#CY17–2

OSTROM WORKSHOP
PROGRAM ON CYBERSECURITY
AND INTERNET GOVERNANCE

white paper series

Emanations of the Informational State: Cyber Operations and the Difficulties

Sandra Braman

Presented at the Inaugural Ostrom Workshop Colloquium on Cybersecurity and Internet Governance, Indiana University Bloomington, April 27–28, 2017.

INDIANA UNIVERSITY BLOOMINGTON
OSTROM WORKSHOP

Emanations of the Informational State: Cyber Operations and the Difficulties[1]

Sandra Braman

"In effect, almost every computer in America is a potential border entry point."
(Rosenzweig, 2012, p. 1)

The more they talk the worse it gets.

When the North Atlantic Treaty Organization (NATO) pulled together an international team of legal experts to consider the extent to which, and the ways in which, existing international law applies to cybersecurity and cyberwarfare, their 2013 conclusions as published in the *Tallinn Manual* highlighted ways in which the state itself, as a specific type of political system, has become uncertain and besieged. "Uncertain," because the state as a Lockean (1690/1964) locus of consciousness, a perceptual entity (Beck, 1990; Scott, 1999) with its own ways of knowing itself and others (Braman, 1985, 2006), has decreasing confidence in its ability to effectively act, exercise power, in general; to act on its knowledge in particular; and, actually, to effectively know. "Besieged" in the sense that states are now often in confrontation with not only other states, but also with non-state actors that include, in addition to corporations, autonomous networks that make information releases by individuals such as Julian Assange and Edward Snowden possible. At the same time, they are experiencing challenges from the international legal community on questions about whether or not particular cyber operations are, in fact, legal.

Just what the "state" is, these days, is discussed more fully below, but in its most abstract form as used here the reference is to the ideal type as it has existed within the Westphalian system as that system developed about 500 years ago. The Westphalian point is important because it is not only individual governments that feel themselves to be under attack in diverse forms, regularly and consequentially. The system in its entirety, too, is weakening and under attack. This matters when thinking about peace and war because international laws of war come from treaties signed by states that, at the point of signing, assumed it would only be states that would be of concern to them for the purposes of those treaties because of the nature of the system within which the agreement was taking place and which the agreement was, in turn, helping to continue to build and sustain.

The inability of the group of international legal experts involved to agree on many aspects of what it means to be a state joined other frustrations at the conclusion of the process by which the first edition of the *Tallinn Manual* (2013) was published. The sources

[1] Thanks to participants in the Inaugural Ostrom Workshop on Cybersecurity and Internet Governance at Indiana University, April 28-29, 2017 organized by Scott Shackleford for their valuable feedback on this work. This piece was first published as: Sandra Braman, "Emanations of the informational state: Cyber operations and the difficulties," *First Monday*, *22*(5), 1 May 2017;
http://journals.uic.edu/ojs/index.php/fm/article/view/7870/6295
doi: http://dx.doi.org/10.5210/fm.v22i15.7870.

of frustration were explicitly detailed in the text. A characteristic of the Tallinn manuals that makes them worth studying now and ensures they will have very long shelf lives as desk references is that they include not only "black letter" points of law and other matters on which they all agreed.[2] They also discuss points upon which they could not agree, identifying majority and minority positions and in most cases including arguments offered by those who take each position. Conclusions from the analysis of the first edition of the *Tallinn Manual* (2013) referred to throughout this piece were based on examination of what could be learned from studying the collection of points of disagreement and looking at interactions among issues raised when looking across them. In the first manual, the concept of "disagreement" was used to refer to a variety of types of reasons why the group of experts did not reach a consensus on particular points. By the second edition, that concept had become unbundled into several types of disagreements -- distinguishing matters that weren't comprehensively discussed and upon which they were uncertain, as well as points of view held by others outside the group but not represented within the group of experts writing the manual -- that were of use in the analysis offered here that for *2.0* also includes an analysis of consensus positions.

To address the many additional areas needing attention that had surfaced during discussions on the first edition, particularly in the area of what to do about cyber operations that do not rise to the level of being considered attacks under the laws of war but that do justify government action, a second, somewhat smaller group of experts – partially overlapping with the group of those involved in the 2013 volume and partially not -- was convened to work on a second edition by the NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE, https://ccdcoe.org/) in Tallinn, Estonia, the institutional home for these processes. It must be assumed that there were also hopes that in the course of continued conversation, taking into account the results of always-continuing technological innovation, what has been learned from additional events, and changes in strategy, it might have been possible to achieve consensus in those areas marked by disagreements at the close of round one.

As it turned out, by the time of the second edition -- published only 4 years after the first -- the group of experts had retreated from a number of its earlier positions, notably but not only as regards non-state actors. In the *Tallinn Manual 2.0* (2017), the state comes through as even less certain, certainly more ambiguous, confused, and in many places self-contradictory. No wonder cybersecurity is considered the "most discussed, but least understood" domain of transnational law (Koh, 2017, p. 488).

This paper explores what changed in the conceptualizations of the state that underlie the analyses of the two Tallinn manuals.[3] On many of the most difficult issues, the experts involved in *Tallinn Manual 2.0* apparently found themselves helpless in the face of an operational need to resolve seemingly unresolvable issues. The result was an analysis that tries to have it both ways at once in a number of critical areas. The most important of

---

[2] The plural is used here because there is enough difference in the positions taken across the two volumes, *Tallinn Manual* (2013) and *Tallinn Manual 2.0* (2017), to justify keeping both on the shelf for reference purposes.

[3] The second edition includes a concordance so that relationships between the rules, different in number and differently numbered in the two editions, can be followed analytically.

those that appeared in the foundational sections of the work are discussed below; it is expected that more will be uncovered as analysis of the additional texts continues.

As the leading figure in the Tallinn manual processes Michael N. Schmitt (2012) admits, these works involve input from legal experts from around the world, being more internationally representative in the second edition than the first, but essentially represent the US position. This fact does not obviate the utility of these documents as lenses into ways in which the state in general and the informational state in particular are being experienced and understood as we think about cyber operations. Indeed, the kinds of struggles around just what it means to exercise sovereignty and jurisdiction for cybersecurity and cyberwarfare issues are at the heart of what it means to be an informational state as a distinct geopolitical form. Taking the time to understand what that means is worth it because it is information policy tools that currently dominate international and domestic relations both. We open with some discussion of the general context.

Background

Revisiting the 2013 first edition as US politics unfold after the presidential inauguration of 2017 finds depressing forewarnings to which a reader did not so alert four years ago. Among the forms of interference deemed illegal under existing international laws of war and now so familiar, for example, are the generation and distribution of false news and interference with the elections of another country via cyberspace (I, Rule 10, p. 45).[4] (As is the case in public discussion of cyber interference by one country in another country's elections, the manual elides interferences with an election through persuasion effected through false news and digitally intervening in actual outcomes by hacking into voting machines, two very different ways for a state to exercise power with very different histories.) Another striking difference in the narratives is the higher visibility of particular private and public interests in the second edition. There intellectual property is treated as a national security concern, an argument bought by the U.S. Department of Homeland Security based on findings from research funded by the Motion Picture Association of America (MPAA) and undertaken by the RAND Corporation (Treverton, et al., 2009). A surprising amount of space is devoted to recurring consideration of whether critiques of government or those in government should be considered military attacks and/or justify a military response under existing international law.

In the first edition "cyberspace" is treated as a black box, but the second defines it as including the physical layer of global networks (hardware and other infrastructure such as cables, servers, and computers), the logical layer of networks (connections between devices that include applications, data, and protocols), and the social layer of networks (individual and group users engaged in activities reliant upon and taking place within the networks) (II, Rule 1). The distinction between cybersecurity and cyberwarfare in the first edition is replaced in the second with the single concept of "cyber operations" to refer to

[4] References in this paper are to the first edition of the *Tallinn Manual* (2013) when they are cited as "I," and to the second edition, *Tallinn Manual 2.0* (2017), when they are cited as "II."

both, a fix in response to the exquisite difficulties of determining when something should be considered an attack, and when there is war, in the cyber domain.

"Laws of war" come from the almost 50 treaties in place about how states must conduct themselves when – and how their actions will be legally understood as – they move towards war (*jus ad bello*), as well as those that deal with how states should conduct themselves and how their actions will be legally understood during war (*jus in bellum*). From the perspective of the ways in which cyberspace has problematized jurisdiction (a contemporary Internet issue), it is worth highlighting that the first of these was signed almost concurrently with the signing of the first international treaty to govern telecommunications networks as they crossed borders (a mid-19th century telegraph issue). Telecommunications treaties dealt with what we now call cybersecurity from the beginning (Rutkowski, 2011), and *Tallinn Manual 2.0* incorporates a great deal of telecommunications policy in the body of international law it examines. There are regular references in the news and public debate to the Geneva Convention, a treaty first passed in 1864 that has been amended several times, most recently in 2005, to extend protections for people against new weapons developed on the basis of continued knowledge production and/or technological innovation. The United Nations charter (1945) is among the laws of war, as are the Nuremberg Principles (1948) that criminalize many acts of war. Others are less well known; the 2008 treaty involved cluster munitions. These treaties are complemented by internationally accepted custom (customary law) and by agreement on general principles of the type enunciated in constitutions at the level of national governments.

Cybersecurity and Theories of the State

States vary in their forms significantly and across multiple dimensions. Even those we commonly treat as essentially alike can differ in profoundly important ways. Distinguishing among state forms according to their capacity for and reliance upon the use of informational power -- rather than power in its instrumental, structural, or symbolic forms -- is particularly useful when thinking about military issues in the cyber domain where all activities, whether preventive, offensive, or defensive, are informational as subject, tool, motivation, or all three. This section introduces the theoretical framework through which analysis of the state as understood by those who wrote the Tallinn manuals is undertaken. The following section looks at the concept of emanations of the state that came into use in *Tallinn Manual 2.0* at the point at which other theorization ceases.

Forms of the State

Caporaso (1996) clearly and usefully explicates a suite of terms based on deep knowledge of the scholarly literature: if the concept of *governance* refers to collective problem-solving in the public realm, and that of *government* to the institutions and the people who occupy key institutional roles, then the concept of the *state* refers to enduring structures of governance as institutionalized in government. Incorporating Bourdieuian field theory and complex adaptive systems theory into the framework allows us to see that any given political form, with its institutions, roles, practices, laws, and policies, represents but a moment of stability within a much wider, more diffuse, and constantly shifting field of

policy and power (Braman, 2006). Specific states and the legal systems that accompany – or emanate from – them derive from and, when transformed, disappear into this broader field. Elements that comprise the field include ethical and behavioral norms, discourse habits, cultural practices, codified and tacit knowledge and knowledge structures, organizational forms, and technologies themselves as well as the formal laws and regulations of officially recognized governments and the decision-making and practices of the private sector writ large (corporate), small (individual), or in between (networks, groups, and movements).

Just which dimensions of states matter for distinguishing among state forms varies by theorist, discipline, venue, and purpose. Typically empirical examinations find that states differ from each other by relative emphasis along a spectrum that often incorporates or intersects with differences along other dimensions as well. It is particularly useful to use dominant form of power as a lens through which to think about cybersecurity as doing so sustains and enriches the focus on the informational structures, processes, and events of such concern in the cyberwar arena. Using a typology of types of states that variously rely upon tools of power in its instrumental, structural, symbolic, and informational forms (Braman, 2006) further discussed below provides a conceptual foundation for addressing the state as it appears in discussions about exercises of power in the cyber domain. When legal experts have a hard time figuring out how cyber operations should be treated under international laws of war, they are engaged in the struggles of the informational state as it strives to understand what it is capable of doing, what it wants to do, what the right thing is to do, and what it is legal to do. This is a Westphalian problem, because as the informational state attempts to establish itself in Westphalian terms it is perturbing the system itself, or worse.

Caporaso (1996), again, provides a very clear and broadly synthetic summary of the characteristics of the Westphalian state as a Weberian ideal type: (1) a jurisdictional monopoly on legitimate violence, (2) a centralized administrative apparatus that collects taxes and implements government policies, (3) authoritative institutions and people who make policy in a wide range of areas, and (4) territorial sovereignty and juridical equality between states. The "Westphalian moment" was the period during which secular states articulated features such as their borders relative to others within the system and reified their characteristics as this type of political form.

Many believe we are undergoing a new Westphalian moment. Historians of the law describe the transformations currently underway in law-state-society relations as so profound in nature that they are equivalent to those that took place with the formation of the international system and the Westphalian state several hundred years ago. Difficulties conceptualizing the state revealed in the Tallinn manuals are manifestations of ways in which the informational state is attempting to identify its borders and legitimate its modes of exercising power within the Westphalian context. Ultimately the historical system may yield to another global formation, but at minimum there will certainly be continuing adaptations and interpretations of the law in an effort to appropriately and effectively implement it in the cyber domain. Either way, this period of turbulence should be expected to continue.

The Informational State

In the digital environment, the ability to use informational power has dramatically increased. And power in its virtual phase has become a site of conflict in its own right. Both matter when analyzing the issues raised in the Tallinn manuals.

Informational power. Analyses of power have typically distinguished among three forms. *Instrumental power* shapes human behaviors by manipulating the material world via physical force. The use of traditional weapons – what are now referred to as "kinetic" to distinguish them from cyber weapons -- is instrumental. This type of power has been so important that political theory classically defines a state as the political entity that exercises physical control over a specified geographic space. *Structural power* shapes human behaviors by manipulating the social world via rules and institutions that limit degrees of freedom, determine how specific activities will be undertaken, and reduce uncertainty. The international law discussed in the Tallinn manuals is itself a form of structural power, a point that does make the alignment of the views of the NATO international groups of experts involved with the US position significant for geopolitical purposes. *Symbolic power* shapes human behaviors by manipulating ideas, words, and images; it is often referred to as soft power (Nye, 2005). Symbolic power also has ancient roots; in modern forms, the exercise of symbolic power has included propaganda, public diplomacy, campaigns, efforts to influence public opinion, and the education system.

Over the course of the informatization of society, a fourth form of power became evident, not because it was new but because its relative importance had become so much greater as a result of the informatization of society (Braman, 2006). *Informational power* shapes human behaviors through manipulation of the informational bases of instrumental, structural, and symbolic power. Today's "smart weapons," that can identify a target and direct themselves to it without human intervention, are examples of the effect of informational power on the exercise of instrumental power. Informational power is influencing structural power – affecting how it is exercised, that is, and how effectively -- when compliance with intellectual property rights law is enacted surveillance of Internet use. Informational power affects the exercise of symbolic power, for example, when web-based messages or on-site advertising are tailored to specific users who are online or walking by.

Informational power can also be exercised through entirely new techniques of power not historically available and that are informational only. Data mining vast quantities of information in diverse forms using pattern recognition is an example of a qualitatively new technique for exercising power. Finding patterns of strategic use through analysis of the information available, of course, is nothing new, but again Engels' law applies – at some point change in quantity (how much you have of a thing) yields change in quality (the nature of the thing itself). The Tallinn manuals are efforts to think through the nature and uses of tools of informational power within the context of conflict and war between states and as they demark the positions and boundaries of the informational state within the Westphalian system.

Power in its virtual phase. Political scientists also have long distinguished between power in its actual phase (as it is being exercised) and in its potential phase (power that is claimed, but not currently being used – this might more accurately be termed "putative" power). Incorporating the insights of neoclassical economics into our thinking, the notion

of “sunk power” (power exercised in the past the effects of which are evident in the present) is useful as well. Actual power is potential power in use, as when guns are firing, laws are being implemented, and persuasive campaigns affect the vote. Potential power becomes actual only through specific practices. Information processing, distribution and use are often necessary for the transformation of power from potential to actual. The number of tanks owned by an army, laws on the books that aren't currently being acted upon, and ideas for communication campaigns are all examples of power in its potential phase.

In today's information-intense environment, it is now also possible to recognize power in what has been termed a "virtual" phase. A concept embedded in a long history of thinking about “vertu” (Braman, 1996) and following economist Roberto Scazzieri (1993) in his definition of virtual materials and processes, virtual power includes techniques of power that are not currently extant but that might be brought into existence using available resources and knowledge.[5] It includes power that can be acquired or developed through transfers of power, use of resources, or shifts in internal or external conditions. Knowledge is so central to power in its virtual phase that every expansion of the knowledge base of a nation-state concomitantly causes a growth in the realm of potential power available to it. An example of power in its virtual phase would be government control over the development of encryption techniques or of scientific research in areas believed to be of value for national security purposes, for in such instances the actual techniques or inventions do not yet exist. Power in its virtual phase is so important to national competitiveness and the ability to protect national security in the 21st century that research and development (R&D) are now considered key resources for the informational state. Government seizure of patents is another means through which a state can take control over power in its virtual phase.

The Informational State and Challenges to the Westphalian System

What those in the information policy world think of as exercises of informational power include the cyber operations of focal concern in the Tallinn manuals. Demchak and Dombrowski (2013) describe the current period as the "cyber Westphalian" moment because states are seeking sovereignty within and over cyberspace, requiring redefinitions of themselves along the way. Describing the efforts through which governments are attempting to replicate the features of the Westphalian state by establishing "cyber borders" as "nonlinear, dangerous" and likely to be lengthy (*Ibid.*, p. 33), they suggest that there is no guarantee that states will continue to be the dominant political form in the future.

The sense that this is a transformational period is shared by others. Mačák (2016) points out that the *Tallinn Manual* has been so influential because the weaknesses of contemporary states have created a crisis. Indicators of crisis for this author include the

[5] When I started using the term “virtual” to refer to power in this phase, the word was in use but had not yet taken on the dominant and ubiquitous usage we are now so familiar with. A new term is needed. Recommendations for another term that would more uniquely capture the particular verb form -- the "tense," or mode of being -- captured by Scazzieri's insights are welcome and will be fully attributed if used.

international community's failure to seriously engage treaty proposals dealing with cyber operations and the extent to which states have shied away from making the decisions about controversial legal questions necessary as a foundation upon which international agreements can be based.

Technologically-driven challenges to the nature of the state are not new. The Tallinn manuals should be read within the context of a long conversation about interactions between networks and jurisdiction that goes back to the mid-19th century treaties for the telegraph (Rutkowski, 2011), signed essentially concurrently with the first of the laws of war, and have continued ever since. Within the Internet design process, jurisdiction was first encountered at the beginning of the 1970s when the first network connections were lit and the computer scientists and electrical engineers involved ran into tariffs (Hauben, 2004). An article published in *First Monday* 20 years ago by Post and Johnson (1996) is still cited today not only because it was a relatively early and accessible analysis of the issue, but also because it explicates the problems so clearly.

Since then attention by legal thinkers has been sustained (see, e.g., Zittrain, 2005). Some explore how jurisdictional problems might be resolved through the lens of a specific legal issue (see, e.g., Matwyshyn, 2004, who focuses on data privacy). Much of the discussion, as in the Tallinn manuals, struggles with the question of whether or not existing laws of jurisdiction within specific countries apply (Spencer, 2006). New law has also been proposed, with calls for a new international instrument specific to the problem as an example (Franklin & Morris, 2002). From the start, there have been those who saw how the Internet could be used to play with jurisdiction to maximize corporate profit via what Froomkin (1997) calls "regulatory arbitrage," a powerful motive for resistance to legal harmonization.

Regime theory, which emphasizes the processes through which diverse stakeholders' expectations come to converge through the development of implicit or explicit principles, norms, rules, and decision-making procedures, is often applied to the evolution of decision-making prior to the achievement of consensually agreed upon law as it evolves in new issue areas or those undergoing radical change (Braman, 2004). Lehmann, *et al.* (2015) and Nye (2014) offer examples of the use of regime theory in the area of cybersecurity, but Mačák is critical, describing reliance on norms as "vacuous" (2016, p. 131) and further evidence of crisis for the Westphalian state. A third view is available from the perspective of complex adaptive systems theory: acknowledging the recency of official recognition of cyberspace as a military domain -- for NATO in the 1990s (Woudsma, 2013), and for the US a decade or so later in terms of official doctrine (U.S. Department of Defense, 2011, 2015) -- Kessler and Warner (2013) describe what the authors of the *Tallinn Manual* are doing as uncertainty absorption.

Awareness of challenges to the Westphalian state due not only but in significant part to technological change is also not new with 21st century cyber concerns. In the 1980s, Anthony Oettinger and his colleagues at Harvard focused attention on network-derived national security issues (see, e.g., Oettinger, Berman & Read, 1980) and concerns about new vulnerabilities of states as a result of digitization were being raised in reports to European governments such as the Nora/Minc report to the government of France and the Tengelin report to the government of Sweden of the late 1970s (Braman, 1991). (System theories distinguish between sensitivity [a perturbation of a system to which the system must respond] and vulnerability [impacts on a system so severe that they could destroy it],

and it is in this sense the term "vulnerabilities" was used.) Turning points such as the 1988 disruption of Internet traffic by the Morris Worm and the 2010 use of Stuxnet to intervene in the operationalizability of the kinetic weapons of another country (Knoepfel, 2014), combined with the general trends towards ever-greater globalization of the Internet and its penetration throughout the social and, now, material worlds (think "Internet of Things"), cybersecurity and cyberwarfare concerns have enormously increased and brought such questions to a head.

Changes in the use of information policy tools for purposes of thinking about war and peace over just the last two decades, however, make vivid how significant a change it is to be thinking in terms of a Westphalian moment in the course of what are, in essence, arms control discussions for the cyber domain. By the mid-1980s, it was estimated that at least 85% of arms control treaties involving kinetic -- physical -- weapons was devoted to what would be considered information policy provisions by the definition used here (Tsipis, et al., 1986). Analysis of these provisions in the 24 arms control treaties and treaty proposals from the first to be signed in 1925 through 1989 (not long before the collapse of the former Soviet Union) found 25 distinct types of information policy tools in use, falling into half a dozen broad categories (Braman, 1991). These tools, which were known as "confidence- and security-building measures," or CSBMs, were diverse, including the articulation of abstract principles, mandated reportage, observation, documentation of manufacturing outputs, administrative techniques, and mass communication. A number of additional suggestions for the use of informational tools to prevent war were discussed in the literature of the period.

Proposals as well as treaties were included in that analysis because the question was what types of information policy provisions were believed to be useful for the national security context, whether or not agreement on them was ultimately incorporated into international law. In a related manner, the *Tallinn Manual* includes detailed discussion not only of those points on which the group of experts on international law agreed, but also on those points where there was disagreement, with valuable articulation of the arguments put forward to support each position.

A comparison of findings from the study of information policy tools in arms control treaties and treaty proposals (Braman, 1991) and of nature of the policy tools under consideration in the first edition of the Tallinn Manual (Braman, 2014a) makes the rise of informational power vivid and brings striking changes across the 25 years to light (Braman, 2017). During the 20th century information was used to try to prevent war and the focus was on mandated releases of information -- requirements placed on information senders. The survival of the state itself as the dominant geopolitical form was not questioned. In the 21st, information is used as a weapon of war and the focus is on what information should be acquired -- what is required of information receivers. Whether or not the state itself will endure as the dominant geopolitical form is consistently questioned and where that question arises arguments get particularly complex and convoluted. During the 20th century the issue was what the state should or could know; in the 21st, in the Tallinn manuals, a new information policy principle has implicitly been introduced: the right of a state *not* to know" (*Ibid*.). The movement from thinking in terms of state horizons to emanations was another manifestation of the changes that had taken place in the nature of the informational state and the ways in which it conducts itself within the Westphalian system.

Emanations of the State

In the mid-1990s, telecommunications policy – laws and regulations for the electronic communication networks that today include the Internet -- was used as tools of power for the informational state, across governments, at its edges, or "horizons."[6] Two decades ago we could think in terms of horizons because it seemed, at the time, that we could still locate where the borders were. Today, that has given way to a term that is less concrete and even more vague; in *Tallinn Manual 2.0*, the word used to refer to the limits of the state is "emanations." This interesting concept has a long history in Greek thought and semantically derives from the Latin. In English, according to the *Oxford English Dictionary*, dominant early usages appeared in medieval philosophy, typically referring to things that flow from, have come into existence because of, God, often in immaterial and impalpable form.

This reference to non-human actors and agency is not new to how people have been thinking about cyberspace. The computer scientists and electrical engineers who designed what we now call the Internet refer to the non-human users who were of as much, if not greater, concern as "daemons" -- another term with a Greek and medieval history used when discussing sources of agency that are neither human nor divine (Braman, 2011; see, e.g., McLaughlin III [RFC 1179], 1990). (Nor is the reliance on a word that comes from ancient Greek; the word "protocol," so fundamental to Internet design and architecture, comes from the Greek *protocollon*, meaning a piece of paper attached to a text describing its contents, a technical standard for the time that, like today's Internet protocols, facilitated the accessing, processing, and distribution of information.)

Use of the concept of emanations began in "modern" discussions of state power several decades ago, among both political scientists and legal thinkers. The frequency of its use in the second edition of the Tallinn Manual's analysis of the application of existing international laws of war to cyberspace is revelatory of the ways in which our conceptualizations of the state – and our experiences of states – are changing. We look here at how the concept has been used in political and legal thought in general and as within discussions about cybersecurity, the types of relationships among those who exercise power and the subjects of power that involve emanations, features of emanations in the cyber domain, and the three types of emanations of the state that receive attention in *Tallinn Manual 2.0*, those of agents, agency, and data. The rising reliance on this concept in discussions of matters such as cybersecurity is a marker of the transition to an informational state.

---

[6] A 1995 special issue of the *Journal of Communication* on "Horizons of the State: Information, Policy, and Power" included, in addition to a theoretical framework (Braman, 1995), research on just how those tools were being used across the domestic/international boundary by a number of governments: Mexico (Barrera, 1995), India (McDowell, 1995; Mody, 1995), Ireland (Bell, 1995), the Philippines (Sussman, 1995), Poland (Jakubowicz, 1995), and the United Kingdom (Sparks, 1995).

Political and Legal Emanations

The concept of emanations came into use in both political science and the law in the course of discussions about the nature of the state. It has a long history; Hobson (1979) reminds us that James Madison when working through the constitutional design problem of federalism in the United States, with its relationships between state and federal law; the European Union (EU) has found it useful for the same reasons as it works through subsidiarity. Scholarly uses begin with Zander, in 1959, who treated court decisions as emanations of the state in his discussion of the general rejection by US courts of decisions made by courts in other countries. Nettl (1968) emphasized that emanations of the state include not only central administration and the law, but also *ad hoc* advisors such as individuals and representatives of industry and labor. Neave (1998) relied upon emanations to explain the role of evaluation as a fundamentally important type of exercise of power by what had become, in his view, the "evaluative state."

Legal scholars of the mid-20th century, too, began to think about the legal system as an emanation of the state. In 1965, Supreme Court Justice William O. Douglas did so in his moving and highly influential opinion for the Court in *Griswold v Connecticut* (1965), where he explicated a theory of rights that go beyond and emanate from those specified in the Bill of Rights. Penumbral rights, importantly, include the right to receive information as an emanation of the First Amendment, and privacy as an emanation of both the First and Fourth Amendments. In the work of authors such as DeBurca (2015), who studies US Supreme Court resistance to law emanating from other states, or Buchanan (1997), who looks at the impact of immunity on state action, the political nature of the legal discussions – and the legal nature of the political discussions – are clearly evident.

The term is still in use in 21st century discussions of the nature of the state. In the realm of security, the concept is relied upon when distinguishing classes of subjects for the purpose of determining whether their actions justifiably warrant a military response from a state under international laws of war that often (though not consistently – see below) insist that the actions or intentions of non-state actors do not. Thinking in terms of emanations makes it possible to treat what are otherwise, and commonly, thought of as private sector entities, issues, and information as if they are closely enough associated with the state to be treated as public, instead. The first and primary uses of the concept in political analyses, though, treat the elements of states as emanations, as in the Chatham House (2006) reference to embassies and armed forces as things that states have the right to protect outside of their territorial jurisdiction.

Embassies and military forces are, of course, easily seen and identifiable, known, stable in form, and classically Westphalian. Recently, though, the concept of emanations is also being used when thinking about entities that are putting pressure on Westphalian states and system. This can be seen in analyses of the growth of regional states (Yeo, 2002) as well as of non-state governance including, importantly, that by corporations (Graczyk, 2015; Michaels, 2010, Ramraj, 2013). It has pragmatic uses, as when the EU thinks in terms of emanations to describe transfers of power, whether from the EU to states or in the other direction. The notion can also be abstractly provocative, as in Zumbansen's (2008) discussion of the reflexive ways in which government and governance are moving away from the state. For Henrikson (1981), the “aura” generated by soft power via persuasive campaigns comprises the emanations of the state.

Significantly for purposes of this paper, political scientists have very recently begun to use the concept of emanations to refer to sources of agency without any agent at all. Andersson (2016) is concerned about danger emanating from "blank spaces, sources of instability about which we have little information. Dey (2016) writes about the impact of the emanations of free-floating "conflictual energy" (p. 564). For Lierse and Seelkopf (2016), emanations from global capital markets – defined no more specifically than that -- influence national policy-making.

All of the kinds of relationships described in the political and legal literatures as emanations can be found with cyber operations, from the earliest conceptualizations involving obvious, traditional, and tightly-bounded tools of state operations such as the legal system and policing units to current meanings as applied to not always visible, non-traditional, loosely or unbounded entities, actions, or information at levels of analysis from the most specific to the most vague and ambiguous. It is important to highlight that the concept has been used to refer to tools of power in all of its forms, from the most material elements of instrumental power such as the weapons and personnel of armed forces, through the fundaments of structural power such as the law, to the persuasive campaigns of symbolic, or soft, power. In the cyber domain, informational tools of power are of particular importance.

Emanations are key to thinking about cybersecurity because the notion provides a means of justifying military response to a threat or attack under existing laws of war because it is defined as involving the state. Both Tallinn manuals open by asserting that although cyberspace itself is sovereign free, governments can claim sovereignty over cyber infrastructure located within their territories and activities associated with that infrastructure.

Features of Cyber Emanations

Three features of cyber emanations, each critical to how states relate to each other, come up in the foundational sections of *Tallinn Manual 2.0*: capacity, the requirements of due diligence, and a right to resist the emanations of others. It is likely that additional features will be discussed in later portions of the work and analyses that follow by these or other authors. The question of what happens to emanations when states act in coordination, whether ephemerally or in projects of some duration, needs attention. As do emanations of non-state actors; antitrust (competition) law developed in response to the effects of some types of these.

Capacity. The term emanations is used to refer to the ability of one entity to affect or engage with another in the most abstract ways. According to Rule 2 in *Tallinn Manual 2.0*, states are obliged to exercise domestic due diligence internally in order to prevent harmful cyber activities that emanate from its territory (II, Rule 2, p. 16). Rule 3 on external sovereignty similarly includes the state's ability to conduct cyber activities in the international arena.

Due diligence. States should be careful about the effects of their own cyber emanations on other states, according to Rule 6 of *2.0*:

> A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber

operations that affect the rights of, and produce serious adverse consequences for, other States (II, Rule 6, p. 30).

Right to resist. The right of states to resist the emanations of others is also asserted in version *2.0*. In Rule 9: "A State may exercise jurisdiction over . . . . (c) cyber activities having a substantial effect in its territory" (II, Rule 9, p. 55). Rule 10 protects the right of states to protect themselves against cyber activities "conducted by foreign nationals against its nationals" (II, Rule 10, p. 60). The manual goes further -- if necessary in order to protect itself, states have the right to disconnect from the Internet altogether as long as they comply with international human rights law (II, Rule 1, p. 13).

Types of Cyber Emanations

Foundational sections of *Tallinn Manual 2.0* discuss three types of emanations of the state important to cyber operations. There are emanations of agency (exercises of informational power); of agents (entities capable of exercising power and being the subject of exercises of power); and of data (informational extensions of the state that have varying relationships with power).

Agency. Emanations of agency involve activities dependent upon and taking place within the network infrastructure (see, e.g., II, Rule 1, p. 11; II, Rule 2, p. 13). In the cyber domain, of course, these are all informational tools of power. Somewhat astonishingly because of its implications for the treatment of non-state actors under existing international law, according to the authors of *Tallinn Manual 2.0*, emanations of the state in the form of agency can involve infrastructure and activities that are either public or private in nature and be exercised via either domestic or foreign infrastructure devoted to either public or private purposes (II, Rule 2, p. 13). Despite this agreement on a very broad notion of state agency, though, the experts did not agree on when the exercise of agency by one state against, or within, or affecting another constituted a violation of sovereignty for the purposes of laws of war (II, Rule 4, pp. 20ff).

Three issues were raised. The first was the degree of infringement upon the target state's territorial integrity. Much of the thinking revolved around criteria for determining when there is damage and distinguishing among levels of damage. As an indication of the extent of disagreement on these points, some experts believed that even causing physical damage, injury, and/or loss of functionality (whether or not by remote means) did not necessarily violate sovereignty.

Second, there were disagreements over the degree of interference with or usurpation of inherently governmental functions. While the general principle received consensual support, disagreements here began again with the problem of determining just when the threshold of impact had been reached. All agreed that that had taken place when a cyber operation forced the repair or replacement of physical components, but not whether reinstallation of operating systems, or cyber operations that result in neither physical damage nor loss of functionality, qualified. Those who believed that such actions could violate sovereignty would treat operations that cause infrastructure or programs to operate differently, altering or deleting data, employing malware, installing backdoors, and causing temporary but significant loss of functionality (as with a major DDoS operation) as attacks under international laws of war.

The most surprising of the problems raised for this group of experts by emanations of agency via informational power was the third, determining what "inherently governmental functions" are. Experts involved in the second edition had no problem reaching a consensus that interference with or usurpation of government functions violated sovereignty and including within that category such matters as changing or deleting data in a manner that interferes with the delivery of social services,[7] the conduct of elections, collection of taxes, effective conduct of diplomacy, and defense activities. But while they agreed that such functions must be "inherently governmental," they also agreed that it was irrelevant for such purposes whether that function is actually performed by the public or by the private sector and they acknowledged that there were many activities for which determination of whether or not the function is governmental at all would be difficult. In combination with ambiguity regarding treatment of non-state actors and recognition that governments can be engaged in commercial activity in markets, the question of what it is that is treated as governmental and what is not in these analyses becomes profound.

Agents. The second type of emanations of the state discussed in *Tallinn Manual 2.0* are those of agents rather than agency. The work vacillates on the questions of whether or not non-state actors are to be considered agents of the state and whether or not attacks upon private sector actors and entities are attacks upon the state. The problem occurs the other way around, too; importantly and again strikingly, entities of the state are *not* treated as governmental when they are involved in commercial markets.

The issue is confounded by the roles that representations and fictive identities play. Those concerned about the relative power of the corporate ability to influence elections in the United States after the US Supreme Court decision in *Citizens United* (2010) released all limits on spending and removed requirements that funders of messages be identified have launched a public debate over whether or not corporations should be legally treated as persons at all. The issues, of course, involve more than elections; the practice of treating corporations as fictive persons equivalent to "natural," or biological persons for many legal purposes goes back to around 1300 because it is only in this way that a state can contract with or give permission to a corporation to do things that accomplish state goals, and only in this way can a governing entity regulate a corporation to ensure that its contributions to society at large and to the government are positive rather than negative. In the cyber domain, from a military perspective, the question is reversed: When should a single biological person or small group of biological persons be legally considered equivalent to the state? A number of issues are raised in the Tallinn manuals about thresholds for answering that question, including the size of a group, its level of deliberate coordination and, importantly, its effects.

Cyberspace is of course not the only realm in which non-state-centric military issues are raised (see, e.g., Radin, 2013), but the role of such actors in the cyber domain is significant, if not dominant. According to Buchan (2016), harmful transborder cyber operations by non-state actors actually exceed those of states.

---

[7] In the United States, there is a similar distinction between the legal treatment of symbolic political speech that is protected and that which is not based on whether or not the speech interferes with institutional processes. Thus under the First Amendment it is legal to burn a flag, but not to burn a draft card because the latter places an administrative burden on the government and the former is communicative only.

Data. The third type of emanations of the state discussed in *Tallinn Manual 2.0* are those of data. For these legal experts, data are included in the social layer of cyberspace. Monitoring data about such things as stock market transactions or critical infrastructure (e.g., energy) activities is considered a cyber operation of concern because it could result in, in the first instance, severe economic loss if doing so results in a loss of confidence in the stock market (II, Rule 4, p. 25) or, in the second example, use of the information acquired to disrupt or destroy the government or society. Experts disagreed, though, over the duration, uniformity, frequency, and/or significance of such monitoring required to justify treating these activities as violations of sovereignty.

Authors of the first edition also disagreed over whether it is possible or normatively preferable for states to have sovereign immunity for their data in the cyber environment (I, Rule 4, p. 25) -- and whether jurisdiction over cyber activities and data created through those activities must necessarily be treated in the same way (I, Rule 10, p. 63). Even those who would not grant states complete jurisdiction over government data and that of its citizens held within the territory of other states acknowledge the right of states to exercise prescriptive jurisdiction over the data even when they are not able to exercise normative jurisdiction over it. Either way, the fact that the state in which data are held has jurisdiction over data within its territory is not problematic as it is often the case in the cyber domain that two or more states simultaneously have jurisdiction.

Data, of course, are not always in intangible forms. For most of human history they have had material presence in letters, books, reference works, and archives. This affects considerations of data emanations of the state because of the history of treaty-based protections for tangible diplomatic communications and archives. Experts disagreed on whether existing treaty provisions in this area should be extended to the cyber realm.

A rhetorical advantage of the concept of emanations is that it offers an opportunity to be ambiguous while maintaining a face of specificity. That use within arguments made in *Tallinn Manual 2.0* is complemented by the practice across arguments of having it both ways, coming to one conclusion on a matter as it arises in one context, and a different conclusion when considering other situations.

Having it Both Ways

Although the group of experts involved in writing *Tallinn Manual 2.0* retreated from accepting non-state actors as sovereign entities for the purposes of implementing international laws of war, it did treat them as sovereign in significant other areas by, essentially, hedging bets. Reading across arguments presented in response to different legal problems yields a sense that the actual position of this group is often "maybe yes, maybe no" or, better, "sometimes yes, sometimes no." In a relatively simple example, difficulties presented by the multi-jurisdictional features of cloud computing are acknowledged as problematic when the experts address limits to a state's ability to identify the source of attacks, but are not acknowledged as pertinent at all when the experts address what states can legally do when a proportionate response is justified (cf., Coeckelbergh, 2011). The examples discussed in more detail here are among the most important of such areas: the treatment of non-state actors, intention, causality, the kinds of knowledge of uses of its infrastructure a state might reasonably be expected to have, something we can call "witting

requirements," and how the differences in technical capacity affect Westphalian juridical equality of states within the cyber domain.

Non-State Actors

Dramatically, authors of the first edition of the *Tallinn Manual* did not agree on whether conflicts with non-state actors could be considered under international laws of war. A minority argued that international acceptance of a War on Terror after 9/11 constituted agreement to analyze cyber operations by non-state actors from the perspective of their impact on sovereignty (I, Rule 1, p. 17). This was a big deal because these treaty-based laws -- to which states had agreed and for which they were developed -- had historically been applied only to tensions between geopolitically recognized states. Other laws, such as those of crime, were applied to harm caused by non-state actors. There was disagreement on how far to take that, but the point was returned to several times in the 2013 *Tallinn Manual*.

By the second edition that viewpoint was no longer being represented explicitly. Instead, the text approaches the question from several directions, alternately treating non-state actor threats as matters to be taken very seriously from a sovereignty perspective and rejecting granting that status. The question came to be understood as not simply binary. Rather, size of a group matters. In the first edition operational capacity was also considered; that may come up in sections of the second edition not analyzed here.

Do non-state actors matter under laws of war? In an important example of what seems like an effort to have it both ways, the second edition of the Tallinn Manual both withdrew from the first edition's "yes" to this question and, simultaneously, expanded on the ways in which the first edition's "yes" should be applied. *Manual 2.0* insists that the external sovereignty rule does *not* apply to non-state actors unless their actions are attributable to a state (II, Rule 4, p. 18), based on the argument that because only states have obligations regarding the sovereignty of other states, only states can breach those obligations. Examples of actions that do not , therefore, violate state sovereignty include malicious hacking by a corporation into a state in response to having been hacked by a cyber operation of that state, and the conduct of cyber operations by a terrorist group against a state. That is, neither terrorist groups nor corporations, as non-state actors, can either act defensively or engage in a proportional response in ways existing international laws of war would treat as legal were the same kinds of activities undertaken or responded to by states. Instead, the group of experts agreed, such matters should be treated under domestic criminal law (*Ibid*.).

However, the second edition of the Manual takes the opposite position that non-state actors *can* trigger due diligence requirements (II, Rule 6, p. 35) when their actions result in serious adverse consequences and affect a right of the target state. To support this position, the experts use the analog of international environmental law as an historical precedent for due diligence regarding damage that can be caused by non-state actors. The test for determining whether or not due diligence would be triggered would be whether or not there would be an obligation were the activities undertaken by a state rather than non-state actor. Importantly for current concerns about releases by WikiLeaks, Edward Snowden, and the Shadow Brokers, an example discussed in the manual was private sector online publication of a country's highly classified documents in another state, an action that does

not trigger due diligence requirements because no international law of the target state is affected even though there could be serious adverse consequences for the state whose documents have been released. At another point the experts assert that the due diligence principle doesn't depend on whether either the actor or the targeted cyber infrastructure is private or public (II, Rule 6, p. 40). Further confusing the matter, governmental institutions that operate as market participants vis-a-vis the Internet can't claim sovereign immunity, although governmental non-commercial operations are given this immunity regardless of location (II, Rule 5, p. 27).

Size of non-state actor. How organized must a group be -- if at all -- in order to be considered capable of mounting an armed attack? (I, Rule 13, p. 58) Published in the same year that Edward Snowden released massive amounts of information from the United States National Security Agency (NSA), and a number of years after Jon Postel demonstrated his ability to shut down the Internet altogether through his individual actions, in the first edition of the *Tallinn Manual* some experts took the position that a single individual acting on his or her own -- as distinct from "cyber volunteers" operating under the direction of a state -- could be legally considered capable of mounting an armed attack (I, Rule 13, pp. 58-59). Others did not agree, adhering to more traditional expectations regarding what it takes to have an impact on institutions and social processes. It is worth highlighting that the cyber-volunteers referred to in 2013 – private individuals acting at the behest of and in service to the state – do not receive any attention in the second edition in 2017.

Intention

Two significant issues involving intention arise in the Tallinn manuals. There is the question of whether the type of motivation involved when considering a responsive cyber operation matters is pertinent to the legal justifiability of self-defense. Several problems are raised by the role of actual intention to harm or attack. The question of how states might know whether or not intention has been manifested are touched upon in a following sub-section on witting requirements.

Motivation as indication of intention. There was disagreement in the first edition over whether or not motivation for an attack needed to be taken into account when determining whether or not a military response is justified. Those who argued for doing so believed that attacks motivated by purely private interests did not justify self-defense, while others took the position that motives are irrelevant if effects are experienced as attack (I, Rule 13, p. 59). The second edition, though, comes down on the side of fully accepting commercial and financial motivations for defensive operations under international laws of war. Specific economic interests such as ensuring stock market stability, preventing financial fraud, and protecting intellectual property rights are discussed. With the justification that doing so is defensive, states can also issue prescriptive regulation on entities abroad for the same reasons.

However, this position is not held consistently. Government entities involved in commercial activities may be justified in acting based on commercial and economic concerns, but are not protected by sovereign immunity from being challenged in foreign courts.

Intention vs. effects. There was a running debate in the first edition of the *Tallinn Manual* over whether the key criterion determining whether or not an action justified a defensive military response should be intention (did the agent intend to attack or harm the targeted state?) or effects (did the agent harm the targeted state whether or not there had been intention to issue an attack?) (I, Rule 13, pp. 54-61). The discussion of this problem worked through diverse situations, including the "classic" scenario of an attack on a stock market that causes a crash. Some experts thought this was "merely" economic, while others would treat that as an armed attack because the consequences would be catastrophic. By the second edition, experts had moved to full support for an "effects doctrine" that makes it much easier for a state to claim a nexus with a particular cyber event -- if there is any substantial connection between a particular cyber operation and effects within a territory of a state, the affected state can act in self-defense, whether or not there had been any intention to harm.

This is a significant development for it justifies military responses by states that may not have been targeted but that, nonetheless, experienced effects of an operation either because the consequences of an operation were global in nature (as an attack on a stock market might be) or as collateral damage. Thus a cyber operation that was intended to breach the sovereignty of another state but fails, for there has been no breach (II, Rule 4, p. 24), would not be considered an attack. If, however, there is no intention to violate sovereignty but a violation does occur, there *is* a breach if sufficient harm is caused. This applies, as well, to effects that may have simply bled over to one or more third party states as a result of attacks on a targeted state. In sum, "intent is not a constitutive element of a breach of sovereignty" (II, Rule 4, p. 25).

Here, too, though, the experts fail to carry through on the position consistently. While the effects doctrine is relied upon to justify *responses* to operations, when it comes to due diligence responsibilities to try to *prevent* operations it is abandoned in favor of intention. That is, whether or not states have complied with their due diligence responsibility to try to prevent their territory from being used either as the base of an attack on another state or as a "transit" state through which networked information passes on the way to an attack is determined by whether or not they tried, even if unsuccessfully. Intention *is not required* to justify military action, but *is all that is required* to comply with international law regarding prevention of harm.

This is a particularly interesting issue for the United States as one of the significant changes to US law following 9/11 was the USA PATRIOT Act of 2001 determination that one could be considered a terrorist if an accumulation of actions generated $5,000 or more in costs to repair damage to a network, computer, database, or website, whether or not any harm was intended. Going even further, the US government argued during the court martial of Chelsea Manning for release of classified information to WikiLeaks that intention should be *determined* by effect. The claim was that if the WikiLeaks information was used by particular individuals or groups to achieve their goals, it must have been Manning's intention that the information released would be used that way (Braman, 2014c). Since versions of an effects doctrine are beginning to make their way through other areas of the law, this aspect of international law for cybersecurity and cyberwarfare is worth attending to for those generally interested in changes in the history, economics, and sociology of the law as well.

Causality

The distinction between power in its actual and potential phases came up several times in the first edition of the *Tallinn Manual*. Its discussion of state responsibilities towards infrastructure distinguished among "merely prospective" cyber operations, operations that have already been planned or are underway, and operations that could happen but are not yet happening (I, Rule 5, p. 27). There was no consensus on whether or not states have a positive responsibility to try to prevent prospective attacks, with some experts questioning whether or not doing so was possible given the characteristics of cyberspace. The group of experts explored questions such as how to incorporate evaluations of state capability into decision-making regarding the appropriate level of responsibilities (I, Rule 12, p. 53).

These distinctions mark steps in a chain of causality discussed in the second edition (see, e.g., II, Rule 7, p. 43). The majority of experts thought responsibility began when material steps to execute an operation are being carried out and there is a reasonable expectation that those steps would be brought to fruition, but others argued that the obligation only begins once an operation is underway. Treatment of potentially disruptive or dangerous political speech in the United States offers a useful analogue for how to think about this distinction. The test used to determine when speech deemed dangerous to the country can be stopped in the United States, given the First Amendment, is often referred to as the "clear and present danger test." The criteria to be evaluated include whether or not the content is incitement, whether incitement is intended, whether the further actions needed to achieve the goal are likely to be carried out, and imminence, how soon those actions might be taken. "Incitement" is a way of referring to the role of discourse in stimulating behavioral action, whether in one individual, a particular mob, or an entire social movement. A multi-methods approach to studying social networks, flows of content, and diverse types of impact would allow us to evaluate cyber operations in the way.

Distinctions among the steps by which effective causation comes about were also important when the group of experts declared that due diligence does not require states to take preventive measures (II, Rule 7, p. 44). In an interesting twist, it is argued that since knowledge is a requirement under Rule 7 regarding due diligence, obligations regarding hypothetical future harmful actions cannot be required (II, Rule 7, p. 45). The text acknowledges another view, not held by any of the experts involved, that states must take reasonable measures to prevent harmful cyber operations from emanating from their territory. Those who hold this perspective point out in particular that there are circumstances in which history had provided so much experience that even considerations of a future action would not be speculative. Instead, the point is implicitly made, it would be genuinely predictive.

Witting Requirements

The first edition of the *Tallinn Manual* devoted a fair amount of space to discussing the nature of the knowledge required in order to trigger due diligence responsibilities on the part of a source or transit state. We might call these "witting requirements." Because fully acting to prevent any malicious uses of a state's cyber infrastructure would simultaneously cripple the state itself, it is not surprising that there is reluctance to go too

far in terms of requiring preventive action. So much so, in fact, that the positions in the 2013 publication seem to introduce a new information policy principle, the right *not* to know (Braman, 2014a). In the second edition, this analysis continues with an effort to more fully articulate just what the "actual knowledge" required to trigger due diligence is (II, Rule 6, p. 40).

What they come up with begins relatively simply. By "actual knowledge," *Tallinn Manual 2.0* means information coming from either a state entity such as an intelligence agency of from another credible source has detected a cyber operation emanating from its territory. The questions to which this leads, though, immediately proliferate and become more complex. From the perspective of information policy, credibility and trust are among the issues of importance that leap out in this text. Which information sources are considered credible enough for the state to act upon, knowing that in doing so harms of various kinds will also be caused? Examples used in the manual are state intelligence agencies, but the language of the rules and their interpretation appear to leave open the question of whether these must be limited to public sector entities. What trends might be underway that challenge the credibility of those sources? How strong is the trust between the state and the information sources, whether public or private, and what factors might effectively weaken that trust?

Additional questions came to mind for the group of experts involved in writing *Tallinn Manual 2.0*. They thought about situations in which there is no credible information source. They noted that an uncooperative territorial state may know its territory is being used but disregard that knowledge, presenting plausible deniability even though the legal obligation remains in place. And they wound up allowing states to rest upon only that knowledge that would have become evident during normal usage of the networks involved (II, Rule 6, p. 41).

The "normal course of events," of course, differs widely across the wildly variant levels of technological capacity of states. There are other factors that affect whether a state "should" have known that its territory was being used to cause cyber harms to other states, as well, yielding a spectrum of positions along a "should have known" scale. The "should have known" standard is higher when it is public rather than private cyber infrastructure that is being exploited, when the malware and vulnerabilities used are publicly known, and when the attacks are cyber operations of types that are always detected, such as DDoS attacks that are always evident because of the higher-than-normal bandwidth usage. On the other hand, when cyber operation involve complex, previously unknown malware, the "should have known" standard is lower.

This standard is important because it protects states from being in breach of due diligence responsibilities under conditions in which there was no reason to expect them to have known. (Similarly, the second edition sets a standard for evaluating the feasibility of efforts to prevent the harm from taking place; if it was unreasonable for a state to terminate the harmful activity because of the costs to itself, there has been no breach of due diligence responsibilities.) However, use of these standards is also a policy tool that makes it possible to have things both ways -- there *is* a due diligence commitment, but there are plenty of ways that states can deny any responsibilities flowing from that commitment.

Equivalence among States

One of the basics of the Westphalian system is that all states are treated the same. They are "juridically" equal, and the running assumption is that international law applies to all states in the same way. In the Tallinn manuals, though, a great deal is made of establishing very different expectations for state responsibilities vis-a-vis other states depending on their level of technological sophistication and their position(s) relative to the global information infrastructure – what political scientists refer to as capacity. While it is easy to recognize that there are such differences and to think of them in the abstract in a very general way, it is often difficult to accurately evaluate the capacity when it comes to informational power of the kinds at the heart of issues raised by cyber operations.

This is true for reasons at two levels of analysis. At the institutional (governmental) level, evaluations of the validity of claims to power in its potential and virtual phases are difficult, for turning power in those phases into actualities involves capacity -- the financial resources, knowledge of how to use those resources, political will, sovereign integrity, stability of administrative control, loyalty and skill among officials, infrastructure, and industrial base. When it comes to the cyber domain, though, the Tallinn manuals acknowledge that single individuals and small, perhaps ephemeral and shifting, groups can also cause significant damage. This makes estimating state capacity even more difficult, as does the ability to spoof identity. Indeed, neither the conceptual nor the methodological tools are in place for evaluating the capacity of an entity's tools of informational power, which do not offer the visual or other type of evidence of kinetic weapons or the documentary evidence of uses of tools of power in their instrumental and symbolic forms. As the first edition noted, "[C]yber capability is not as dependent on a State's size, population, or economic and military capacity as is the capacity to use conventional force" (I, Rule 12, p. 53).

Such unequal expectations of states is one of the assumptions *cum* arguments used to support the position in *2.0* that having constructive knowledge does not in itself trigger an obligation to take preventive measures (II, Rule 6, pp. 41-42). Rather, a state "must act as a reasonable State would in same or similar circumstances" (II, Rule 6, p. 42), with the emphasis when evaluating similarity on how a state is situated vis-a-vis the network and how it is equipped. What matters is whether or not a state like in kind technologically "in the normal course of events would have discovered the use of the cyberinfrastructure in question" (*Ibid*.)

The level of technological sophistication also came into consideration when thinking through what feasible preventive measures might be proportionate to the risk of potential harm (II, Rule 7, p. 45). Here the experts recommend taking into account pertinent scientific and technological developments as well as the unique circumstances of each case. Preventive efforts that can be taken might involve setting up CERTs (Community Emergency Response Teams), putting in place information security policies, and adopting domestic legislation that would require companies to report cyber incidents in order to be able to generate accurate threat assessments.

The "feasibility" criterion for complying with due diligence is always "contextual." The first edition was not confident about this matter. After noting the relationship between cyber capability and size, it emphasizes how difficult it is for a state to determine whether or not another state actually has the ability and the resources to follow through on cyber

threats. Because of this inability to know, the second group of experts treated the problem as relatively unimportant among cyber threats (II, Rule 12, p. 53).

As further elaborated upon in the second edition, factors that matter when capability and likelihood of follow-through *are* being evaluated include the technical capacity of the state, its intellectual and financial resources, the state's institutional capacity for carrying out preventive or mitigating measures, and the extent of control a state actually has over cyber infrastructure on its territory (both because of private ownership and because of the difference between ownership and control). It also depends upon the type of attack involved; *Tallinn Manual 2.0* highlights the fact that almost every state has the capacity to block IP addresses, but not all have the capacity to deal with highly complex and dynamic cyber operations.

Although the groups of experts involved in writing the Tallinn manuals acknowledge that individuals and small groups can be capable of great harm to states, there is also a running assumption that differences among states in cyber capacity will run along historical lines in traditional "developed vs. developing" terms. This generates significant differences in responsibilities as articulated for developed and developing societies under international law as applied to cyber operations. One would think that would invite the use of the cyber infrastructure of "developing" societies for attacks.

Agents as emanations of a state appear here again. If a state doesn't have the capacity to defend or proportionately respond itself, the authors of the second edition of the *Tallinn Manual* recommend that it might hire a private firm to handle the problem. Given the importance of the distinction between state and non-state actors running throughout these manuals, it is worth noting that the possibility of turning to a more technologically sophisticated public sector entity, another state, for this assistance is *not* mentioned.

Finally but importantly, due diligence responsibilities may best be met not by intervening, but by monitoring what is going on (II, Rule 7, p. 47). Possible conflicts between the responsibilities of a state exercising due diligence and those of an administrator whose focal concern is the network, instead, is a classic example of the kinds of tensions that can arise between what we can call "network citizenship" (primary allegiance to the network) vs. geopolitical citizenship (primary allegiance to one's jurisdictional identity). This potential conflict became evident in discussions among Internet designers within the technical document series (the Requests for Comments, or RFCs) that has provided both the medium for and record of technical decision-making for network protocols (Braman 2014b).

Conclusions

A border we know, a horizon we can grasp, but an emanation we can only sense.

The intricate discussions that erupt regularly in *Tallinn Manual 2.0* about who does what (state or non-state) to whom (non-state or state) in which sequence and with what consequence read very much like medieval philosophers working through the number and rotations of spheres within spheres. The reader yearns for Occam's Razor. One hears Thomas Kuhn (1962) intoning in the wings on the nature of arguments presented during fundamental changes in paradigm, how we understand the world. As Kuhn tells us, the very level of complexity of the reasoning in the Tallinn manuals is a sign that the phenomena, events, and processes they talk about are *not* understood.

The use of digital technologies has transformed how we relate to ourselves and to each other in small and large groups, near and far. It has made possible entirely new forms of organization, altered the relationship of the species to time and space, and brought us new ways to both work and play. It should not be surprising that just as dyads, communities, corporations, and polities have undergone change and are continuing to mutate as a result of digital affordances, so is the nature of what has been the global geopolitical system. The internal contradictions, significant areas of disagreement, reliance on ever-more vague terms to refer to the kinds of relationships and actions to which the law is being applied, and efforts to have it both ways at once on some of the most difficult and fundamental issues are all signs that the Westphalian system of states itself -- in addition to the states of which it is comprised -- is experiencing profound challenges in the cyber domain.

For the informational state, it is the cyber domain that increasingly and comprehensively drives all others. As the analyses of the Tallinn manuals make clear, efforts by the informational state to craft and operationalize an identity and exercise power within the Westphalian system are disruptive to the system itself. In the long run, it is this author's guess that it will be the informational state that survives and thrives and the Westphalian system that will give way. Another stable equilibrious global political formation may evolve, but that is only one among the possible outcomes of turbulence and chaos in complex adaptive systems.

Meanwhile, since within the terms of existing international laws of war, the more they talk about the cybersecurity and cyberwarfare issues so familiar in kind to Westphalian states, the worse it gets. It may be, then, that the job of legal scholars, researchers, scholars, citizens, and thinkers of all kinds is to identify other languages and structures, modes of evidence and thought, that can provide a foundation for resolving the question of how to make and keep peace in a world dominated by informational power.

References

Andersson, Ruben. (2016). Here be dragons: Mapping an ethnography of global danger, *Current Anthropology*, *57*(6), 707-731.

Barrera, Eduardo. (1995). State intervention and telecommunications in Mexico, *Journal of Communication*, *45*(4), 51-70.

Bell, Desmond. (1995). Communications, corporatism, and dependent development in Ireland, *Journal of Communication*, *45*(4), 70-88.

Braman, Sandra. (2017). The medium as power: Information and its flows as acts of war. In Cherian George (Ed.), *Communication and power*, pp. 3-22. Berne, Switzerland: Peter Lang, ICA Theme Book Series.

Braman, Sandra. (2014a). Cyber security ethics at the boundaries: System maintenance and the *Tallinn Manual*. In Ludovica Glorioso & Anna-Maria Osula (Eds.), Proceedings: 1st workshop on ethics of cyber conflict, pp. 49-58. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Braman, Sandra. (2014b). The geopolitical and the network political: Internet designers and governance, *International Journal of Media and Cultural Politics, 9*(2), 277-296.

Braman, Sandra. (2014c). "We are Bradley Manning": The legal subject and the WikiLeaks complex, *International Journal of Communication, 8*, 2603-2618.

Braman, Sandra. (2011). The framing years: Policy fundamentals in the Internet design process, 1969-1979, The Information Society, 27(5), 295-310.

Braman, Sandra. (2006). *Change of state: Information, policy, and power*. Cambridge, MA: MIT Press.

Braman, Sandra. (2004). The processes of emergence (pp. 1-11) & The emergent global information policy regime (pp. 12-37). In Sandra Braman (Ed.), *The emergent global information policy regime*. Houndsmills, UK: Palgrave Macmillan.

Braman, Sandra. (1996). From virtue to vertu to the virtual: Art, self-organizing systems, and the network economy, *Readerly/Writerly Texts: Essays on Literature, Literary/Textual Criticism, and Pedagogy, 3*(2), 1996, 149-166.

Braman, Sandra. (1995). Horizons of the state: Information policy and power, *Journal of Communication, 45*(4), 4-24.

Braman, Sandra. (1991). Vulnerabilities of the state and the New World Information and Communication Order, *Media Development, 38*(3), 6-8.

Braman, Sandra. (1990). The CSCE and information policy for the new Europe. Presented to the Second Conference: Europe Speaks to Europe, Moscow, December.

Braman, Sandra. (1985). The "facts" of El Salvador according to objective and new journalism, Journal of Communication Inquiry, 13(2), 75-96.

Buchan, Russell. (2016). Cyberspace, non-state actors and the obligation to prevent transboundary harm, *Journal of Conflict & Security Law*, *21*(3), 429-453.

Buchanan, G. Sidney. (1997). A conceptual history of the state action doctrine: The search for governmental responsibility, Part II, *Houston Law Review*, *34*, 665-775.

Caporaso, James A. (1995). The European Union and forms of state: Westphalian, regulatory or post-modern? *Journal of Common Market Studies*, *34*(1), 29-52.

Chatham House. (2006). The Chatham House principles of international law on the use of force in self-defense, *International & Comparative Law Quarterly*, *55*, 963-972.

Citizens United v Federal Election Commission (FEC), 558 US 310 (2010).

Coeckelbergh, Mark. (2011). From killer machines to doctrines and swarms, or why ethics of military robotics is not (necessarily) about robots, *Philosophy of Technology*, *24*, 269-278.
Demchak, Chris C. & Dombrowski, Peter. (2011, Spring). Rise of a cybered Westphalian age, *Strategic Studies Quarterly*, 32-61.
DeBúrca, Grálnne. (2016). Internalization of international law by the CJEU and the US Supreme Court, *I*CON*, *13*(4), 987-1007.
Demchak, Chris & Dombrowski, Peter. (2013). Cyber Westphalia: Asserting state prerogatives in cyberspace, *Georgetown Journal of International Affairs*, 29-38.
Dey, Pascal. (2016). Destituent entrepreneurship: Disobeying sovereign rule, prefiguring post-capitalist reality, *Entrepreneurship & Regional Development*, *28*(5-7), 563-579.
Franklin, Jonathan A. & Morris, Roberta J. (2002). International jurisdiction and enforcement of judgments in the era of global networks: Irrelevance of, goals for, and comments on the current proposals, *Chicago-Kent Law Review*, *77*, 1213-1294.
Froomkin, A. Michael. (1997). The Internet as a source of regulatory arbitrage. (SSRN only)
Graczyk, Joel M. (2015). Could a corporation serve in Congress? Corporations and citizenship under the constitution, *Journal of Business and Security Law*, *16*, 85-110.
Griswold v Connecticut, 381 US 479 (1965).
Hauben, Rhonda. (2004). The Internet: On its international origins and collaborative vision, *Amateur Computerist*, *12*(2), http://www.ais.org/~jrh/acn/ACn12-2.a03.txt.
Henrikson, Alan K. (1981). The emanation of power, *International Security*, *6*(1), 152-164.
Hobson, Charles F. (1979). The negative on state laws: James Madison, the Constitution, and the crisis of Republican government, *The William and Mary Quarterly*, *36*(2), 215-235.
Jakubowicz, Karl. (1995). Media within and without the state: Press freedom in Eastern Europe, *Journal of Communication*, *45*(4), 125-139.
Kessler, Oliver & Werner, Wouter. (2013). Expertise, uncertainty, and international law: A study of the Tallinn Manual on cyberwarfare, *Leiden Journal of International Law*, *26*(4), 793-810.
Knoepfel, Sascha. (2014). Clarifying the international debate on Stuxnet: Arguments for Stuxnet as an act of war. In J.-F. Kremer & B. Muller (Eds.), *Cyberspace and international relations*, pp. 117-124. Berlin/Heidelberg: Springer Verlag.
Koh, Harold Hongju. (2017). The emerging law of 21st century war, *Emory Law Journal*, *66*(3), 487-512.
Kuhn, Thomas. (1962). *The structure of scientific revolutions*. Chicago: University of Chicago Press.
Lehmann, Todd C., Rolfsen, James A., & Clark, Terry D. (2015). Predicting the trajectory of the evolving international cyber regime: Simulating the growth of a social network, *Social Networks*, *41*, 72-84.
Lierse, Hanna & Seelkopf, Laura. (2016). Room to manoeuvre? International financial markets and the national tax state, *New Political Economy*, *21*(1), 145-165.
Locke, John. (1690/1964). *An essay concerning human understanding*. New York: William Collins & Sons.
Lukes, Steven. (2005). *Power: A radical view*, second edition. Basingstoke, UK: Palgrave Macmillan.

Mačák, Kubo. (2016). Is the international law of cyber security in crisis? In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), Proceedings of the 8th International Conference on Cyber Conflict, pp. 127-139. Tallinn: NATO CCD COE.
Matwyshyn, Andrea M. (2004). Material vulnerabilities: Data privacy, corporate information security, and securities regulation, *Berkeley Business Law Journal*, *3*, 129, http://scholarship.law.berkeley.edu/bblj/vol3/iss1/4/.
McDowell, Stephen. (1995). The decline of the License Raj: Indian software export policies, *Journal of Communication*, *45*(4), 25-50.
Mody, Bella. (1995). State consolidation through liberalization of telecommunications services in India, *Journal of Communication*, *45*(4), 107-124.
Michaels, Ralf. (2010). The mirage of non-state governance, *Utah Law Review*, *2010*(1), 31-45.
Neave, Guy. (1998). The evaluative state reconsidered, *European Journal of Education*, *33*(3), 265-284.
Nettl, J. P. (1968). The state as a conceptual variable, *World Politics*, *20*(4):559-592.
Nye, Joseph S. (2014). The regime complex for managing cyber activities. Global Commission on Internet Governance Paper Series, 1.
Nye, Joseph S. (2004). *Soft power: The means to success in world politics*. New York: Public Affairs.
Oettinger, Anthony G., Berman, Paul J., & Read, William H. (1977). *High and low politics: Information resources for the 80s*. Cambridge, MA: Ballinger Publishing Co.
Post, David R. & Johnson, David. (1996). Law and borders: The rise of law in cyberspace, *First Monday*, *1*(1), http://firstmonday.org/ojs/index.php/fm/article/view/468/389. Republished in *Stanford Law Review* (1996): 1367-1402.
Radin, Sasha. (2013). Global armed conflict? The threshold of extraterritorial non-international armed conflicts, *International Law Studies*, *89*, 696-743.
Ramraj, Victor V. (2013). Beyond the courts, beyond the state: Reflections on Caldwell's 'Horizontal rights and Chinese constitutionalism,' *Chicago-Kent Law Review*, *88*, 93-103.
RFC 1179. (1990). Line printer daemon protocol. L. McLaughlin, Ed., The Wollongong Group.
Rosenzweig, Paul. (2012). The international governance framework for cybersecurity, *Canada-United States Law Journal*, *37*(2), Art. 10, 1-28.
Rutkowski, Anthony. (2011). Public international law of the international telecommunication instruments: Cyber security treaty provisions since 1850 *13*(1), 13-31.
Scazzieri, Roberto. (1993). *A theory of production*. Cambridge: Cambridge University Press.
Scott, James C. (1999). *Seeing like a state: How certain schemes to improve the human condition have failed*. New Haven, CT: Yale University Press.
Shackleford, Scott & Craig, Amanda. (2014). Beyond the new 'digital divide': Analyzing the evolving role of national governments in Internet governance and enhancing cybersecurity, *Stanford Journal of International Law*, *50*, 119-184.
Schmitt, Michael N. (2012). International law in cyberspace: The Koh speech and Tallinn Manual juxtaposed, *Harvard International Law Journal*, *54*, 13-37.

Spencer, A. Michael. (2006). Jurisdiction and the Internet: Returning to traditional principles to analyze network-mediated contacts, *University of Illinois Law Review*, 71-126.

Sussman, Gerald. (1995). Transnational communications and the dependent-integrated state, *Journal of Communication*, *45*(4), 89-106.

Treverton, Gregory F., Matthies, Carl, Cunningham, Karla J., Goulkah, Jeremiah, Ridgeway, Greg, & Wong, Anny. (2009). *Film piracy, organized crime, and terrorism*. Santa Monica, CA:

Tsipis, Kosta, David W. Hafemeister, and Penny Janeway, Eds. (1986). *Arms control verification: The technologies that made it possible*. McLean, VA: Pergamon-Brasssey's International Defense Publishers.

United States Department of Defense. (2015). *The Department of Defense Cyberstrategy*. Washington, DC: United States Department of Defense.

United States Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense.

Woudsma, Peter. (2013). Cyber defence: A major topic in NATO's transformation. NATO, Transformer 2013-01.

Yeo, Colin. (2003). Agents of the state: When is an official of the state an agent of the state? *International Journal of Refugee Law*, *14*(3), 509-533.

Zander, Michael. (1959). The act of state doctrine, *The American Journal of International Law*, *53*:4, 826-852.

Zittrain, Jonathan L. (2005). *Jurisdiction*. St. Paul, MN: Foundation Press.

Zumbansen, Peer. (2008). Law after the welfare state: Formalism, functionalism, and the ironic turn of reflexive law, *The American Journal of Comparative Law*, *56*(3), 769-808.