PART I

Beyond Stability, toward Cyber Peace: Key Concepts, Visions, and Models of Cyber Peace

1

Cyber Peace

Is That a Thing?

Renée Marlin-Bennett

1 INTRODUCTION

This book defines "positive cyber peace" as a digital ecosystem that rests on four pillars:

> (1) respecting human rights and freedoms, (2) spreading Internet access along with cybersecurity best practices, (3) strengthening governance mechanisms by fostering multistakeholder collaboration, and (4) promoting stability and relatedly sustainable development.

These pillars merit broad support for their emphasis on justice, good governance, and diffusion of technology to bridge the so-called "digital divide." They were developed through a global vetting process over time and in different fora, and they represent views of technologists, civil society thought leaders, and representatives of intergovernmental organizations (see Permanent Monitoring Panel on Information Security of the World Federation of Scientists, 2009; Shackelford, 2014). Nevertheless, the conceptualization of cyber peace and its pillars deserves further probing. Is cyber peace really a kind of peace? International relations and global studies theories include a substantial body of literature on peace, a condition and/or a relation that is both more capacious than the pillars and, perhaps, in some ways inconsistent with them. In addition, the pillars seem to be different kinds of things. The first refers to abstractions that are instantiated in law and take form through the practices of governments. The second is a diffusion of a technology along with technical standards. The third is a preference for a certain form of governance, and the fourth once again brings up a technical issue, but then pivots to sustainability. If the pillars are supporting an edifice, they are doing so unevenly.[1] In this chapter,

[1] The critique presented in this chapter raises concerns that resonate with criticism of the concept, "global public goods," as discussed by David Long and Frances Woolley (2009). They suggest that "the concept is poorly defined, avoids analytical problems by resorting to abstraction, and masks the incoherence of its two central characteristics [the confusion of nonrivalness and nonexcludability]. The conclusion is that even if the concept of global public goods is effective rhetorically, precise definition and conceptual disaggregation are required to advance analysis of global issues."

I probe the ontological basis of the concept of cyber peace and uncover tensions in the meanings embedded in it.

The task begins with ontological questions about what kind of thing cyber peace is. This section draws on the definitions cyber peace advocates use to taxonomize the stated or implied assumptions about cyber peace as a condition or as a set of practices. As a condition, cyber peace is sometimes defined as a kind of peace, and at other times as something within cyberspace. Distinct modes of ontologizing cyber peace as a set of practices include cyber peace as cyber peacemaking, as maintaining the stability of information technology, and/or as cyber defense actions. The second section looks to international relations and cognate field scholarship for insight into further honing the conceptualization of cyber peace. The topics in this section include unpacking cyber as a modifier of peace, unpacking the concept of peace itself, exploring the boundaries of cyber peace by looking at how it is different from similar social things, and analyzing the implications of metaphors associated with cyber peace. The chapter concludes with a brief comment on the intent of the critique.

2 CONTENDING DEFINITIONS

The ontological question is what kind of thing is cyber peace or would it be if it were to exist?[2] Unless practitioners and scholars can come to some kind of consensus around the ontological nature of cyber peace the project risks incoherence. As cyber peace has slipped into the lexicon, beginning around 2008, the term has been used differently by the several interlocutors who draw upon it. Cyber peace is sometimes understood as a social condition or quality, sometimes as a set of practices, and sometimes as both. In this section, I interpret some core texts to tease out differences between the meanings and discuss the theoretical consequences of the differences.[3]

In drawing upon a text, I do not mean to imply that my short selections are representative of everything authors think about cyber peace, or that their definition is incorrect. Instead, I use these different articulations to show the variety of ways

[2] Thomas Hofweber (2005, p. 256) provides a pithy definition of ontology as the part of metaphysics "that tries to find out what there is: what entities make up reality, what is the stuff the world is made from?" The terms "ontology" and "ontological" in this chapter refer specifically to social ontology, the understanding of the stuff of the social world. John Searle (2006, p. 16) provides the examples of "baseball games, $20 bills, and national elections" as social things that depend on collective agreement over their ontologies. I can differentiate between professional baseball and Little League games; between $20 in US versus Canadian dollars; and among various kinds of national elections. Intersubjective agreement about the ontology of a $20 bill allows me to pay the cashier. In other words, we can agree epistemologically about how to determine whether the bills I proffer are indeed $20 bills. In Searle's formulation: "X *counts as* Y *in context* C" (2006, p. 18). But what counts as cyber peace in a given context is not a settled thing. As I argue in this chapter, inconsistent ontologies for what cyber peace is or for what it ought to encompass can work against the goal of creating a better normative framework.

[3] The insight that cyber peace is used in multiple ways is certainly not new. Wegener (2011) specifically draws out the distinctions.

cyber peace is imagined. Highlighting the unsettledness of the essence of cyber peace is the point of the exercise.

3 THE CONDITION OF CYBER PEACE

An early use of the word "peace" in the context of cyberspace and the Internet is a 2008 forward written by the former Costa Rican president and Nobel laureate, Óscar Arias Sánchez, for the International Telecommunications Union's (ITU) report on the ITU's role in cybersecurity (Arias Sánchez, 2008). He referred to the need to promote "peace and safety in the virtual world" as "an ever more essential part of peace and safety in our everyday lives" and the urgency of creating a "global framework" to provide cybersecurity (p. 5). He implied that this safe place within cyberspace can be implemented through intergovernmental coordination around cybersecurity practices. The result would be to create the condition of feeling secure, very much along the lines of what one expects from the concept of "human security" (Paris, 2001; United Nations Development Program, 1994). Techniques, such as the adoption of cybersecurity best practices, Arias suggested, are tools that *promote* this safe world, but these tools are not themselves cyber peace. In context, it seems that peace and safety are not two separate goals but rather one: Safety *as* peace – either as a kind of peace or perhaps as a part of peace.

Ungoverned cyberspace is dangerous because of "the pitfalls and dangers of online predators" (Arias Sánchez, 2008, p. 4) who inhabit it. As a state of (albeit non-) nature, it is a Hobbesian (Hobbes, 1651) world of war and crime or, more precisely, the disposition toward violence which could break out at any time. This ungoverned, dangerous world of cyberspace is to be cordoned off and, perhaps, eliminated. Global coordination on cybersecurity is thus essential to promote the condition of safety.

Hamadoun Touré, writing in the introduction to *The Quest for Cyber Peace*, a joint publication of the ITU and the World Federation of Scientists (WFS), similarly seems to draw upon this Hobbesian view of ungoverned cyberspace when he writes that "[w]ithout mechanisms for ensuring peace, cities and communities of the world will be susceptible to attacks of an unprecedented and limitless variety. Such an attack could come without warning" (2011, p. 7). He continues, enumerating some of the devastating effects of such an attack. Touré's description suggests that conditions of cyberspace could break the security provided by the sovereign state (the leviathan) to its citizens. Violence is lurking just under the surface of our cyber interactions, waiting to break out. Touré, in a policy suggestion consistent with some liberal institutionalists' thinking in international relations, understands the potential of an international regime[4] (though he does not use that term) of agreed-upon rules that

[4] The special issue of *International Regimes*, edited by Stephen Krasner (1982), is widely viewed as the beginning of international regimes scholarship. However, Hayward Alker and William Greenberg (1977) introduced a similar concept of the same name earlier. More recent scholarship has focused on regime complexes (Alter & Raustiala, 2018).

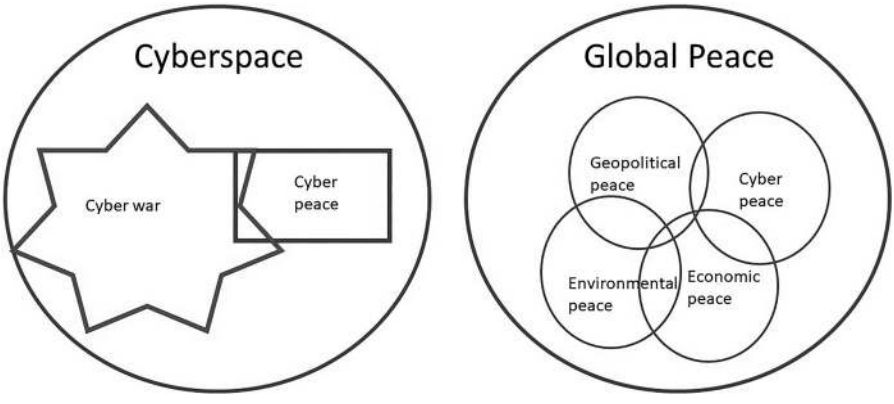

FIGURE 1.1 Different ontologies of cyber peace as conditions. On the left, both cyber peace and cyber war exist as kinds of social conditions within places of cyberspace. Cyber war is always attempting to penetrate and disrupt cyber peace. On the right, cyber peace is a subset of global peace, along with other kinds of peace.

would provide the condition of cyber peace in the absence of a single authoritative ruler. Arias and Touré both envision cyberspace as having a zone of lawlessness and war and a zone of safety and peace.

Henning Wegener's (2011) chapter in *The Quest for Cyber Peace* defines cyber peace more expansively than Touré did. More importantly, Wegener's ontology is subtly different from the division of cyberspace into the peaceful and violent zones I associated with Arias and Touré. Wegener writes:

> The starting point for any such attempted definition must be the general concept of peace as a wholesome state of tranquility, the absence of disorder or disturbance and violence – the absence not only of "direct" violence or use of force, but also of indirect constraints. Peace implies the prevalence of legal and general moral principles, possibilities and procedures for settlement of conflicts, durability and stability.
>
> We owe a comprehensive attempt to fill the concept of peace – and of a culture of peace – with meaningful content to the UN General Assembly. Its "Declaration and Programme of Action on a Culture of Peace" of October 1999 provides a catalogue of the ingredients and prerequisites of peace and charts the way to achieve and maintain it through a culture of peace (2011, p. 78).

By identifying cyber peace as a kind of peace rather than as a carve out of cyberspace, Wegener shifts the focus away from cyberspace as the world in which cyber peace exists or happens and, instead, connects to the material reality of the geopolitical world. The distinction is illustrated in Figure 1.1. The image on the left represents the definition invoked by Arias and Touré. The image on the right represents the definition invoked by Wegener.

4 CYBER PEACE AS PRACTICES

Other interlocutors use the phrase "cyber peace" to refer to practices, which can range from using safer online platforms for cross-national communication to "cyber peace keeping" or "cyber policing" to engineering a robust, stable, and functional Internet. This approach is consistent with (though not intentionally drawing upon) what has been called the "practice turn" in international relations (Adler & Pouliot, 2011; for example, Bigo, 2011; Parker & Adler-Nissen, 2012; Pouliot & Cornut, 2015). Practices constitute meaningful social realities because of three factors. First, it matters that human beings enact practices, because in doing so we internalize that action and it becomes a part of us. Second, there is both a shared and an individual component to practices. Individuals are agentic because they can act; the action has social relevance because others act similarly. Third, practices are constituted and reconstituted through patterned behavior; in other words, through "regularity and repetition" (Cornut, 2015). Since cyber peace is an aspiration rather than something that exists now, a practice theory focus could point toward emerging or potential practices and how they are accreting.

One example of this aspirational view of practices can be found in the 2008 report, "Cyber Peace Initiative: Egypt's e-Safety Profile – 'One Step Further Towards a Safer Online Environment'," which defines cyber peace in terms of young people engaging in the practices of communicating and peacemaking.[5] According to Nevine Tewfik (2010), who summarized the findings in a presentation to the ITU, information and communications technologies (ICTs) "empower youth of any nation, through ICT, to become catalysts of change." These practices would then result in a more peaceful condition in geophysical space. Specifically, the end result would be "to create safe and better futures for themselves and others, to address the root causes of conflict, to disseminate the culture of peace, and to create international dialogues for a harmonious world" (p. 1). The report emphasized the initiative's efforts to promote safety of children online. An inference I draw from the presentation slides is that the dissemination of the culture of peace happens when children can engage safely with each other online. Cyberspace can be a place where children – perhaps because of their presumed openness to new ideas and relations – engage in peacemaking. Thus, the benefits of the prescribed cyber peace activities would spill over into the geophysical world.

Cyber peace is often defined as practices that maintain the stability of the Internet and connected services. (The tension between stability and peace will be

[5] The report on which the presentation was based is apparently no longer available online It was a joint project of Suzanne Mubarak Women's International Peace Movement, Egypt's Ministry of Communications and Information Technology, the International Telecommunication Union, and the Global Alliance for ICT and Development, in collaboration with Microsoft and Cisco Systems. The Ministry's website no longer features it, which perhaps has to do with the association of Suzanne Mubarak, or it may too old to be featured on the site. A summary of the report can be found on the website of the Virtue Foundation (Virtue Foundation Institute for Innovation and Philanthropy, n.d.).

discussed later.) Drawing on this definition leads advocates to argue for prescriptions of protective behaviors and proscriptions of malign behaviors to maintain the functional integrity of the global ICT infrastructure. Key to this is the connection between a stable global network of ICTs and the ability to maintain peaceful practices in the geophysical world. The WFS, for example, had been concerned with all threats to information online ("from cybercrime to cyberwarfare"), but the organization's permanent monitoring panel on information security "was so alarmed by the potential of cyberwarfare to disrupt society and cause unnecessary harm and suffering, that it drafted the Erice Declaration on Principles of Cyber Stability and Cyber Peace" (Touré & Permanent Monitoring Panel on Information Security of the World Federation of Scientists, 2011, p. vii). The declaration states: "ICTs can be a means for beneficence or harm, hence also as an instrument for peace or for conflict" and advocates for "principles for achieving and maintaining cyber stability and peace" (Permanent Monitoring Panel on Information Security of the World Federation of Scientists, 2009, p. 111). These principles about how to use ICTs are, in fact, practices. By adhering to the principles and acting properly, engagements in cyberspace and ICTs promote peace in the world. The declaration seems to refer to a general condition combining life as normal without the disruptions that warlike activities cause to "national and economic security," and life with rights, that is human and civil rights, "guaranteed under international law."

In other words, for this declaration stability is a desired characteristic of cyberspace and peace is a desired characteristic of life in the world as a whole. However, it does not follow that stability is inherently peaceful, unless peace is tautologically defined as stability. The absence of cyber stability might harm peace and the presence of cyber stability might support peace, but the presence of stability is not itself peaceful, nor does it generate peace.[6] At best, we can say that peace is usually easier to attain under conditions of stability.

Another text focusing on cyber peace as a set of practices is the Cyberpeace Institute's website. It first calls for "A Cyberspace at Peace for Everyone, Everywhere," which seems to hint at cyber peace as a condition of global society, but the mission of the organization is defined primarily as the capacity to respond to attacks, and only secondarily as strengthening international law and the norms regarding conflictual behavior in cyberspace. Indeed, defense capacity is emphasized in the explanation that "The CyberPeace Institute will focus specifically on enhancing the stability of cyberspace by supporting the protection of civilian infrastructures from sophisticated, systemic attacks" (CyberPeace Institute – About Us, 2020). The ability to mount a swift defense in response to an attack does not create peace, it simply means that our defenses may be strong enough

[6] The use of cyber weapons by human rights activists to counter oppressive regimes is discussed in the section on boundaries (Section 7).

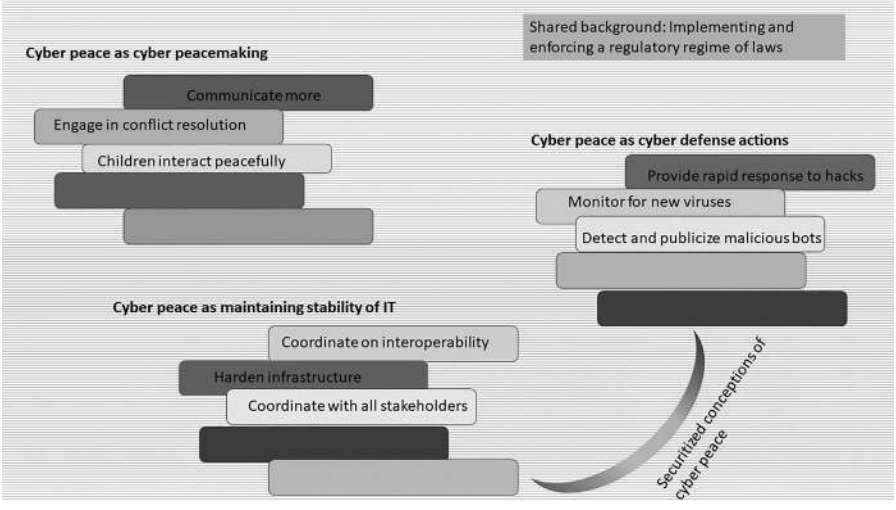

FIGURE 1.2 Cyber peace as the sum of practices in both securitized and non-securitized conceptualizations, against a shared background of implementing and enforcing a regulatory regime of laws.

that the attacks do not disrupt the stability of the Internet and other information technologies.

These conceptualizations of cyber peace as collections of practices thus ontologize kinds of cyber peace, which are distinct, but comparable. By comparing them, we can see underlying tensions regarding what can be considered peaceful – Is it peace making or securitization (defense and stability)? – though, as noted in the descriptions above, no collection of practices is wholly of one type. Figure 1.2 depicts different collections of practices that have been bundled together as the definition of cyber peace. (For clarity, I have not shown overlaps.) All of these conceptualizations are proposed against a background of a regulatory regime of implementing and enforcing laws.

5 CYBER PEACE AS BOTH CONDITIONS AND PRACTICES

A third category blends conditions and practices, seeing the condition of cyber peace emerge as greater than the sum of its constituent parts, which are practices. In an early iteration of his work on this concept, Scott Shackelford (2014) paints this sort of hybrid picture of cyber peace. He claims that the practices of polycentric governance related to cybersecurity spill over into a positive cyber peace:

> Cyber peace is more than simply the inverse of cyber war; what might a more nuanced view of cyber peace resemble? First, stakeholders must recognize that a positive cyber peace requires not only addressing the causes and conduct of cyber

> war, but also cybercrime, terrorism, espionage, and the increasing number of incidents that overlap these categories (p. 357).

This can happen, Shackelford suggests, through a process of building up governance on limited problems, thereby proliferating the number of good governance practices. The polycentric governance model specifically rejects a top-down monocentric approach:

> [A] top-down, monocentric approach focused on a single treaty regime or institution could crowd out innovative bottom-up best practices developed organically from diverse ethical and legal cultures. Instead, a polycentric approach is required that recognizes the dynamic, interconnected nature of cyberspace, the degree of national and private-sector control of this plastic environment, and a recognition of the benefits of multi-level action. Local self-organization, however – even by groups that enjoy legitimacy – can be insufficient to ensure the implementation of best practices. There is thus also an important role for regulators, who should use a mixture of laws, norms, markets, and code bound together within a polycentric framework operating at multiple levels to enhance cybersecurity (p. 359, notes omitted).

These interconnected, overlapping, small to medium-scale governance practices build upward in Shackelford's model and could eventually become a thick cybersecurity regime. When the regime is thick enough, cyber peace obtains. This model relies on a securitized notion of cyber peace, despite the discussion in the text of positive cyber peace that is more far-reaching than just the absence of war. His more recent work, co-authored by Amanda Craig, expands cyber peace to include global peace-related issues and practices, including development and distributive justice. They write:

> Ultimately, "cyber peace" will require nations not only to take responsibility for the security of their own networks, but also to collaborate in assisting developing states and building robust regimes to promote the public service of global cybersecurity. In other words, we must build a positive vision of cyber peace that respects human rights, spreads Internet access alongside best practices, and strengthens governance mechanisms by fostering global multi-stakeholder collaboration, thus forestalling concerns over Internet balkanization (Shackelford & Craig, 2014, p. 178, note omitted).

Figure 1.3 depicts this model of best practices developed from the ground up, ultimately producing a kind of cyber peace that exceeds the summation of all the different practices.

The point of this exercise of categorizing different definitions of cyber peace is to say that a definitional consensus has not been reached and to remind ourselves that the ontology built into our definitions matters for how we think about what sounds like a very good goal. Moreover, ontological foundations matter for how the practitioners among us craft policies in pursuit of that goal.