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."

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

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.

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

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).

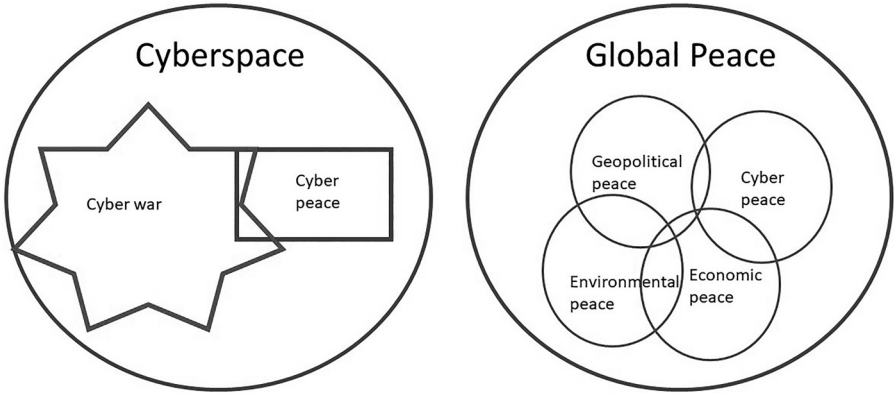

FIGURE 1.1 Different ontologies of cyber peace as conditions. On the left, both cyber peace and cyber war exist as kinds of social conditions within places of cyberspace. Cyber war is always attempting to penetrate and disrupt cyber peace. On the right, cyber peace is a subset of global peace, along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

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

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).

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

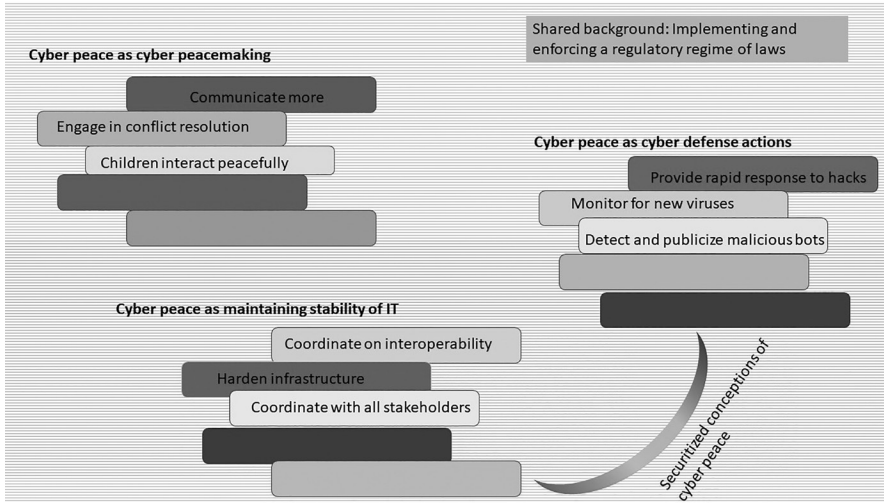

FIGURE 1.2 Cyber peace as the sum of practices in both securitized and non-securitized conceptualizations, against a shared background of implementing and enforcing a regulatory regime of laws.

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

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

> 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.

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

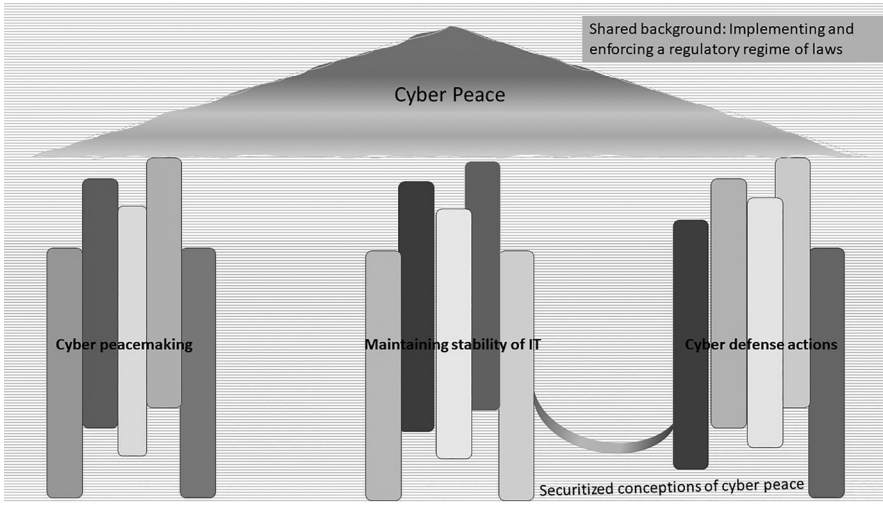

FIGURE 1.3 Peaceful practices and shared background emerge as cyber peace, which is greater than the sum of its parts.

6 HONING THE CONCEPT OF CYBER PEACE

The four parts of this section critically engage further with cyber peace, pointing to conceptual elements that could be productively honed to make a sharper point. The point here is not to provide an answer of what cyber peace is or should be but, rather, to draw upon scholarship from international relations and cognate fields to uncover contradictions and missed implications of the current usage. I begin by taking a closer look at "cyber" and "peace" and then turn to the boundaries of cyber peace as a social thing, followed by a discussion of the consequences of some of the metaphors associated with cyber peace.

6.1 *Unpacking the "Cyber" Element*

"Cyber" is a shortening of "cybernetics," a term introduced by Norbert Wiener, who used it to refer to the control of information machines and human groups. He emphasized: "*Cybernetics takes the view that the structure of the machine or of the organism is an index of the performance*" (Wiener, 1988, p. 57; italics in original) because the structures – that is, the properties of the machine or organism – determine what the machine or organism is able and unable to do, and what it is permitted to do, must do, and must not do. Cybernetics concerns control and order; its purpose is to be a bulwark against disorder and entropy. The shortened form quickly came to connote that which involves computers and information technology. "Cyberspace," famously introduced in *Neuromancer* by William Gibson (1994), rapidly became the narrative means of reimagining a communications technology (the Internet) as a place

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

(albeit a heterotopia [Foucault, 1986; Piñuelas, 2008]) *in* which or *on* which people (reimagined as users) do things and *to* which they go. As discussed in the section on cyberspace as a condition, we then imagine cyberspace to be a state of (non-) nature apart from the real-life physical world we live in, and we think of it as dangerous because it is ungoverned or incompletely governed. Some instances of cybercrime give credence to that, though such crimes may well be subject to law enforcement by real-life police or others. The irony is that although the cyber refers to the *realization of control*, cyberspace is thought of as a place of *lack of control*, as David Lyon (2015) has recognized.

More recent morphing of the usage of "cyber" turns it into a noun associated with military activity using information technology-intensive tools. This particular nominalization immediately calls to mind warnings from securitization theory (Balzacq, 2005; inter alia, Buzan, 1993; Hansen, 2000; Waever, 1996). The theory focuses on how language constrains our thinking and specifically on how language recasts situations, people, processes, relations, etc. as security threats, and leads to a creeping expansion of control by institutions that command the use of force. This should be understood as a danger rather than a deterministic outcome,[7] and I am not arguing that we should excise "cyber" from the dictionary. But I am mindful of the securitizing language that drags the concept of cyber peace back toward a sort of negative peace. As Roxanna Sjöstedt (2017) puts it, "If you construct a threat image, you more or less have to handle this threat."

In short, "cyber" is complicated. The word connotes the constitution of a space outside our ordinary existence in geographical space. Cyber implies order in the form of efficient control through code and other engineered rules that ought to work well. Yet cyber also hints at disorder and even chaos, since rules are often circumvented. Additionally, the military's appropriation of cyber as a shortening of "cyber conflict" or "cyber war" risks turning cyber peace into an oxymoron, taking on the sense of martial peace. That linguistic change may condition thinking and securitize the very thing that ought to be desecuritized.

6.2 *Unpacking the "Peace" Element*

If anything, peace is even more complicated than cyber. Peace is the main focus of the entire field of peace studies, and it is also an important topic for scholars of conflict management and conflict resolution, as well as of international relations more

[7] Jan Ruzicka (2019) points out the problem of case selection bias in empirical studies of securitization, with studies of successful instances of securitization being more common in the scholarship than studies of failures. A notable exception is Myriam Dunn Cavelty's (2013) nuanced study of cyber insecurity and the multiple ways it is framed. Although she leaves open the possibility of further non-securitizing responses to threats of cyberspace, she concludes that "the stronger the link between cyberspace and a threat of strategic dimensions becomes, the more natural it seems that the keeper of the peace in cyberspace should be the military" (p. 119).

broadly. Peace always sounds good – better than war, at any rate.[8] But the war-peace dichotomy may hide the definitional complexity. Johann Galtung differentiates between "negative peace," understood as the absence of violence in a relationship and "positive peace," a more complex term that is often used to refer to relations that are just, sustainable, and conducive human flourishing in multiple ways (see also Shackelford, 2016). In its most expansive connotation, the relationship of positive peace is tied to peacebuilding and, ultimately, to amity. The main thrust of this volume envisions cyber peace as positive cyber peace. But the caveats articulated by Paul Diehl (2016, 2019) about positive peace and its usefulness as a social type of thing are worth considering. He notes, first of all, the lack of consensus among positive peace researchers about what is actually included in it:

> Conceptions include, among others, human rights, justice, judicial independence, and communication components. Best developed are notions of "quality peace," which incorporate the absence of violence, but also require things such as gender equality in order for societies to qualify as peaceful (2019).
>
> The lack of clarity over what positive peace is has, Diehl suggests, epistemological consequences.
>
> Many of [the things that are required for societies to qualify as peaceful], however, lack associated data and operational indicators. Research on positive peace is also comparatively underdeveloped (2019).[9]

While Diehl finds the concept of positive peace desirable, he warns that the concept is underdeveloped in three important ways, and each of these resonates with considerations about cyber peace.

First, what are the dimensions of peace and why is so little known about how the many dimensions interact? His concern should provoke cyber peace theorists to consider whether the four pillars are dimensions in Diehl's terms and, if so, whether they comprise *all* the dimensions. Given the potential for multiple dimensions of peace, perhaps only some are required for the situation to be deemed peaceful.

[8] Though I called out the martial quality of "cyber" (discussed in the section on cyber), one could argue that "peace" is as likely to make "cyber" seem *less* military as "cyber" is likely to make "peace" sound *more* military.

[9] To be fair, Diehl is interested in identifying better ways of understanding and studying positive peace and not just critiquing the deficiencies. It is also important to note that Diehl takes a mainstream (neopositivist) approach to social science methodology. He is concerned about operationalizing positive peace in ways that will allow researchers to subject it to mainstream hypothesis testing. That is, he is less interested in critical interpretivist approaches adopted by many theorists outside the mainstream. (Theorists outside the mainstream include those working on critical, feminist, and green theories, to name a few.) Many of the scholars writing about positive peace ally with the non-mainstream camp (to borrow a rather warlike metaphor). Disagreements over appropriate methodological approaches to research notwithstanding, most scholars will likely agree that conceptual clarity is necessary for good research, and that is the key point that Diehl is making. (Herbert Reid and Ernest Yanarella [1976] offhandedly made just that point for research on positive peace, p. 340, n. 107.) I would add that conceptual clarity is similarly necessary for advocacy based on that concept.

Alternatively, perhaps cyber peace is actually an ideal type, and the different dimensions make a situation more or less cyber peaceful.

Second, Diehl also raises the concern about an undertheorized assessment of how positive peace varies across all forms of social aggregation ("levels of analysis" in international relations scholarship). How does positive peace manifest differently in different contexts? For cyber peace, this critique points to the not fully developed idea of how the scale works in cyberspace and how that matters. A neighborhood listserv is different from Twitter, but shares some characteristics relevant to peace – flame wars and incivility are a problem in both environments. But the risks of manipulation of communication by foreign adversaries on Twitter and the kinds of policies that would be required to make peace on Twitter means, I suggest, that the environment of cyberspace is similarly complicated with regard to scale.

Third, Diehl (2019) notes that "some positive peace concepts muddle the distinction between the definitional aspects of peace and the causal conditions needed to produce peaceful outcomes." I think that the four cyber peace pillars may fall prey to this lack of conceptual clarity and, perhaps, to a sort of tautology.

7 BOUNDARIES

The next topic is boundaries and the distinctions that create them. An argument can be made that we are witnessing the creation of cyber peace as a new social entity, a thing. Andrew Abbott (1995) suggests new things emerge through a process of yoking together a series of distinctions. This is an iterative process of asking what are the characteristics of the new thing and what are not? "Boundaries come first, then entities" (p. 860). Cyber peace has yet to cohere into the sort of enduring, reproducing institution that would count as one of the Abbott's new social entities, but we do see the setting of "proto-boundaries" that may become stable when we examine the processes of trying to name and implement cyber peace. In this section, I discuss three "points of difference" that are important for the concretization of cyber peace: Between (1) cyber peace and cyber aggression, (2) cyber peace/aggression and cyber lawfulness/crime, and (3) associating multistakeholder cyber governance with cyber peace and (implicitly) associating other forms of cyber governance with non-cyber peace.

A basic distinction is between the common sense understanding of what constitutes cyber peace versus cyber aggression. The case of the 2007 cyberattack against Estonia is a clear example of cyber aggression. A more complicated case is Stuxnet, the malicious computer worm discovered in 2010, which was deployed against computer equipment used in the Iranian nuclear program. One interpretation of the Stuxnet operation would name it cyber aggression. A different interpretation would find the use of this cyber weapon de-escalatory when considered in its broader geopolitical context. Stuxnet decreased the rapid ramping up of Iran's ability to develop nuclear arms, which made an attack with full military force unnecessary. On the

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

one hand, information technology was used for a hostile purpose. On the other, the targeted cyber attack removed a significant threat with apparently no loss of life (though the spread of the worm through networks resulted in monetary losses). Perhaps in this case it makes sense to think of the possibility that Stuxnet was actually consistent with cyber peace. (See also Brandon Valeriano and Benjamin Jensen's assessment of the potential de-escalatory function of cyber operations in Chapter 4 of this volume.)

But is it possible to thread that needle – to use low-intensity, carefully targeted cyber operations (limiting their harmful consequences) to avoid more hostile interventions – as a matter of strategy? And if so, do such actions promote cyber peace? The 2018 United States Department of Defense cyber strategy tries to do this with its "defend forward" approach to cyber security, and by "continuously engaging" adversaries (United States Cyber Command, 2018, pp. 4, 6). The implicit analogy to nuclear deterrence likely conditions decision makers' expectations, in my view. As Jason Healey explains, proponents of the strategy seek stability through aggressiveness. They assert that "over time adversaries will scale back the aggression and intensity of their operations in the face of US strength, robustly and persistently applied" (2019, p. 2). But Healey is cautious – noting the risk of negative outcomes – as persistent engagement could produce an escalatory cycle. In short, further characterizing the nature of cyber peace requires achieving greater clarity in differentiating between the kinds of cyber aggression that promote more peaceful outcomes rather than less.

The second point of distinction creates a boundary between problems that involve criminal violations versus those that rise to the level of aggressive breaches of cyber peace. Unlike cyber aggression, cybercrime, I suggest, is not the opposite of cyber peace. The scams, frauds, thefts, revenge porn postings, and pirated software that are everyday cybercrimes seem to me to be very bad sorts of things, but as policy problems they generally fall into the category of not lawful, rather than not peaceful. A society can be peaceful or cyber peaceful even in the presence of some crime; all societies have at least some crime. Countering cybercrime requires cyber law enforcement and international collaboration to deal with transnational crimes. Countering cyber aggression requires efforts toward (re)building cyber peace. These might include diplomacy, deterrence, or – the less peaceful alternative – aggression in return. Automatically folding cybercrime into the category of things that threaten cyber peace risks diluting the meaningfulness of cyber peace.

A caveat must be added, however. The boundary between cybercrime and cyber aggression is complicated by what Marietje Schaake describes as "the ease with which malign actors *with geopolitical or criminal goals* can take advantage of vulnerabilities across the digital world" (2020, emphasis added). The "or" should be understood as inclusive: "and/or." Cybercrimes can be used to attain geopolitical goals (acts of cyber aggression), criminal goals, or both. The 2017 "WannaCry" ransomware attack, attributed to North Korea, provides an example of both cyber

aggression and cybercrime. Initially, WannaCry was assumed to be the work of an ordinary criminal, but once North Korea's involvement became apparent, the evident geopolitical aim and the attack's aggressiveness became more important. We would sort WannaCry and similar aggressive actions in the category of "threats" to cyber peace rather than into the category of (only) "not lawful."

Yet cybercrimes can, paradoxically, be tools *for* cyber peace too. Cybercrimes involving activities in support of human rights provide oppressed individuals and groups opportunities to fight back against their oppressors. Circumventing repressive surveillance technology might be an example of this. In that case, breaking the law could, arguably, be an example of cyber peace rather than a difference from it.

Third, the cyber peace pillar on multistakeholder collaboration assumes a distinction between cyber peace and non-cyber peace in terms of forms of governance. The definition of cyber peace includes a strong preference for developing "governance mechanisms by fostering multistakeholder collaboration" (Shackelford, 2016). Shackelford sees bottom-up multistakeholder governance as a form of polycentricity and as good in itself. But both polycentricity and multistakeholderism are problematic points of distinction for what is or is not cyber peaceful. Michael McGinnis and Elinor Ostrom (2012, p. 17), commenting on a classic article by Vincent Ostrom, Charles Tiebout, and Robert Warren (1961), call attention to how the authors:

> [...] did not presume that all polycentric systems were automatically efficient or fair, and they never denied the fundamentally political nature of polycentric governance. The key point was that, within such a system, there would be many opportunities for citizens and officials to negotiate solutions suited to the distinct problems faced by each community.

A multistakeholder form of polycentric governance, however, involves not just citizens and officials negotiating solutions, but firms and other private actors as well, which potentially skews that political nature because the resources the different stakeholders have to draw upon in their negotiations can differ by orders of magnitude. As Michael McGinnis, Elizabeth Baldwin, and Andreas Thiel (2020) explain, polycentric governance can come to suffer from dysfunction because of structural forms that allow some groups to have outsized control over decision-making processes. And this is certainly true for a cyberspace governance organization like the Internet Corporation for Assigned Names and Numbers (ICANN), where the industry interests have significantly more say in outcomes than users. Furthermore, whereas polycentric governance evolves organically out of efforts to solve problems of different but related sorts, multistakeholderism is designed into the governance plan from its initiation, as was clearly the case with ICANN.

Moreover, as Kavi Joseph Abraham (2017) explains, stakeholderism is actually not about creating better forms of democratic governance. Rather, its origin story can be traced to "systems thinking" in engineering and related management

practices that emphasized the need for control of complexity. Complex systems, as engineers came to understand, involved multiple inputs, feedback loops, contingencies, outputs, etc. Controlling such systems required coordination of *all* those factors. That idea of coordinating all inputs into processes spilled over into the academic field of business management, where the firm came to be seen as a complex system. Control involved the coordination of material inputs plus the coordinated activity and decision-making of people – workers, managers, customers, shareholders, suppliers, communities affected by effluents from the firm's factory, etc. Groups that had a role to play were thus identified as "stakeholders," but unlike the assumed equality of citizens in a democracy, there was never any assumption that stakeholders should be equal or equivalent. Managing is about dealing with complexity, not about governing while protecting rights. We should not assume that multistakeholderism is uniquely suited to be the governance form for cyber peace.

8 METAPHORS

Finally, I raise the issue of metaphors and how they enable and limit thinking in some way (Cienki & Yanow, 2013; Lakoff & Johnson, 1980). First, is cyber peace the right metaphor that describes the sought-after goal? How would cyber peace be different from cyber order, cyber community, or cyber health? Given that much of the activity that goes on in cyberspace is commercial and given that commercial transactions are generally competitive rather than peaceful, does it make sense to talk about cyber *peace* when the goal is not friendly relations but, rather, a competitive market in which exchange can happen without the disruption of crime? How is cyber peace distinct from a well-functioning cyber market? Yet another alternative would be to rethink the marketization of cyberspace and to imagine instead a regulated utility and the provision of cyber services to the global public.

Moreover, by invoking peace in the context of what is often intended to be best practices of cyber security to maintain a stable Internet we fall prey to "inadvertent complicity" (Alker, 1999, p. 3), distracting attention from real violence. Overusing the peace metaphor flattens the differences between deeply consequential and ethically crucial peacemaking in the world, and getting people to use better passwords. We can see this flattening dynamic even when considering initiatives promising to save lives (anti-cyberbullying initiatives as a cyber peace practice, for example). I think cyberbullying is truly awful, and in the United States, it is a crime. It is often also a mental health challenge, both for the bully and bullied. It's a social pathology and a behavioral problem. It is also a cyber governance issue, as E. Nicole Thornton and I discussed in an article on the difficulties faced by owners of social media websites trying to prevent hijacking of their sites by bullies (Marlin-Bennett & Thornton, 2012). But is it useful to think of cyberbullying as a violation of cyber peace? (And doesn't doing so give the bully too much power?) Cyber peace becomes

https://doi.org/10.1017/9781108954341.001 Published online by Cambridge University Press

hyperbole, notwithstanding the well-meaning campaigns such as that of the Cyber Peace Foundation (CyberPeace Corps, 2018). Peace is a strong word. By invoking peace (and war by implication), context and historicity can be washed away, obscuring the difference between cyberbullying and Russian cyber election disruptions that threaten to do grave harm to democracies.

9 A FINAL THOUGHT

In the oft-cited special issue of *International Organization* on international regimes, the final article was written by Susan Strange (1982). The title was "*Cave! hic dragones*: a critique of regime analysis." A note in smaller type at the bottom of the page reads "The title translates as 'Beware! here be dragons!' -an inscription often found on pre-Columbian maps of the world beyond Europe." The article, she explains in the first paragraph, does not ask "what makes regimes and how they affect behavior, it seeks to raise more fundamental questions about the questions." Her intent, instead, was to ask whether the regime concept is at all a useful advance for international political economy and world politics scholarship. She famously decided that the concept of the international regime was a bad idea for seven reasons (five main and two indirect). She was wrong. The concept of the international regime has endured and is widely accepted, and it has been useful. But I do not think that the concept of an international regime would have been nearly as well integrated into our scholarly lexicon now if it had not been for Strange's intervention. Over the subsequent years, proponents of the regime concept had to work to improve the concept to counter her claims, which were really quite fair, if expressed bluntly.

I do not have as negative an opinion of cyber peace as Strange did of international regimes, but her charge that the concept of international regimes was "imprecise and woolly" seems to fit the concept of cyber peace, as well. By analyzing the different meanings ascribed to cyber peace, I hope to do what Strange, intentionally or not, did for regimes theory: Make it better.

REFERENCES

Abbott, A. (1995). Things of Boundaries. *Social Research*, *62*(4), 857–882.

Abraham, K. J. (2017). *Governing through Stakeholders: Systems Thinking and the Making of Participatory Global Governance* [Thesis, Johns Hopkins University].

Adler, E., & Pouliot, V. (2011). *International Practices*. Cambridge University Press.

Alker, H. R. (1999). *Ontological Reflections on Peace and War*. SFI Working Paper #99-02-011 (Unpublished Material). www.santafe.edu/research/results/working-papers/ontological-reflections-on-peace-and-war

Alker, H. R., & Greenberg, W. J. (1977). On Simulating Collective Security Regime Alternatives. In G. M. Bonham & M. J. Shapiro (Eds.), *Thought and Action in Foreign Policy* (pp. 263–305). Birkhäuser. https://doi.org/10.1007/978-3-0348-5872-4_9

Alter, K. J., & Raustiala, K. (2018). The Rise of International Regime Complexity. *Annual Review of Law and Social Science*, *14*(1), 329–349. https://doi.org/10.1146/annurev-lawsocsci-101317-030830

Arias Sánchez, Ó. (2008). Foreword by the Patron of the Global Cybersecurity Agenda. In *Cybersecurity for ALL: ITU's Work for a Safer World* (pp. 4–5). International Telecommunications Union. www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-CYBER-2007-PDF-E.pdf

Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations*, *11*(2), 171–201. https://doi.org/10.1177/1354066105052960

Bigo, D. (2011). Pierre Bourdieu and International Relations: Power of Practices, Practices of Power. *International Political Sociology*, *5*(3), 225–258.

Buzan, B. (1993). From International System to International Society: Structural Realism and Regime Theory Meet the English School. *International Organization*, *47*(3), 327–352. https://doi.org/10.1017/S0020818300027983

Cienki, A., & Yanow, D. (2013). Why Metaphor and Other Tropes? Linguistic Approaches to Analysing Policies and the Political. *Journal of International Relations and Development*, *16*(2), 167–176. https://doi.org/10.1057/jird.2012.28

Cornut, J. (2015, December 1). *The Practice Turn in International Relations Theory*. Oxford Research Encyclopedia of International Studies. https://doi.org/10.1093/acrefore/9780190846626.013.113

CyberPeace Corps. (2018, May 23). Cyberbullying Is a Form of Bullying, and Adults Should Take the Same Approach to Address It: Support the Child Being Bullied, Address the Bullying Behavior of a Participant, and Show Children That #cyberbullying Is Taken Seriously. #CyberPeaceFoundation #CyberPeaceCorps https://t.co/bdbcE1Vd2l / Twitter [Social Media]. Twitter. https://twitter.com/cyberpeacecorps/status/999215740816429056?lang=ca

CyberPeace Institute – About Us. (2020). CyberPeace Institute. https://cyberpeaceinstitute.org/about-us Accessed June 14, 2021.

Diehl, P. F. (2016). Exploring Peace: Looking Beyond War and Negative Peace. *International Studies Quarterly*, *60*(1), 1–10. https://doi.org/10.1093/isq/sqw005

Diehl, P. F. (2019). Peace: A Conceptual Survey. In Oxford Research Encyclopedia of International Studies. Oxford University Press. https://doi.org/10.1093/acrefore/9780190846626.013.515

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105–122. https://doi.org/10.1111/misr.12023

Foucault, M. (1986). Of Other Spaces. *Diacritics*, *16*(1), 22–27.

Gibson, W. (1994). *Neuromancer*. Ace Books.

Hansen, L. (2000). The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School. *Millennium*, *29*(2), 285–306. https://doi.org/10.1177/03058298000290020501

Healey, J. (2019). The Implications of Persistent (and Permanent) Engagement in Cyberspace. *Journal of Cybersecurity*, *5*(1), 1–15. https://doi.org/10.1093/cybsec/tyz008

Hobbes, T. (1651). *Leviathan*. Andrew Crooke, at the Green Dragon in St. Paul's Churchyard. www.gutenberg.org/files/3207/3207-h/3207-h.htm

Hofweber, T. (2005). A Puzzle About Ontology. *Noûs*, *39*(2), 256–283.

Krasner, S. D. (Ed.). (1982). International Regimes (special issue). *International Organization*, *36*(2).

Lakoff, G., & Johnson, M. (1980). *Metaphors We Live By*. University of Chicago Press.
Long, D., & Woolley, F. (2009). Global Public Goods: Critique of a UN Discourse. *Global Governance*, *15*(1), 107–122.
Lyon, D. (2015). Beyond Cyberspace: Digital Dreams and Social Bodies. *Information Technology, Education, and Society*, *1*(2), 5–21. https://doi.org/10.7459/ites/16.1.02
Marlin-Bennett, R., & Thornton, E. N. (2012). Governance within Social Media Websites: Ruling New Frontiers. *Telecommunications Policy*, *36*(6), 493–501. https://doi.org/10.1016/j.telpol.2012.01.002
McGinnis, M. D., Baldwin, E. B., & Thiel, A. (2020). *When Is Polycentric Governance Sustainable? Using Institutional Theory to Identify Endogenous Drivers of Dysfunctional Dynamics*. https://ostromworkshop.indiana.edu/events/colloquium-series/index.html
McGinnis, M. D., & Ostrom, E. (2012). Reflections on Vincent Ostrom, Public Administration, and Polycentricity. *Public Administration Review*, *72*(1), 15–25.
Ostrom, V., Tiebout, C. M., & Warren, R. (1961). The Organization of Government in Metropolitan Areas: A Theoretical Inquiry. *The American Political Science Review*, *55*(4), 831–842.
Paris, R. (2001). Human Security: Paradigm Shift or Hot Air? *International Security*, *26*(2), 87–102.
Parker, N., & Adler-Nissen, R. (2012). Picking and Choosing the 'Sovereign' Border: A Theory of Changing State Bordering Practices. *Geopolitics*, *17*(4), 773–796. https://doi.org/10.1080/14650045.2012.660582
Permanent Monitoring Panel on Information Security of the World Federation of Scientists (WFS). (2009). *Erice Declaration on Principles for Cyber Stability and Cyber Peace*. World Federation of Scientists. www.aps.org/units/fip/newsletters/201109/barletta.cfm
Piñuelas, E. (2008). Cyber-Heterotopia: Figurations of Space and Subjectivity in the Virtual Domain. *Watermark*, *2*, 152–169.
Pouliot, V., & Cornut, J. (2015). Practice Theory and the Study of Diplomacy: A Research Agenda. *Cooperation and Conflict*, *50*(3), 297–315. https://doi.org/10.1177/0010836715574913
Reid, H. G., & Yanarella, E. J. (1976). Toward a Critical Theory of Peace Research in the United States: The Search for an "Intelligible Core." *Journal of Peace Research*, *13*(4), 315–341. https://doi.org/10.1177/002234337601300404
Ruzicka, J. (2019). Failed Securitization: Why It Matters. *Polity*, *51*(2), 365–377. https://doi.org/10.1086/702213
Schaake, M. (2020). The Lawless Realm. *Foreign Affairs*, *99*(6). www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm
Searle, J. R. (2006). Social Ontology: Some Basic Principles. *Anthropological Theory*, *6*(1), 12–29.
Shackelford, S. J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge University Press. https://doi.org/10.1017/CBO9781139021838
Shackelford, S. J. (2016). Business and Cyber Peace: We Need You! *Business Horizons*, *59*(5), 539–548. https://doi.org/10.1016/j.bushor.2016.03.015
Shackelford, S. J., & Craig, A. N. (2014). Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity Symposium. *Stanford Journal of International Law*, *50*(1), 119–184.
Sjöstedt, R. (2017). *Securitization Theory and Foreign Policy Analysis*. Oxford Research Encyclopedia of Politics. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.479

Strange, S. (1982). Cave! Hic Dragones: A Critique of Regime Analysis. *International Organization*, 36(2, International Regimes), 479–496.

Tewfik, N. (2010, November 26). Cyber Peace Initiative: Egypt's e-Safety Profile – "One Step Further Towards a Safer Online Environment". www.itu.int/dms_pub/itu-d/md/10/wtim8/c/D10-WTIM8-C-0036!!PDF-E.pdf

Touré, H. I. (2011). Cyberspace and the Threat of Cyberwar. In H. I.Touré & Permanent Monitoring Panel on Information Security of the World Federation of Scientists (WFS) (Eds.), *Cyberspace and the Threat of Cyberwar* (pp. 7–13). International Telecommunications Union. www.itu.int/pub/S-GEN-WFS.01-1-2011

Touré, H. I., & Permanent Monitoring Panel on Information Security of the World Federation of Scientists (WFS) (Eds.). (2011). *The Quest for Cyber Peace*. International Telecommunications Union. www.itu.int/pub/S-GEN-WFS.01-1-2011

United Nations Development Program. (1994). Human Development Report. http://hdr.undp.org/en/content/human-development-report-1994

United States Cyber Command. (2018). *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

Virtue Foundation Institute for Innovation and Philanthropy. (n.d.). Egypt's Cyber Peace Initiative. Virtue Foundation. https://virtuefoundation.org/project/cyber-peace-initiative/

Waever, O. (1996). European Security Identities. *Journal of Common Market Studies*, 34(1), 103.

Wegener, H. (2011). A Concept of Peace. In H. I.Touré & Permanent Monitoring Panel on Information Security of the World Federation of Scientists (WFS) (Eds.), *The Quest for Cyber Peace* (pp. 77–85). International Telecommunications Union. www.itu.int/pub/S-GEN-WFS.01-1-2011

Wiener, N. (1988). *The Human Use of Human Beings: Cybernetics and Society*. Da Capo Press.