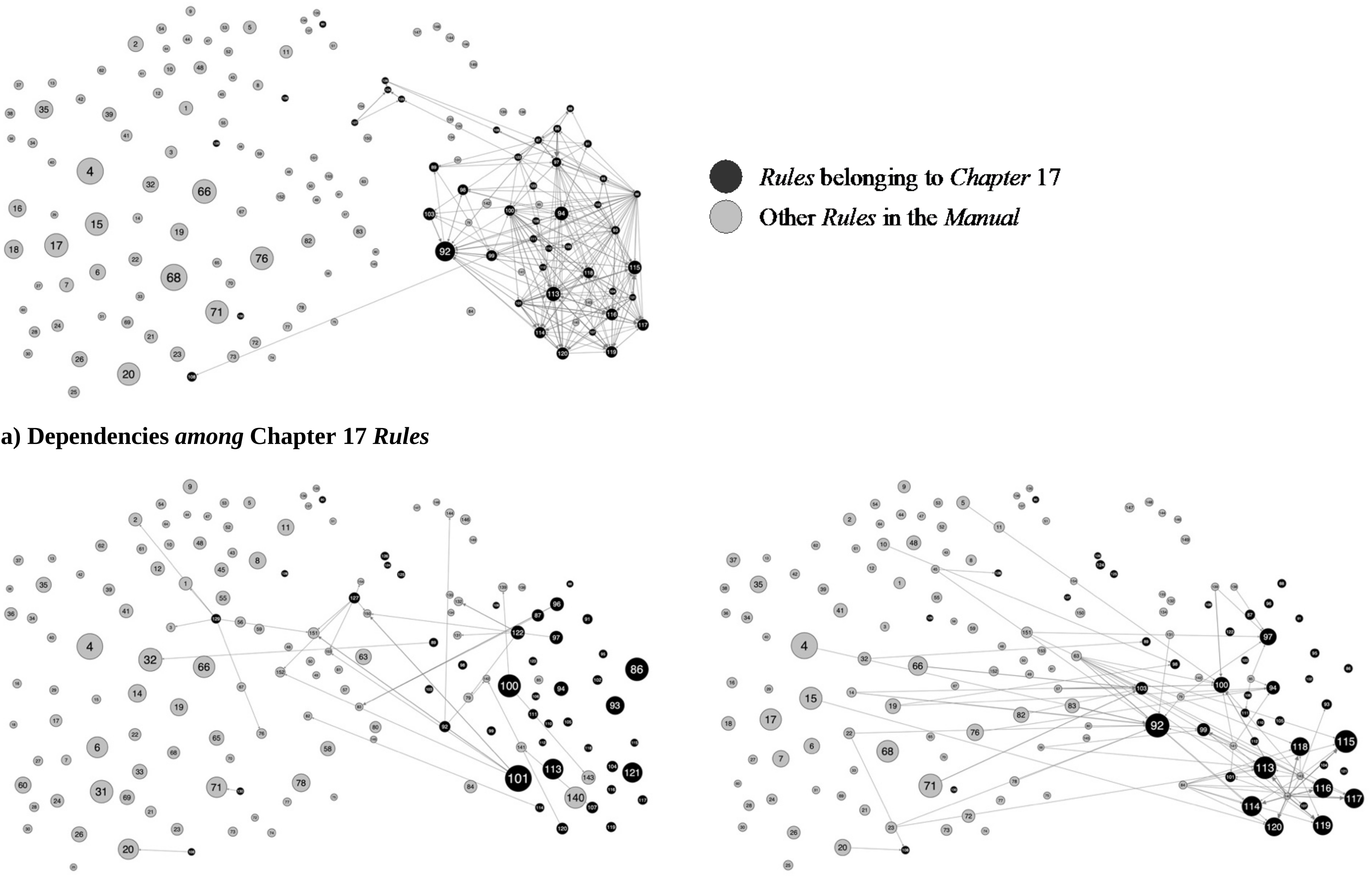
		Part I					Part II						Part III				Part IV				
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Part I	**1. Sovereignty**	14	1	10	13	3	4	4	3	1		2		8	6	1		2			1
	2. Due diligence	5	6	2	9	2	1							1	4		1				2
	3. Jurisdiction	9		18	4		3	11	14	1	3					1	2	1		4	1
	4. Law of International Responsibility	12	22		96	3	4	3	2		1	1		6	18	6	5	11			
	5. Cyber operations not per se regulated by international law	11	2		15	1	1	2	1					3	7		2	1			
Part II	**6. International human rights law**			1	2	1	34					1									
	7. Diplomatic and consular law		2	3	7	1	1	16				1			1		2				
	8. Law of the sea	8		2	5				18	1		3		2	3	1	2	2			
	9. Air law	3		5					3	3				1	5	1		3			1
	10. Space law			1	17				1	1	3	3	1		7	1	2	2			
	11. International telecommunication law	3	1	3	1		1	1	4	3	1	6						9			
Part III	**12. Peaceful settlement**	2		1	4	1								1	3	1	2				
	13. Prohibition of intervention	8			9	1	2							4	4	2		2			
	14. The use of force	2	3		20	1		1					1	1	28	5		2			
	15. Collective security			1	2		2						1		9	11	4	5			
Part IV	**16. The law of armed conflict generally**													1			12	15	1		1
	17. Conduct of hostilities	3			1	1									1	2	4	324	9		13
	18. Certain persons, objects, and activities																	53	6	5	
	19. Occupation																		2	5	
	20. Neutrality	1	3		2				1						1			2			7

Part I: General international law and cyberspace

Part II: Specialised regimes of international law and cyberspace

Part III: International peace and security and cyber activities

Part IV: The law of cyber armed conflict


● *Rules* belonging to *Chapter* 17
● Other *Rules* in the *Manual*

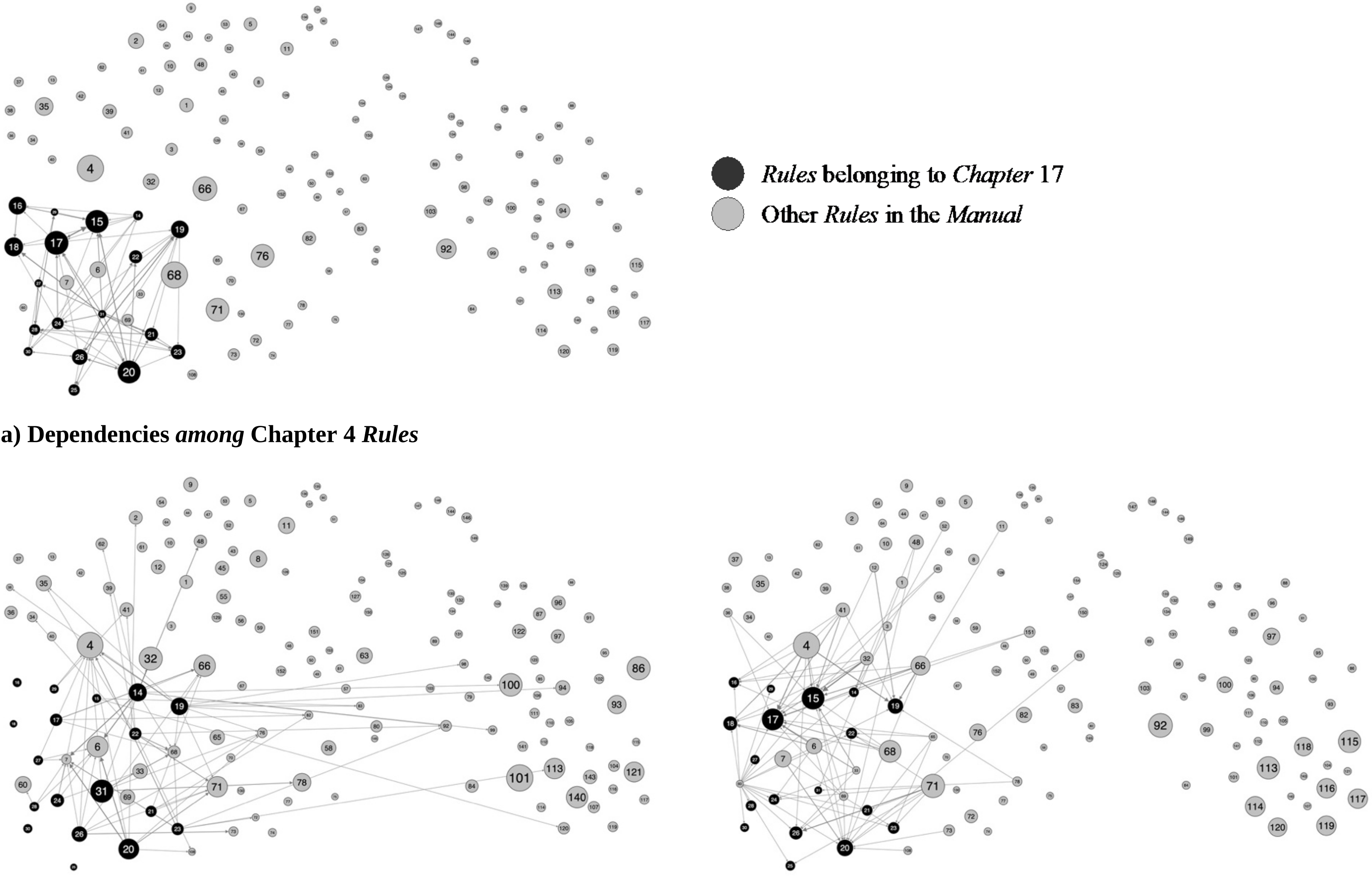
(a) Dependencies *among* Chapter 17 *Rules*

(b) References made to *Rules* in *Chapter* 17

(c) References made by *Rules* in *Chapter* 17

Figure 6. *Rule* Dependence in Chapter 17 on Cyber Action and Conduct

Source: Figure (a), (b) and (c) based on Figures 3, 5 and 4 respectively. See notes to these Figures for details


● *Rules* belonging to *Chapter* 17
○ Other *Rules* in the *Manual*

(a) Dependencies *among* Chapter 4 *Rules*

(b) References made to *Rules* in *Chapter* 4

(c) References made by *Rules* in *Chapter* 4

Figure 7. *Rule* Dependencies in Chapter 4 Focusing on Cyber Responsibilities

Source: Figure (a), (b) and (c) based on Figures 3, 5 and 4 respectively. See notes to these Figures for details.

5 Cybersecurity and Information Security

Our purpose here is to take note of *Rules* that refers to cybersecurity (i.e. cyber security) specifically and then to highlight *Rules* directed more generally at information security.

Three *Rules* mention "cyber security" explicitly. One is located in *Part* I on international law, namely, *Rule* 24 on states "entitled to take countermeasures" (Schmitt 2017, 131). The others are located in *Part* II on legal principles for cyberspace in a specialized area, and *Part* III on cyber activities, peace, and security. These are, *Rule* 48 addressing cyber operations in territorial areas, and *Rule* 69 on defining the use of force, respectively. Interestingly, none carry notable salience in the system as a whole.

We recognize that attention to cybersecurity is reflected in many Rules without reference to the terms "cyber security". We do not wish to underestimate the relevance of cybersecurity here. The same holds for explicit attention to "information security" as shown in **Table 7**; to security of media, including social media, in **Table 8**; and to e-Services, e-Commerce, and e-Government, in **Table 9**.

Table 7. *Rules* on "Information Security"

Rule*		***Chapter****		**Eigen centrality**
4	Violation of sovereignty	**1**	Sovereignty	0.996
15	Attribution of cyber operations by State organs	**4**	Law of international responsibility	0.817
6	Due diligence (general principle)	**2**	Due diligence	0.469
36	Obligations to respect and protect international human rights	**6**	International human rights law	0.032

Source: Based on *summed frequency by cell* Design Structure Matrix in **Table 3** for text of *Tallinn Manual 2.0* [6]. * All Rule and Chapter titles are direct quotes from [6].

Note: Eigenvector centrality generated with Gephi 0.9.2 software [16].

Table 8. ***Rules*** **on "Security of Media, including Social Media"**

Rule*		***Chapter****		**Eigen centrality**
66	Intervention by States	**13**	Prohibition of intervention	0.868
15	Attribution of cyber operations by State organs	**4**	Law of international responsibility	0.817
35	Rights enjoyed by individuals	**6**	International human rights law	0.567
6	Due diligence (general principle)	**2**	Due diligence	0.469
2	Internal sovereignty	**1**	Sovereignty	0.434
39	Inviolability of premises in which cyber infrastructure is located	**7**	Diplomatic and consular law	0.352
21	Purpose of countermeasures	**4**	Law of international responsibility	0.318
120	Warnings	**17**	Conduct of hostilities	0.271
41	Inviolability electronic archives, documents, and correspondence	**7**	Diplomatic and consular law	0.229
10	Extraterritorial prescriptive jurisdiction	**3**	Jurisdiction	0.226

Source: Based on computational analysis for text of *Tallinn Manual 2.0* [6]* Rule and Chapter titles are direct quotes from [6].

Note: Eigenvector centrality generated with Gephi 0.9.2 software [16].

Table 9. ***Rules*** **on "e-Services, e-Commerce, and e-Government"**

Rule*		***Chapter****		**Eigen centrality**
66	Intervention by States	**13**	Prohibition of intervention	0.868
2	Internal sovereignty	**1**	Sovereignty	0.434
69	Definition of use of force	**14**	The use of force	0.244
28	Reparation (general principle)	**4**	Law of international responsibility	0.204

Rule*		***Chapter****		**Eigen centrality**
14	Internationally wrongful cyber acts	**4**	Law of international responsibility	0.141
142	Respect for and protection of cultural property	**18**	Certain persons, objects, and activities	0.114
43	Use of premises and activities of officials	**7**	Diplomatic and consular law	0.055

Source: Based on computational analysis for text of Tallinn Manual 2.0 [6]. * Rule and Chapter titles are direct quotes from [6].

Note: Eigenvector centrality generated with Gephi 0.9.2 software [16].

6 Stand-Alone *Rules*

The *Tallinn Manual 2.0* harbors four *stand-alone Rules,* namely isolated *Rules* with no connection to other *Rules* in the system. These are shown in **Table 10**. Interestingly, they are all clustered in *Part* IV on the *Law of Armed Conflict.*

Table 10. Stand-Alone *Rules*

Rule*		***Chapter****	
90	Mercenaries	**17**	Conduct of hostilities
135	Protection of detained persons	**18**	Certain persons, objects, and activities
136	Correspondence of detained persons	**18**	Certain persons, objects, and activities
137	Compelled participation in military activities	**18**	Certain persons, objects, and activities

Source: Based on summed frequency by cell Design Structure Matrix in Table 3 for text of *Tallinn Manual 2.0* [6].

Note: * All Rule and Chapter titles are direct quotes from [6].

The first stand-alone *Rule*, *Rule* 90, states that mercenaries “involved in cyber operations do not enjoy combatant immunity or prisoner of war status” [6]. This *Rule* is explained, or justified, by reference to customary law and the conditions that define mercenaries. It remains open for debate whether contemporary cyber-hackers can be considered mercenaries or enemy combatants if they are situated behind enemy lines. To non-lawyers, *Rule* 90 might appear to place cyber hackers in a particularly unprotected position, due less perhaps to their skill set than to their mercenary status.

By contrast, the second and third stand-alone *Rules*—*Rule* 135 and *Rule* 136—appear to provide some protection for entities defined therein. *Rule* 135 concerns the protection of information about interned and other people(s). *Rule* 136 gives detained or interned individuals access to cyber venues for communication. The fourth stand-alone *Rule* is *Rule* 137, on prisoners of war.

We cannot derive or infer a logic about the stand-alone or isolated status of these four *Rules*. *If* they are fundamental to the entire system, *then* why are they not linked to the network model in one way or another? Given that they are unconnected, they appear to be "tacked on." If they were "tacked on" then what would their status be, relative to the system as a whole? Should these *Rules* be given the same attention as all other *Rules*? Since they are *stand-alone*, there is no way of determining their salience relative to other *Rules* or within each of the *Parts*.

7 Where is Authority in *Tallinn Manual 2.0*?

By definition, every legal system is anchored in authority principles. We recognize that the Introduction addresses authority of the *Manual* (italics inserted), here we ask: *Where* is authority located in *Tallinn Manual 2.0*? The answer is clear: Authority for cyber operations is almost exclusively assigned to the state system.

Higher centrality *Rules* on authority are shown in **Table 11**. Of these, three are explicitly related to the state and its jurisdiction, that is *Rules* 1 & 2 on sovereign authority of the state over cyber infrastructure, people, and cyber activities located within its territory and *Rule* 4 on violation of state sovereignty.

Noteworthy *Rules* on jurisdiction of authority are Rules 8–9 in conduct of cyber operations by a state within its territory, and Rules 10–11 on "extraterritorial enforcement," whereby a state can exercise authority over cyber activities outside its territory under international law or with the consent of another country.

Rules of higher salience on *attribution* of cyber action authorized by the state include: *Rule* 15 on attribution of cyber operations by conducted by state organs; *Rule* 16 on cyber operations conducted by a state organs made available to another state are attributable to the later; *Rule* 17 on when cyber acts by non-state actors are attributed to a state; and *Rule* 19 on when authority assigned to a state for cyber operations in other state is not regarded as unlawful; and *Rule 21* on authority of state to induce response from other state to comply with the legal obligations later owes. These *Rules* are all situated in *Part* I on International Law.

Finally, *Rule* 34 (in Part II) on applicability of human rights, as applicable to cyber operations, in foreign territory under a state authority; *Rule* 66 is on limits of state intervention in other states, and *Rule* 76 on role and authority of United Nations on the collective security—both located in Part III; and *Rule* 115 in Part IV on verification of the objectives to be attacked before authorization of cyberattack.

Table 11. High-salience *Rules* on Authority

Rule*		***Chapter****		**Eigen centrality**
4	Violation of sovereignty	**1**	Sovereignty	0.996
66	Intervention by States	**13**	Prohibition of intervention	0.868
17	Attribution of cyber operations by non-State actors	**4**	Law of international responsibility	0.849
76	United Nations Security Council	**15**	Collective security	0.819
15	Attribution of cyber operations by State organs	**4**	Law of international responsibility	0.817
19	Circumstances precluding wrongfulness of cyber operations	**4**	Law of international responsibility	0.549
16	Attribution of cyber operations by organs of other States	**4**	Law of international responsibility	0.545
2	Internal sovereignty	**1**	Sovereignty	0.434
1	Sovereignty (general principle)	**1**	Sovereignty	0.349
115	Verification of targets	**17**	Conduct of hostilities	0.347

Source: Based on summed frequency by cell Design Structure Matrix in **Table 3** for text of *Tallinn Manual 2.0* [6].

Note: * All Rule and Chapter titles are direct quotes from Schmitt (2017). * Rule and Chapter titles are direct quotes from [6]. Eigenvector centrality generated with Gephi 0.9.2 software [16].

8 Feedback: How the “Pieces” Fit Together

Feedback, in its various forms, reflects the complexity of order and disorder, “which gives it [the complex system] adaptive power” [11]. The interested reader may wish to trace the connections among Rules in any of the Figures above in order to infer or identify feedback relations embedded in *Tallinn Manual 2.0*. These figures reflect different facets of the *Manual.* In those terms, these Figures reflect the cohesion as well as the "adaptive" power of *Manual.*

Far more stark, however, is the network view of *first order feedback* between two *Rules* shown in **Figure 8**. Jointly the *arrowhead, source, destination,* and *weight* provide a compelling view of the network interface, or edge, systemwide. This Figure reveals only the *direct* feedback between nodes (*Rules*) and across *Parts;* all others are "hidden" from view. Here we draw attention to six notable features:

First, and most obvious, 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 and the relatively sparse *Rule* feedback dependencies within Parts II and III.

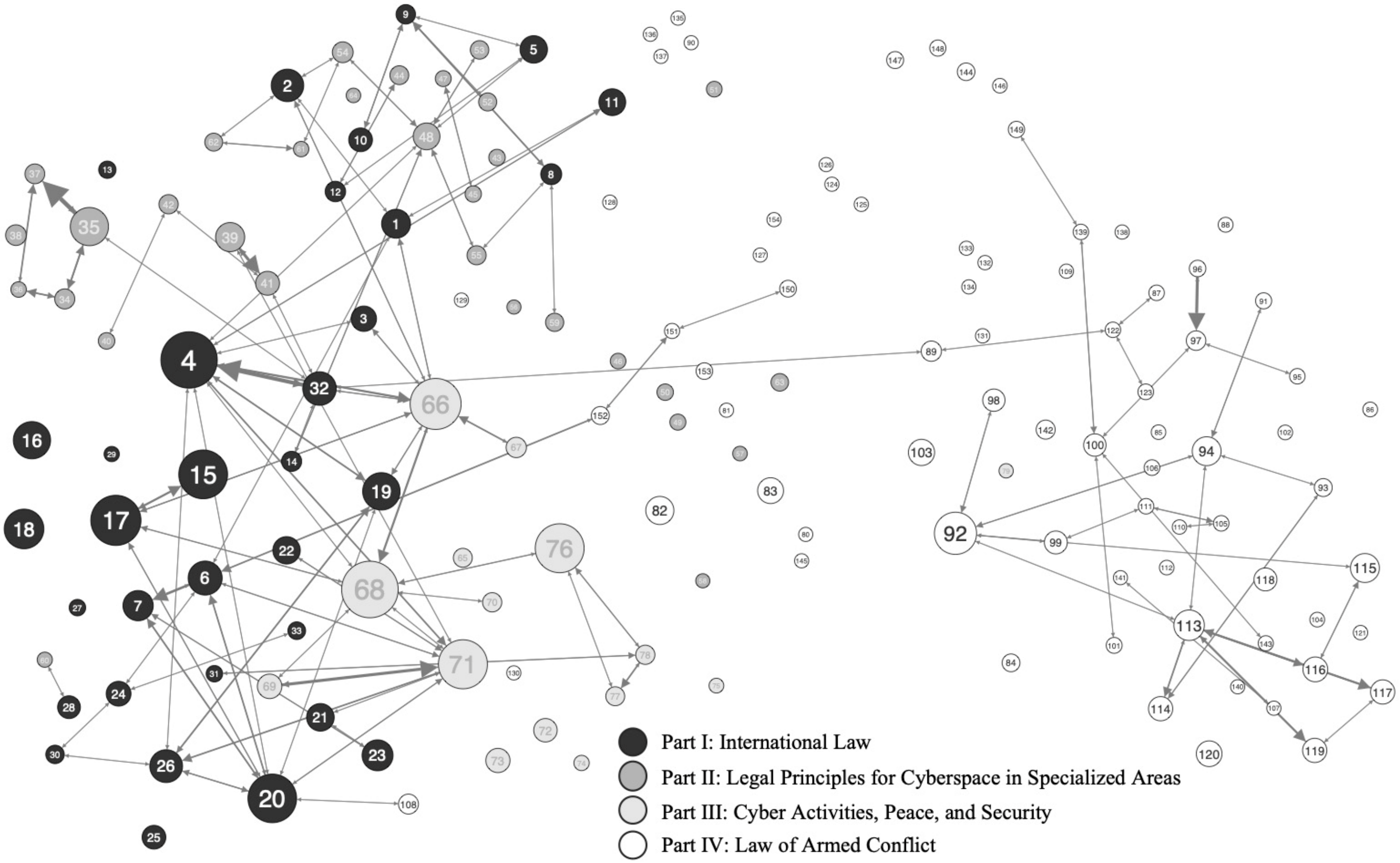
Second, is the corollary that follows that there is *no feedback* between the *Rules* in Part IV and Parts II and III. This may well be due to the somewhat unchartered character of the cyber domain and its situational logic in matters of war and peace. This is more an affirmation of the power of international law, perhaps, than of its diffusion systemwide.

Third are the *multiple direct instances* of feedback between Parts I & II (twelve loops); Parts I & III (sixteen loops); and Parts I & IV (only three loops). This stands as further indication of the strength of international law

Fourth is the *very "thin" direct feedback* link holding the pieces of the *Tallinn Manual 2.0* together, that is, muted or limited feedback involving Part I and Part IV (three feedback loops), and Parts II and Part III (only one direct feedback link).

Fifth is the structure of "thin" direct feedback connections. The system as a whole is directly held together by edges of three sets of *Rule*s—(a) *Rules* 6 and 152; (b) *Rules* 20 and 108; and (c) *Rules* 32 and 89—that connect Part 1 and Part IV. Interestingly, *none* of the Rules in Part IV—*Rules* 152, 108 and 89—are of high salience.

Sixth is an issue referred to earlier, namely, the seeming pivotal role of *Rule* 92. The many references to, and from, *Rule* 92—shown in Figures 2 and 3, for example—signal features of system structure, but they do not contribute to any "pivotal" role connecting Part 1 and Part IV. *Rule* 92 on "Definition of Cyberattack," in Part IV is directly linked to several other *Rules* within *Part* IV *and* thus serves to reinforces the logic of the *Law of Armed Conflict*



4
32
66
68
71
76
20
15
17
16
18
19
1
2
3
5
6
7
8
9
10
11
12
13
14
21
22
23
24
25
26
27
28
29
30
31
33
34
35
36
37
38
39
41
42
48
55
59
67
69
72
73
77
78
82
83
89
92
94
97
98
99
100
103
113
114
115
116
117
118
119
120
● Part I: International Law
● Part II: Legal Principles for Cyberspace in Specialized Areas
● Part III: Cyber Activities, Peace, and Security
○ Part IV: Law of Armed Conflict

Figure 8. First-order Feedback in the *Tallinn Manual 2.0.*

Source: Based on *summed frequency by cell* Design Structure Matrix in **Table 3** for text of *Tallinn Manual 2.0* [6].

Note: Based on **Figure 3** on "edge salience view" of the *Tallinn Manual 2.0* [6]. Node size represents eigenvalue centrality score. Arrow width indicates the frequency with which the source *Rule* (node) refers to the target *Rule* (node) at the head of the arrow.

Table 12 identifies the count of direct feedback loops throughout the *Manual*. All other potentially supportive feedback connections in the overall system architecture are indirect, that is, travelling through various intervening e*dges*.

Table 12. Direct Feedback Loops between *Rules* in the *Parts* of *Tallinn Manual 2.0*.

	Part I	**Part II**	**Part III**	**Part IV**
Part I	56	12	16	3
Part II	12	26	1	
Part III	16	1	20	
Part IV	3			62

Source: Derived from the database of **Figure 8** “First-order Feedback in the *Tallinn Manual 2.0*.”

9 End Note

This paper presents an application of computational methods to a seminal work in international law, namely, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. The product of expertise and excellence, the *Tallinn Manual 2.0* is groundbreaking in scale and scope.

We proceeded from the assumption that text-as-conduit imposes a sequential linear order on a system of interconnected logic, and that text as such cannot do justice to what is clearly a system of considerable complexity. Policy documents usually written in text form—word after word, sentence after sentence, page after page, section after section, and chapter after chapter—which often masks some of their most critical features. The text form cannot easily show “hidden” features such as interconnections among elements or the relative salience of issues, for example.

Informed by complexity science and commensurate computational logic, notably [17] —while recognizing pervasive challenges of policy and practice [18, 19] —this paper presents the *Tallinn Manual 2.0* in the most detailed terms. It puts forth a “proof of concept” for the contribution of computational methods to our understanding of policy documents. Our method consists of steps to: (1) convert the text form into a formal system structure, (2) construct a design structure matrix (DSM) in order to represent content, concepts, and organization, (3) identify interconnections among *Rules* (across *Chapters* and *Parts*), (4) compute the salience of interconnection between *Rules*, (4) create a network model of the whole system and, on this basis, (5) draw on the basic results as a reference mode, (6) explore alternative system properties and examine diverse aspects of this seminal work.

It is fair to ask: “what is the value of this approach?”

The results reveal the central features of the *Manual* that are difficult to identify or to recognize simply by reading the text.

Our purpose in this *End Note* is not to review or summarize the results. Rather it is to highlight the obvious: different perspectives or levels of aggregation yield different information and provide different “lenses” through which to “read” the *Manual*. We have approached the computational initiative from many different perspective. We began with a reference case wherein all *Rules* and interfaces are considered “equal” (**Table 1**).

But what if all *Rules* were not equal? What if all interfaces or edges were not similar?

We then departed from the reference case and explored the *Manual* through different “lenses,” by replacing the assumption of all elements being “equal” and with an empirical model anchored in frequency of *Rule* references **(Table 3).** Then we presented network views of the reference case, and illustrated its contents in tabular form. All are correct in that they consist of accurate and empirical specification of content.

Furthermore, the results generate a degree of transparency for the entire legal system by providing information that is not readily available by reading the text form alone. For example, they allow us to determine the relative salience of individual *Rules*, and to identify *Rules* that are unconnected to the rest of the corpus.

The results amply demonstrate how the principle of *sovereignty* pervades and dominates all aspects of international law for cyber operations and, by extension, how authority is vested in the state. More important however, the results also show great *variation* among *Rules* in terms of their relevance to the entire system. We can now identify the *Rules* that are most salient by *Chapter* and *Part*.

Of the many specific results of this investigation, those related to direct feedback connections are among the most significant. We referred to the “thin line” holding the system together. If this is correct, we must also recognize the low salience of the indirect or intervening connections that may be buttressing the “thin line.”

The logic of the *Tallinn Manual 2.0* 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. This is a powerful assumption indeed, one that augments rather than undermines the complexity of international law in this context. In retrospect, it is clear that until very recently cyberspace has been a matter of low politics for the state system as a whole. This is no longer the case. Not only is the cyber domain highly politicized, its operations are based on principles other than those anchored in sovereignty. Now that cyberspace has been catapulted to the highest levels of high politics, the international community as a whole 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.

Then, by definition, legal systems are structured to resist pressures for rapid change. Equally, by definition, all matters “cyber” transcend any efforts to limit the rates of change for any aspect thereof. We recognize that the *Tallinn Manual 2.0* was not designed to “fit” the characteristic features of cyberspace but 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 transmitted, 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 by non-state entities.

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.