NEW AMERICA

CYBERSECURITY INITIATIVE

HEATHER M. ROFF

CYBER PEACE

Cybersecurity Through the Lens of Positive Peace

MARCH 2016

About The Author

Heather M. Roff received her Ph.D in Political Science from the University of Colorado at Boulder (2010). She is currently a Senior Research Fellow in the Department of Politics and International Relations at the University of Oxford, a Research Scientist in the Global Security Initiative at Arizona State University, and has held faculty positions at the Korbel School of International Studies at the University of Denver, the University of Waterloo, and the United States Air Force Academy. Her research interests include the law, policy and ethics of emerging military technologies, such as autonomous weapons, artificial intelligence, robotics and cyber, as well as international security and human rights protection. She is author of Global Justice, Kant and the Responsibility to Protect (Routledge 2013), as well as numerous scholarly articles. She blogs for the Huffington Post, the Duck of Minerva, and has written for the Bulletin of the Atomic Scientists, Slate, Defense One, the Wall Street Journal, the National Post and the Globe and Mail. She is currently working on a new monograph on autonomous weapons and the future of war. She is a recognized expert on autonomous weapons and has testified at the United Nations Convention on Certain Conventional Weapons and provided guidance for the International Committee for the Red Cross.

Acknowledgements

Thanks go to David Danks, Michael Gross, Patrick Lin, Bradley Jay Strawser, Fritz Allhoff, Adam Henschke, and Rob Morgus, all of whom have helped me in one way or another to develop thoughts on this paper or through providing thoughtful comments and feedback on earlier drafts. Thanks also go to Peter W. Singer for thinking that there is something interesting to say about philosophy, cyber and Kant.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security Program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work—for the countries, for companies and for individuals.

Find out more at **newamerica.org/cybersecurity-initiative**.

Contents

INTRODUCTION

When one hears the word “cyber,” it is most often paired with one of these words: security, threats, vulnerabilities, exploits, intrusions, attacks, or war. Indeed, the entire landscape of “cyber” is seen as insecure and hostile. Attempting to make sense of this space, authors invoke metaphors like the “Wild West,”[1] or something akin to public health safety concern,[2] or they analogize it as a new type of “public commons”[3] like the sea or space, or as a “state of nature”—and with it a state of war—where no law governs and anarchy reigns.[4] With each metaphor or analogy, scholars and practitioners suggest ways of solving problems related to insecurity. In the case of the Wild West, we need a “sheriff” to impose order. In the public health instance, we need a way of monitoring, responding and quarantining when necessary for the safety of others. And for the public commons, we need a useful way of solving collective action problems and resource distribution and protection. When it comes to war, however, we need strong capabilities to defend our interests and rights.

Cybersecurity on all of these readings, however, becomes defined as vulnerability reduction or elimination. Reducing vulnerabilities is about protecting oneself, building up defenses, mitigating risk, deterring attacks. In short, it is a notion of “security” that is predominantly a Western oriented concept tightly linked to politicization and militarization. As international relations scholar Mohammad Ayoob explains, security is seen as invulnerability, and invulnerability becomes linked to “the primacy of political variables,” for those political variables determine “the degree of security that states and regimes enjoy.”[5] An object, thing, or person only becomes important enough to warrant “security” when the state recognizes one as threatening its security. He notes,

> Different types of vulnerability, including those of the economic and ecological varieties, become integral components of this definition of security only if and when they become acute enough to take on overtly political dimensions and threaten state boundaries, state institutions, or regime survival.[6]

> **Much of the scholarship on cyber peace assumes that it is merely the absence of any hostile actions.**

Ayoob’s insights apply, in many respects, to cybersecurity. The vulnerability of cyberspace, of infrastructures connected through information technologies, the intellectual property of firms, the fragility of a networked economy, are all items that must be addressed under a Comprehensive National Cybersecurity Initiative. As President Obama explains, the United States must view the cyber threat as a threat to national (i.e. state) security, and by doing so: establish a front line of defense, defend against the full spectrum of threats, and strengthen the cybersecurity environment.[7] Where "strengthening" the cybersecurity environment involves "develop[ing] strategies to deter hostile or malicious activity in cyberspace."[8]

Yet security is not merely about militarized defense. Indeed, much work from human security and peace studies takes a different approach to establishing the conditions for security and peace. Thus it is unfortunate that there is a dearth of scholarship and policy attention on the notion of cybersecurity and cyber peace from these other perspectives.

It is my contention that much of the scholarship on cyber peace assumes that it is merely the absence of any hostile actions; it is a "negative" conception of cyber peace. Moreover, due to this negative conception, one that is conceptually coupled with a highly Westernized view of security, the language and posture of cybersecurity becomes militarized and implicitly linked to the state. While it is certainly true that cyber threats to the state do exist, many have not materialized, and the vast majority affect other actors not connected or weakly connected to state security. Viewing cyber peace as negative peace, then, is insufficient to account for the normative and policy changes needed to establish a true sense of cybersecurity.

To do this, I argue that we should instead conceptualize cyber peace in terms of positive peace, and with this step think of cybersecurity through human security aims. Cyber peace ought to be understood in terms of multiple, continuum-like, dimensions. Doing so will enable us to move past circular debates, such as whether we ought to condone "hacking-back," to generate new ideas about the meaning of cybersecurity and peace. The argument proceeds in three sections.

First, I briefly lay out why the cybersecurity as negative peace argument fails. Second, I suggest that we ought to view cybersecurity from the perspectives of human security and positive peace. Human security looks to the individual as the appropriate referent to be secured and not the state. Moreover, following scholar Johan Galtung's peace theory, I argue that cyber peace must be grounded in a conception of positive peace that eliminates structural forms of violence. Viewing security from this perspective shifts our attention to the various objects of security and various structures we require to become secure, and ultimately, more peaceful. Finally, I suggest some ways forward from a policy and behavioral perspective to bring about cyber peace.

> **While it is certainly true that cyber threats to the state do exist, many have not materialized, and the vast majority affect other actors not connected or weakly connected to state security.**

CYBERSECURITY AS A NEGATIVE PEACE

As noted at the outset, much of the common language concerning cybersecurity links it in such a way that "security" is automatically militarized. This militarization takes place at two levels. The first is semantic. We hear that cyber defense is too difficult because one cannot adequately defend all possible attack entry points, and that cyber "favors the offense." If one is not experiencing a cyber attack, if one is not "in hostilities" as it were, then one is at peace. Here, the discourse is to protect our "networks" or "systems" or "critical infrastructure" by keeping others out of them. One accomplishes this by way of deterrence.[9] The deterrence model, for better or worse, gets held up as the ideal strategy. Perhaps this is due to the fact that it is impossible to defend against every attack vector, or perhaps it is a holdover from Cold War thinking. Security, then, is when nothing happens, and this type of semantic sleight of hand lends itself to the negative peace construct. Of course, though, we ignore that something is almost always happening.[10]

The second avenue by which cybersecurity becomes militarized is more subtle. Here we see the discourse of "national security interests" and "threats to national security."[11] Cybersecurity, it is said, is a national security interest. This is certainly true, as most cyber attacks affect individuals, firms, and corporations, and these actors make up the thing we call the "nation."[12] Attacks against these agents are overwhelmingly forms of cybercrime or acts of "hactivism."[13]

> **The trouble with viewing cybersecurity as a national security issue is that the state cannot effectively protect the rights and property of its citizens due to the externality of the threat and a lack of cooperation from other states.**

The problem, however, arises when one asks about what to do about "threats" to "national security." In other words, what is the way to mitigate a national security threat? The principal actor in this equation is the state. As Georg Sørensen explains, "states constitute the primary nexus when it comes to security for individuals and groups."[14] Thus when a threat becomes a "national security threat" the agent or actor to address that threat is traditionally thought of as the state. While some might want to separate state security from national security, the two are conceptually and practically linked.

State security is, to be sure, about maintaining territorial integrity and state sovereignty, the two internationally recognized state rights. This Westphalian construct undergirds the entire international legal system. Yet what we mean by "sovereignty" is by no means clear. Sovereignty is about the ability of a state to govern itself, to be the supreme power, and to be the source of the rule of law. If something threatens a state's capacity to govern, or sets itself up as an equal, there is a problem. What is more, when there are "attacks" against individuals or groups within a state, it has three avenues with which to secure the rights of its citizens.

First, a state can utilize its internal juridical institutions. If a criminal act takes place within its jurisdiction, then it may prosecute and punish wrongdoers. These mechanisms seek to maintain and reestablish justice. Cyber attacks, which are seen as criminal in nature, cannot be said to threaten a state's national security on this account, for if they did, the state would be unable to uphold the rule of law in regards to those criminal acts.

Second, a state can seek cooperation internationally when criminal acts are perpetrated against its citizens but the state lacks jurisdiction to hold those guilty accountable. International law, treaties and cooperative agreements can help a state to seek remedy. In these cases, we begin to see the emergence of something unique: the mapping of state and national security. While we may want to draw a conceptual distinction between the two types of "security," in this instance (and in others) the state acts as the principal agent in seeking redress, and it is also seen as being the victim in need of redress. For example, if a criminal gang in another country perpetrates a cyber attack on a U.S. firm, and the host country refuses to cooperate with the United States in law enforcement activities, we say that both the firm and the United States is wronged. However, the victim state's security is clearly not at risk. If it were, the attack would extend beyond mere criminality to an act of war (or "armed attack" or a "use of force," or something that threatens a state's rights and gives it permission to act in self-defense). Rather, we would say that the victim state may have legitimate cause to initiate countermeasures or retorsions against the other (host) state.

Finally, there is the option of armed hostilities. If a state's rights are violated, and by definition its national security too, then the state has recourse to self-defense. In international law, this is of course when a state has suffered an armed attack, but given that most cyber attacks (that we are publicly aware of) do not rise to the level of an armed attack, then a state cannot say that its rights are being violated.

The trouble with viewing cybersecurity as a national security issue while simultaneously wanting to separate it from state security (and thus militarization), is that the state cannot effectively protect the rights and property of its citizens due to the externality of the threat and a lack of cooperation from other states. The Westphalian model of state as principal assumes that national security boils down to "protecting the components of the state from outside threat and interference. The idea of the state, its institutions, its territory will all be clearly defined and stable in their own right."[15] Indeed, "the link between national security at the level of the state and individual and group security ought to be clear: 'the creation of stronger states is a necessary condition for both individual and national security.'"[16] What is more, permitting individuals within the state to enforce their rights without the sanction of the state generates a tension between the public rule of law and private enforcement.

It is no surprise, then, that many frame the solution to the cybersecurity problem as peace through legal governance. In what became known as the Erice Declaration, the World Federation of Scientists advocated for six principles for "achieving and maintaining cyber stability and peace." All but one look to top-down governance. Yet by framing the issue this way, the Scientists discount problems associated with unjust social structures, as well as the unsatisfactory nature of the entire international legal framework. For governance, international law will prove unsatisfactory because it is either based on custom (that is, what states already do), or consent (through treaties). Problems associated with cybersecurity, however, have not been solved through state practice, and few treaties exist on cybersecurity. Those that do tend to be between like-minded states, not between states that are adversarial at the outset. Moreover, even if states were to agree on a "common code of conduct" and a "harmonized global legal framework" this in no way entails that enforcement of such a code would result. International law is, for all intents and purposes, about self-enforcement.

> **We must coherently link securing cyberspace with securing the state, but also have a broad understanding of the boundaries of cyberspace.**

Even the International Telecommunication Union (ITU) frames the discussion as risk and threat mitigation, where cyber peace is the opposite of cyber war. To achieve cyber peace for them is to institute a "legal framework."[17,18] What is more, the ITU is true to the traditional top-down governance vs. private enforcement model, encouraging "preventive self-defense," and when appropriate "active self-defense," when those governance structures are lacking.[19]

Scott Shackelford's more recent attempt to escape from the top-down governance model falls victim to the same loop, however. Arguing that "polycentric governance" can help to "manage" cyberspace by embracing "self-regulation and bottom up-initiatives," he relies on a conceptual framework that is ill-suited to the cyber problem.[20] While we should praise his insistence that cyber peace would need "multi-stakeholder governance to foster collaboration across multiple regulatory scales, as well as...[emphasizing] targeted measures to address global collective action problems," he fails to see that the "polycentric" approach is only applicable to a very small number of cases related to resource scarcity and public commons.[21] Ostrom's theory of polycentric governance, on which Shackelford builds his argument, assumes a bounded community or "society," identifiable and measurable resource scarcity and individual need, and the power of existing societal norms.[22] Cyberspace, however, lacks all of these features.

Indeed, one of the most problematic features of using the polycentric approach to the problem of generating cyber peace is that there must be a society with existing norms of behavior within the group. Indeed, these existing norms must be constantly reinforced through interpersonal interaction.[23] Human beings are inherently able to learn and adapt to norms of behavior, and norms within a group play powerful roles in shaping individual and group behavior.[24] Yet cyberspace is one of the few areas where anonymity is the rule rather than the exception, and this face-less interaction would frustrate and work at cross purposes to norm formation.[25]

The top-down governance solution posited by the likes of the Scientists, the ITU and other scholars, contributes to the acceptance of cybersecurity as negative peace. To see this more clearly, we need only accept the idea that (cyber)security is gained through dominance, typically due to the establishment of a legitimate monopoly of coercive power to enforce laws internally and the ability to deter external aggression from other states. In the first instance, the state's power keeps order under the rule of law; in the second instance, the state's military and economic power allow it to make war. International law is merely the consent of states acting as they desire to act (consent or practice), and when there is dispute between states, they retain the right of self-defense (i.e. war). Peace boils down to the impoverished idea of "no war"–internally or otherwise.

Yet given that many of the problems associated with cybersecurity have nothing to do with establishing the rule of law, as we already live within states under the rule of law, we are left with a myopic view that to be secure is to ensure enough power and capability to “offset” any potential aggressor or win any confrontation.[26] Security is thought of as a zero-sum game, whereby one agent’s gain is another’s loss. However, due to the nature of cyberspace, the attempt to gain dominance comes at the cost of insecurity for all others. As Myriam Dunn Cavelty explains, “actions geared toward gaining more [cyber] security are (directly and indirectly) to blame for making both the virtual but also, by implication, the real world less and not more secure.”[27] Instead of coming to a more robust understanding of security, and thus peace, one is caught in a vicious cycle of defense, development, exploit, defense, development, exploit. As negative peace is defined as the absence of hostilities, negative cyber peace is the absence of cyber attacks. Cybersecurity becomes conceptually linked with state security in an odd and ill-fitting way, one where any relative gain in security actually becomes an absolute loss overall.

To move forward, I suggest that we think beyond top-down governance and militarized notions of security. We ought to be aware of the unique characteristics of cyberspace and how applying other governance solutions may or may not work given these features. To do this, I argue that we must coherently link securing cyberspace with securing the state, but also have a broad understanding of the boundaries of cyberspace. In short, we need to know what cyberspace is, what objects constitute it, who plays inside of it or acts through it, or who attempts to gain or establish power over others and by which means.

RETHINKING CYBERSECURITY: HUMAN SECURITY AND POSITIVE PEACE

If we are to move past the zero-sum nature of present viewpoints about cybersecurity—and thus cyber peace—we must stop framing the problem as one of cyber insecurity and negative peace. As Alexander Wendt famously noted, “anarchy is what states make of it,” meaning that the concept of anarchy is not a given. How actors construct concepts influences how they will act (and react). Cyber, like anarchy, is a concept. Humans construct it, both physically and conceptually, and so we should think of it in Wendtian terms.

First, we should reframe the cybersecurity discussion along human security lines. As the previous section argued, cybersecurity is beyond state security. It is beyond state security because cyberspace and cyber vulnerabilities challenge the traditional state-as-solution paradigm. Since the state-as-solution paradigm does not work, we ought to question why we tend to attempt to take the state as object of security. I suggest that we ought to rather look to the correct referents of security: individuals. Human security looks to those acts that threaten an individual's safety. As conceptualized in the human security literature, such acts can come from two directions: violent and nonviolent threats.[28] In short, human security is seen as a conflict and development system that endeavors to secure the individual both from fear and from want.

Second, we should also adopt a positive peace framework. Johan Galtung's theory of positive peace engendered the field of "peace and conflict studies" or the study of "conditions of peace work."[29] Galtung set out to understand the conceptual and empirical underpinnings of existing peaceful societies and peacebuilding. His theory, and its subsequent practical adaptation, can be a heuristic with which to view cybersecurity and cyber peace.

From the theoretical standpoint, Galtung's theory of peace is premised on the fact that peace is the absence of violence. However, his construction of violence is nuanced. Instead of violence being a narrow concept of physical or lethal harm, he notes that violence is far more than bodily incapacitation, "or deprivation of health... at the hands of an actor who intends this to be the consequence." To Galtung, "If this were all violence is about, and peace is seen as its negation," then we ignore too many other facets of violence to hold peace up "as an ideal."[30]

On his account, he identifies six dimensions of violence: physical and psychological; negative vs. positive influence; object oriented; direct/personal vs. indirect/structural; intended vs. unintended; and potential vs. latent.[31]

Violence, then, may happen between individuals, between structures and individuals or even between structures. It does not merely focus on a human agent, but also includes objects, as well as physical and psychological states. Thus on Galtung's account, "peace as the absence of violence" comes in two distinct forms: negative peace and positive peace. Negative peace is the absence of direct personal violence. Positive peace, however, is the absence of structural violence. Achieving positive peace, then, is to change the social structure that enables stratification, inequality, and disequilibrium. It is a more robust concept than the absence of individuals directly harming each other physically or mentally.

From a cybersecurity perspective, both the human security and positive peace frameworks give us better purchase on establishing cybersecurity in hopes for cyber peace. This is so because cybersecurity goes beyond and is broader than the notion of violence as bodily harm. Indeed, arguments that posit cyber "war" will never take place because war is fundamentally of "violent character," where violence is "always potentially or actually lethal," has too narrow a focus.[32] Beyond overly restricting what counts as an act of war, it misses the entire scope of coercive and violent acts that can happen to individuals via cyber means.

Thus it makes sense to locate the principal referent of security not with the state, but with those agents who act in and through cyberspace. Indeed, as Dunn Cavelty argues, we ought to instead look to how individual citizens can be secured through the reduction of vulnerabilities in cyberspace.[33] For her, even an over emphasis on securing technological systems or "critical infrastructure" is unbalanced and not a true "public good" because even this vision of cybersecurity "mainly benefits the few and already powerful entities and has no or even negative affects for the rest [of us]."[34]

Taking the human as the value base for all other potential rights claims, means then that we must show how the other objects of security are adequately connected to the human. What might be these secondary objects to secure? We have information/data, property/infrastructure, functionality, and even artificial agents. Each is connected to the human life in some way that gives meaning or value to human life.[35] However, "human life" can be divided into two distinct categories:

that of an individual person and her wellbeing; and that of the society necessary to sustain her human life. This latter category would of course encompass claims the state has to defense against threats towards "national security," but those claims are grounded in individual agent's rights and lives.[36]

Table 1

Galtung's Six Dimensions

Dimension of Violence	Meaning	Example
Physical vs. Psychological Violence	**Physical:** "violence that works on the body"—human beings are hurt somatically to the point of killing. **Psychological:** "violence that works on the soul"—humans are hurt to the extent that there is a decrease in their mental capacities	**Physical:** detention, hurting, maiming, killing **Psychological:** through things like indoctrination, lies, brainwashing, threats.
Negative vs. Positive Influence	**Negative:** influence by punishment **Positive:** influence by reward	**Negative:** Cutting off of hands for stealing **Positive:** Bribery
Object: Truncated Violence	Threats or destruction of objects subclass of violence because of the psychological effects on persons equals violent acts.	Threats of violence; displays of weapons testing; destruction of property
Subject/Agent Acting: direct/personal vs. indirect/structural	**Direct/Personal:** a person commits acts of violence against another. **Indirect/Structural:** no direct person commits acts of violence, but violence is built into the structure (social, institutional, regulatory) as "social injustice;" repression	**Direct/Personal:** Any agent that directly commits a violent act against another **Indirect Structural:** The entire structure begets violence; e.g., Jim Crow laws; slavery; sexism
Intended vs. Unintended	**Intent:** requiring an agent to intend violent act will miss structural violence. Intent matters, but is not a necessary feature for violence.	**Intent:** Requiring "intent" from an individual will make systematic racism not deemed violent. **Unintended:** Requiring no intent would mean including too much in the definition.
Manifest vs. Latent	**Manifest:** violence that is observable (though it need not be directly due to potential violence) **Latent:** Unstable situations where violence may readily and easily come about due to instability.	**Manifest:** Police brutality against African Americans **Latent:** civil resistance movements

Source: Galtung, Johan. "Violence, Peace and Peace Research" Journal of Peace Research, Vol 6:3 (1969):168.

The potential actors that may threaten any one of these entities are: humans, artificial agents, corporations, non-state actors, states, and the structure of cyberspace itself. In short, they are persons and structures. In any one of these potential combinations, insecurity—in and out of cyberspace—can occur due to vulnerabilities in networks, computers, software, hardware, data, the objects they are connected to, or the actions or practices of individuals utilizing any of these objects. Additionally, how we attempt to achieve security in any one of these areas also requires a forward looking attitude towards the very goals of security: peace.

Cyber peace is the end state of cybersecurity. Yet it is not a mere absence of attacks, rather it is a more robust notion about the very conditions for security. Working from Galtung's framework allows us to include more facets of violence, and so it is more amenable to understanding cyber threats. The opposite side of this coin, then, is that his framework can also help us to understand the necessary defenses to make individuals more secure against forms of cyber violence.

Cybersecurity, then, is a continuum. At one end is complete insecurity—a state of war; and at another end is complete security—a state of cyber peace. Along this continuum many different types of violence can occur, to many different subjects and objects. Taking the six dimensions of violence, then we can unpack what they might be in the cyber context. This construct is merely one way of viewing violence through cyber means and in cyberspace, it is not meant to be exhaustive:

Looking then at the various ways one can be subject to violence, and what a cyber counterpart might be, we can begin to identify ways at mitigating or eliminating those forms of violence. We can also see how in the cyber domain negative peace can only be achieved once positive peace has come about. In other words, the structure of cyberspace permits the types of insecurities that allow an agent to exploit a vulnerability in an object that is either directly connected to the human body for life sustaining or life enhancing purposes or exploit a vulnerability in the insecurity of protocols, architectural vulnerabilities in the Internet, programming errors, or by utilizing malicious code to cause psychological violence. Structural violence in cyberspace is a necessary condition for personal cyber violence to exist.

> **Cybersecurity, then, is a continuum. At one end is complete insecurity—a state of war; and at another end is complete security—a state of cyber peace. Along this continuum many different types of violence can occur, to many different subjects and objects.**

Table 2

Dimensions of Cyber Violence

Dimension of Violence	Meaning	Cyber Context
Physical vs. Psychological Violence	**Physical:** "violence that works on the body"—human beings are hurt somatically to the point of killing. **Psychological:** "violence that works on the soul"—humans are hurt to the extent that there is a decrease in their mental capacities	**Physical:** Direct hacking of a device connected to the human body for life sustaining or enhancing purposes (e.g., a pacemaker, a cochlear implant, prosthetic limb, neural implant) **Psychological:** Cybercrime, cyber terrorism, cyberwar,* cyber espionage
Negative vs. Positive Influence	**Negative:** influence by punishment **Positive:** influence by reward	**Negative:** Doxing[37] **Positive:** Bribery
Object: Truncated Violence	Threats or destruction of objects subclass of violence because of the psychological effects on persons equals violent acts.	Destruction or manipulation of data, software, hardware, firmware, or any object regulated by the above.
Subject/Agent Acting: direct/personal vs. indirect/structural	**Direct/Personal:** a person commits acts of violence against another. **Indirect/Structural:** no direct person commits acts of violence, but violence is built into the structure (social, institutional, regulatory) as "social injustice;" repression	**Direct/Personal:** Any agent that directly commits a malicious act using cyber means against another **Indirect Structural:** The entire structure of cyberspace as insecure, and the continued fight by structural agents (states, institutions, corporations) to keep it this way.
Intended vs. Unintended	**Intent:** requiring an agent to intend violent act will miss structural violence. Intent matters, but is not a necessary feature for violence.	**Intent:** Those agents who engage in malicious cyber activities. **Unintended:** The acquiescence to the insecure cyber environment.
Manifest vs. Latent	**Manifest:** violence that is observable (though it need not be directly due to potential violence) **Latent:** Unstable situations where violence may readily and easily come about due to instability.	**Manifest:** Observable intrusion or attack **Latent:** The entire structure of cyberspace

Source: Author.

THE WAY FORWARD

Let's begin with the "wedding cake" approach to cyberspace. Martin Libicki's notion of cyberspace has three distinct "layers:" the physical; the syntactic; and the semantic.[38] The physical layer consists of the physical infrastructure, things such as undersea cables, satellites, one's computer, and even cellphone towers. This forms the bottom layer. The syntactic layer, "contains the instructions that designers and users give the machine and the protocols through which machines interact with one another—device recognition, packet framing, addressing, routing, document formatting, database manipulation, etc."[39] The syntactic layer resides, in a sense, on top of the physical layer. Finally, the semantic layer is the "topmost" layer, and it "contains the information that the machine contains," such as the word document that I am now writing or my email or contacts list.[40] This data, however, only makes sense to us because it is "encoded in natural," as opposed to computer, language. Thus one imagine cyberspace like a wedding cake: the bottom layer consists in physical objects; the second layer in software, internet protocols and the like; and the top layer is the content.[41] Cybersecurity, then, secures each of these layers and the components that comprise them.[42]

Additionally, we need to extend this model to include human (and nonhuman) agents as objects of security connected to cyberspace. While I do not really act "in" cyberspace, I can act "on" the physical layer, such as cutting undersea cables or demobilizing a satellite, and I can act "through" cyberspace. Cyberspace, like a waterway, is merely a route or way for my ideas, intentions, and actions to manifest themselves.[43] Moreover, from the human perspective, cybersecurity is as much a practice—like the oft touted "cyber hygiene" mantra—of individuals interacting with various technologies, ms or data.[44]

Artificial agents, however, can act "in" cyberspace. Depending upon the type of agent, they can learn, be goal oriented, be simple reflex agents that act only on specific met conditions, or model-based agents that can model what the end result might be if the agent acts on specific conditions.[45] They reside in cyberspace, where humans do not. These agents may too be deserving of security. Identifying the scope of cyberspace, as well as the objects and agents to be secured in and through it is vital, for as Betz and Stevens explain, "what we decide to include or exclude from cyberspace has significant implications for the operations of power."[46] This is because even the act of defining what or who is in and what or who is out is itself an act of power. And power always is a relational concept between agents.[47]

Viewing the cyber landscape from this vantage point, we see that it encompasses both vertical as well as horizontal dimensions. Each structure, agent, and content has meaning and is vulnerable in some way, and each must be secured through different means. For instance, securing the physical layer might mean that agents should stop tapping into fiber-optic cables,[48] or routers,[49] or perhaps installing malware on computers.[50] Or to secure the syntactic layer, we need to secure the logical infrastructure, such as the Transport Control Protocol (TCP), the Internet Protocol (IP), the Domain Name System (DNS), the Border Gateway Protocol for routers, Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). While it is beyond the scope of this paper to do an in depth analysis of all of the vulnerabilities with the various existing protocols, some of their widely known problems include: untrustworthy certificate issuing authorities, stealing credentials, spoofing one's location, forging IP packets, outrunning or tricking the DNS to lead to a false webpage, inability to verify updates, or network overloading.[51] For the semantic layer we should look at greater encryption, as well as possess a better ability to track and control the "shed" of our data. For even open source information may leave one vulnerable to social engineering or other types of attacks, such as spear-phishing.

> **By looking at how positive peace is operationalized in the social sciences, we can see which mechanisms support peaceful societies and those that do not.**

Moreover, it is often the case that governments purposefully frustrate the abilities of software and hardware developers to develop secure technologies. Indeed governments actively attempt to break encryption methods,[52] install backdoors,[53] hack cybersecurity software,[54] and tamper with hardware that will corrupt an end product (through the supply chain.)[55] Often, their rationale is based on the national/state-security paradigm outlined before. Individual security must be overridden to protect national security, and the state must do the overriding. Except, it is unclear whether and to what extent any states can actually protect national security given the multitude of players, private industry's monopoly on information communication technologies, and their own poor record of protecting their networks.

While I have suggested that the present focus on top-down international governance is not sufficient as a way forward, this is not to say that there are no useful ideas that we can garner from the traditional top-down approach. By looking at how positive peace is operationalized in the social sciences, we can see which mechanisms support peaceful societies and those that do not. We might then, be able to look for counterparts to these mechanisms in the cyber context. If there is no existing counterpart, then we might desire to stop and ask whether this particular device is a necessary condition for cyber peace. From the policy side of things, it may help to shape behavior or drive various actors towards forming those necessary conditions.

Empirically, we have ample research and evidence about which factors influence peace, as well as make societies more resilient when faced with security challenges.[56] The Institute for Economics and Peace identifies eight "pillars" that affect peace and resilience to violence or grievances in societies.[57] For simplicity, I have restructured their findings into four necessary factors for positive peace: a society, trust, governance, and the free flow of information.

At bottom, one must be able to identify the society in which one interacts. One must be able to identify who is in one's group and who is not. The heterogeneity or homogeneity of the group may affect its cohesion, but of paramount importance is the demarcation of boundaries. When it comes to cyberspace, we may want to demarcate those boundaries as those which map on to sovereign state territories, or we may choose to do so regionally. What is important is that the group has membership features. Much like Ostrom's cases in polycentric governance, one must start from the assumption of a collective.

Second is the topic of trust. One must have trust in one's institutions, such as one's government, one's business environment, and other individuals within one's community for peace to flourish.[58] If one is subjected to rampant corruption, political instability, and no way to resolve one's grievances, then one cannot be said to have much "trust" in anything. The problem for cybersecurity, however, is that we are uncertain what "trust" really means. We can be said to "trust" in infrastructure, personal agents, potential partners, informational sources, or in authorities.[59] Moreover, we smuggle in all different meanings of "trust" when we use this term. For instance we speak about reliability, verifiability, confidence, certainty, cooperation, or particular mental states.[60] Yet we in no way systematically use this term or make explicit what we mean by it when we reference trust and cybersecurity. Moreover, we lack an ability to have any purchase on distrust in cyberspace.[61]

Governance is also a key feature for positive peace, but it is not governance for governance's sake. While I have certainly been critical of previous attempts at defining or outlining cyber peace for their excessive focus on top-down governance, it is still a necessary feature. Yet it must be a socially just form of governance: a society with public, identifiable rules of law, adjudicated by a neutral judge, and enforced equitably across society. Moreover, equality before the law is also crucial for individuals to feel secure in their ability to resolve differences.

Beyond the rule of law, however, corruption and large gaps between the rich and the poor exacerbate the ability for various other institutions and regimes to govern. The inability to attain an education, for instance, or receive adequate nutrition will adversely affect a society's ability to remain peaceful. Moreover, the free flow of information, such as freedom of the press or an open Internet, is positively associated with more peaceful societies.

The top-down approach to peace is only one aspect, however. All agents who act in and through cyberspace can do their part to help make it, and the individuals affected by it, secure. While states may be able to negotiate treaties, enact law, or even bolster particular technologies, firms and individuals also play an important part. The creation of new and more secure protocols, for example, would help in many areas, or the creation of international nongovernmental organizations devoted to ameliorating causes of structural cyber violence, would also be a way forward.

Thus, mapping the positive peace framework onto cybersecurity, and thus cyber peace, is no easy task. There are many difficulties that must be addressed; however, if what we know—both theoretically and empirically—about peace holds, then we ought to utilize these findings in our prescriptions for achieving cyber peace. Difficulties notwithstanding, the ideal is still something we can attempt to achieve.

> **The problem for cybersecurity is that we are uncertain what "trust" really means...We in no way systematically use this term or make explicit what we mean by it.**

CONCLUSION

Using the notion of "security," which is predominantly Western-oriented and coupled with politicization and militarization, is unhelpful to achieve cybersecurity. Cybersecurity discourse as a national security threat, whereby the state is the agent who addresses this threat is false. While there are certainly vulnerabilities abound, the top-down, Westphalian model, cannot fully help us here. Indeed, it risks privileging particular policy models, discourses, resource allocation, and behaviors. In so doing, it fails to address the plurality of vulnerabilities and thus vulnerable individuals.

Instead of relying on the negative peace concept of cybersecurity, where security is the mere absence of attack (or in Galtung's words "interpersonal violence"), I argue that we should look to the two different frameworks to guide our understanding of cybersecurity: human security and positive peace. The human security framework rejects taking the state as the object of security and instead locates security with the individual person. Cybersecurity is yet another dimension of securing the individual.

Moreover, part of securing the individual is understanding what makes her insecure. It is here, with Galtung's work on peace, that we can utilize his discussion of interpersonal and structural violence. Using Galtung's theory as a foil for cybersecurity issues, we can begin to map out how to achieve positive cyber peace. By achieving positive cyber peace and eliminating forms of structural cyber violence, we will remedy many of the problems seen as intractable today. Thus instead of finding yet another analogy for what cyberspace is "like," or debating about how far individuals or firms can "hack back," we ought to examine the very structure of cyberspace, the types of violence that can occur within and through cyberspace, and begin to address those problems at the source.

Cyber peace is achievable. There are technological solutions to particular problems, for we created the technology. Moreover, there are diplomatic solutions to particular problems, if international actors would see past narrow self-interest. Finally, there are human solutions to human problems. Peace is not an unattainable goal; it is rather a negotiation between the rights, lives, wellbeing and security of each individual in relation to all others. It is not a "hard won battle," for then it would be an imposition of another's will upon someone else, and this is not peace but victory. Cybersecurity and cyber peace are two sides of the same coin, and as such must be sought together.

Notes

[1] Shahani, Aarti. “Not Everyone Agrees On How To Tame Obama’s Cyber ‘Wild West.’” NPR. February 14, 2015. http://www.npr.org/2015/02/14/386227403/not-everyone-agrees-on-how-to-tame-obamas-cyber-wild-west

[2] Lapointe, Adriane. “When Good Metaphors Go Bad: The Metaphoric ‘Branding’ of Cyberspace.” Center for Strategic & International Studies (Sept. 2011). http://csis.org/files/publication/110923_Cyber_Metaphor.pdf.

[3] Hurwitz, Roger. “Depleted Trust in the Cyber Commons” Strategic Studies Quarterly (Fall 2012):20-45. http://www.au.af.mil/au/ssq/2012/fall/hurwitz.pdf

[4] Hobbes, Thomas, and Edwin Curley. Leviathan: with selected variants from the Latin edition of 1668. Vol. 8348. Hackett Publishing, 1994.

[5] Ayoob, Mohammed. Book Reviews, World Politics, Vol. 43, No. 2 (Jan. 1991): 259

[6] Ibid.

[7] United States Foreign Policy: The Comprehensive National Cybersecurity Initiative. The White House. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

[8] Ibid.

[9] Maucione, Scott. “Lawmakers Want DoD Cyber Policy to Deter Attacks, Retaliate.” Federal News Radio. September 29, 2015. http://federalnewsradio.com/cybersecurity/2015/09/lawmakers-want-defense-cyber-policy-deter-attacks-retaliate/

[10] Norse. “Norse Attack Map.” http://map.norsecorp.com

[11] Gertz, Bill. “Deterrents against cyberattacks outlined; China, Russia, North Korea links confirmed.” Washington Times. September 30, 2015. http://www.washingtontimes.com/news/2015/sep/30/inside-the-ring-robert-work-says-pentagon-plans-to/?page=all#pagebreak

[12] While properly a nation is an ethnically homogenous group of individuals, and so properly there are very few “nation states” in the world, colloquially many people identify the “nation” as that entity that is made up of individuals, groups, and corporations and is governed by the “state.”

[13] “2015 Cyber Attacks Timelines Master Index.” Hackmageddon. http://www.hackmageddon.com/2015-cyber-attacks-timeline-master-index/

[14] Sørensen, Georg. “Individual Security and National Security: The State Remains the Principal Problem.” Security Dialogue 27, no. 4 (1996): p. 374.

[15] Ibid, 375.

[16] Ibid, 375. Sørensen is here citing Barry Buzan. See Buzan, Barry. People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era (Hemel Hempstead: Harvester, 1991).

[17] Touré, Hamadoun I. “The Quest for Cyber Peace” International Telecommunication Union (2011): 81. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf

[18] “Cyber peace should, therefore, be the quest of all nations. The advantages of cyber peace far outweigh the destructive consequences of cyber conflict.” Ibid, 5.

[19] Ibid, 84-85.

[20] Shackelford, op. cit., 101.

[21] Ibid, 101.

[22] Ostrom, Elinor. Governing the Commons: The Evolution of Institutions for Collective Action

(Cambridge University Press, 1990). Ostrom's examples, such as fisheries, pastures, and are circumscribed for methodological clarity. Indeed, she says that "I focus entirely on small scale CPRs [Common Public Resources], where the CPR is itself located within one country and the number of individuals affected varies from 50-15,000 persons who are heavily dependent on the CPR for economic returns" (26). Moreover, the limits on the CPRs chosen are also that they are "(1) renewable vs. nonrenewable resources, (2) situations where substantial scarcity exists, rather than abundance, and (3) situations in which the users can substantially harm one another, but not situations in which participants can produce major external harm for others" (26).

[23] Ostrom, Elinor. "Collective Action and the Evolution of Social Norms" Journal of Natural Resources Policy Research, Vol. 6:4 (2014): 235-252.

[24] Foucault, Michel. "The History of Sexuality: Volume I-An Introduction." (1978).

[25] Even absent the problems of appropriating the polycentric approach to cyber, Shackelford's project ultimately collapses back to the concept of rule-of-law governance and negative peace. Despite his claims to the contrary. Shackeford, op. cit., 357; 363; 365.

[26] Work, Bob. "The Third U.S. Offset Strategy and its Implications for Partners and Allies." Delivered at the Willard Hotel, Washington, D.C. January 28, 2015. http://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies

[27] Dunn Cavelty, op. cit. p. 702. Italics in original.

[28] Ibid, 233-242.

[29] Galtung, Johan. Peace by Peaceful Means: Peace Conflict, Development and Civilization. (Sage Publications, 1996): 9.

[30] Galtung, Johan. "Violence, Peace and Peace Research" Journal of Peace Research, Vol 6:3 (1969):168.

[31] Ibid.

[32] Rid op. cit., p. 12

[33] Dunn Cavelty, op. cit. 711-712.

[34] Ibid, 707.

[35] Dunn Cavelty tries to make a similar move in her treatment of cybersecurity and human security. She invokes Floridi's notion of "information ethics" where "all informational objects are in principle worth of ethical consideration" (712). However, while she would like to use this approach, she does not explain further how the connection to the human plays out.

[36] McMahan, Jeff. Killing in War (Oxford: Oxford University Press, 2009).

[37] Doxing is the malicious practice of publishing someone's private or identifying information about a particular individual on the Internet.

[38] Libicki, Martin. Cyberdeterrence and Cyberwar (Santa Monica: RAND, 2009): 12. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

[39] Ibid. 12.

[40] Ibid, 12.

[41] Some scholars like Schackelford, call the second layer the "application layer" and the third layer the "content layer." Where the notion of the content layer gets tricky however, is in how threats to the content layer include social engineering attacks, like spear phishing. Here one can identify potential targets—data on a system of individual X—but to get that data one has to know something about an agent and not the data. It is a mixing of the layer with an actor. Shackelford, Scott J. Managing Cyber Attacks in International Law, Business, and

Relations: In Search of Cyber Peace. Cambridge University Press, 2014.

42 Bayuk et. al, define cyberspace as “the global collection of electronic circuits that allow people to share information without physical connectivity” (Bayuk et. al, 245). But this definition fails in that it downplays the physical side of cyberspace. Cyberspace has to be physical and connected through physical objects because all of its components are physical. While some might think that my wireless router enables information to flow to my computer sans physical connectivity, it misses the infrastructure that puts into place the ability for my computer to sense the router, send signals to it, receive signals, and how the router is in fact physically connected to various infrastructures. Others, like Thomas Rid, fail to even provide a definition of cyberspace, claiming instead that the term is “a now-common metaphor to describe the widening reaches of the Internet” (Rid, 166). The Internet is only one aspect of cyberspace. For instance, I may have a network in my home that is not connected to the Internet. Does that mean that this network, which only connects several devices, such as my computer and a printer in a small confined geographic location, is not part of cyberspace? Clearly not, for there is cyberspace connecting them that has nothing to do with the Internet. Bayuk, Jennifer L., Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, and Joseph Weiss. Cyber security policy guidebook. John Wiley & Sons, 2012. Rid, Thomas. Cyber war will not take place. Oxford University Press, 2013. Koepsell, David R. The Ontology of Cyberspace: Philosophy, Law, and the Future of Intellectual Property (Open Court Press, 2003): 124.

43 Luciano Floridi believes that our data is an extension of ourselves. However, I cannot enter discussion of this here. Cf. Floridi, Luciano. The Fourth Revolution: How the Infosphere is Reshaping Human Reality, (Oxford University Press, 2014).

44 Dunn Cavelty, M. “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities” Science and Engineering Ethics, 20 (2014): 702.

45 Russell, Stuart and Peter Norvig. Artificial Intelligence: A Modern Approach, 2nd Ed. (Prentice Hall, 2003).

46 Betz, David J. and Tim Stevens. Cyberspace and the State: Toward a Strategy for Cyber-Power (Routledge, 2011): 36.

47 Baldwin, David. Economic Statecraft (Princeton University Press, 1985).

48 Khazan, Olga. “The Creepy, Long-Standing Practice of Undersea Cable Tapping” The Atlantic, July 16, 2013. http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/

49 Zetter, Kim. “NSA Laughs at PCS, Prefers Hacking Routers and Switches” Wired Magazine, September 4, 2013. http://www.wired.com/2013/09/nsa-router-hacking/

50 Appelbaum, Jacob and Judith Horchert and Christian Stöcker. “Shopping for Spy Gear: Catalog Advertises NSA Toolbox” Der Spiegel, December 29, 2013. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

51 For a good discussion of the various vulnerabilities see: Shackelford, op. cit. chapter 3, and Andreas, Jason and Steve Winterfeld. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (Syngress Press, 2011).

52 Ball, James and Julian Borger and Glenn Greenwald. “Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security” The Guardian, September 6, 2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

53 McCarthy, Tom. “NSA Director Defends Plan to Maintain ‘Backdoors’ into Technology Companies”

The Guardian, February 23, 2015. http://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies

[54] Zetter, Kim. "U.S. and British Spies Targeted Antivirus Companies" Wired Magazine, June 22, 2015. http://www.wired.com/2015/06/us-british-spies-targeted-antivirus-companies/

[55] Gorman, Siobhan. "U.S. Report to Warn on Cyberattack Threat from China" The Wall Street Journal, March 8, 2012. http://www.wsj.com/articles/SB10001424052970203961204577267923890777392. Adl-Tabatabai, Sean. "NSA and GCHQ Have Backdoor Access to Millions of SIM Cards, Snowden Leak" YourNewsWire.com, February 20, 2015. http://yournewswire.com/nsa-and-gchq-have-backdoor-access-to-millions-of-sim-cards-snowden-leak/

[56] The Global Peace Index finds that in countries with low levels of positive peace, 91 percent of major resistance campaigns were primarily violent, lasted longer and have more radical aims, as opposed to countries with high levels of positive peace where 51 percent were nonviolent. Moreover, countries with high positive peace scores have historically fewer civil resistance movements overall. Institute for Economics and Peace, op. cit., 91.

[57] The Global Peace Index identifies: a well-functioning government, sound business environment, equitable distribution of resources, acceptance of the rights of others, good relations with neighbors, free flow of information, high levels of human capital, and low levels of corruption. These are all measured in different ways to form the data from which they draw. However, it is apparent that a well functioning government is one form of governance, and that governance is to distribute resources equitably, moreover "trust" is seen in almost every measure, from trust in institutions, business, other people, states, and the like. All of this, moreover, is premised on a unitary model: society. Without this, none of the other pillars would stand.

[58] Ibid.

[59] Falcone, Rino, Munindar Singh, Yao-Hua Tan. "Bringing Together Humans and Artificial Agents in Cyber-Societies" in Rino Falcone, Munindar Singh, Yao-Hua Tan (Eds.) Trust in Cyber-Societies: Integrating the Human and Artificial Perspectives (Springer, 2001): 2.

[60] I thank David Danks for helping me with the various categories of trust in machine learning and psychological areas.

[61] McKnight, Harrison D. and Norman L. Chervany. "Trust and Distrust Definitions: One Bite at at Time" in Rino Falcone, Munindar Singh, Yao-Hua Tan (Eds.) Trust in Cyber-Societies: Integrating the Human and Artificial Perspectives (Springer, 2001):27-54.

All photos in this report are supplied by, and licensed to, **Shutterstock.com** unless otherwise stated.