Chapter 13
The Security Culture of a Global and Multileveled Cybersecurity

Zenonas Tziarras

Abstract This paper seeks to argue for the development of a global and multileveled management of cybersecurity. To do so we first define cybersecurity by situating it within the broader framework of the changing concept of security. To this end we look at the evolution of the security concept, mainly since the end of the Cold War, and its relationship to cybersecurity in today's global affairs. Then we identify the referent object of security, the importance of cyberthreats, and the need for a multileveled management of cybersecurity and cyberthreats. For such a management to be possible and effective, this paper argues that the development of a security culture of multileveled cybersecurity is necessary. To demonstrate how that could happen policy-wise, we briefly look at the current state of international cooperation on cybersecurity and put forward the idea of a framework of multileveled and global cooperation based on a strategy aiming at developing a global security culture of cybersecurity. Moreover, it is suggested that the development of this security culture should be gradual, based on horizontal and vertical multileveled cooperation, by starting with "low-politics" or non-politically sensitive cybersecurity matters. Such a multileveled framework of cybersecurity, with successful communication lines on and between all levels, may even provide a good platform for cooperation in other domains as well.

Keywords Cybersecurity • Cyberspace • Cyber-Defense • Security culture • Strategy

Z. Tziarras (✉)
Department of Politics and International Studies, University of Warwick,
Coventry CV4 7AL, UK
e-mail: z.tziarras@warwick.ac.uk; ztziarras@strategyinternational.org

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_13, © Springer Science+Business Media New York 2014

13.1 Introduction

Technology has become the main driver of globalization. Indeed, we could speak of economic or cultural globalization but the reason why national economies and cultures have been integrating more and more is not free trade or multiculturalism-oriented policies. Time and space have shrunk because of the evolution of technology and everything that comes with it. Likewise, every means of transportation has been a product of technological advancement. Today, the rapid increase in global human interactions, financial transactions, international cooperation, and the increasing importance of non-state actors in global affairs, has become possible and easy through the use of information or cyber technology. In other words, the emergence of cyberspace has created a whole new world and dimension which is nonetheless interlinked with practices and actors of everyday life. In this context, Anthony Giddens's argument that globalization is "the intensification of worldwide social relations that link distant localities in a way that local happenings are shaped by events occurring many miles away and vice versa," becomes even more relevant almost two and a half decades later.[1]

But how should we then approach security and cybersecurity thus dealing with cyberthreats more effectively? This paper seeks to argue for the development of a global multileveled management of cybersecurity. To do so we first need to define cybersecurity by situating it within the broader framework of the changing concept of security. To this end we look at the evolution of the security concept mainly since the end of the Cold War and its relationship to cybersecurity in today's global affairs. Then we identify the referent object of security, the importance of cyberthreats, and the need for a multileveled management of cybersecurity and cyberthreats. For such a management to be possible and effective this paper advocates for the development of a security culture of multileveled cybersecurity. To demonstrate how that could happen policy-wise we briefly look at the current state of international cooperation on cybersecurity and put forward the idea of a framework of multileveled and global cooperation based on a strategy aiming at developing a global security culture of cybersecurity.

13.2 On (Cyber) Security

Admittedly, security is an essential element in everyone's life. Given the fact that security and insecurity affect people's lives every day, one could easily comprehend the extent to which they matter in global politics and international relations. However, the end of the Cold War complicated the discussion about the concept of security as it created a new global security environment which has been constantly

[1] Anthony Giddens, *The Consequences of Modernity* (Cambridge: Polity Press, 1990). 64.

changing since then. Thus, security has become a contested concept with definitions ranging from national and international security to human security.

The term "International Security" first appeared during the Cold War and used to have a much narrower meaning than it does today.[2] One could easily understand why during the Cold War the prevailing concept of (International) Security was "strategy." Not only was security understood within the framework of strategy, but that turned out to be the concept on which the theory of (neo) Realism was based. Neorealism, and therefore security, was used to be expressed through four key elements: "state, strategy, science and the status quo;" these are still some of the main characteristics of Realist theory.[3] This concept of security and the theory of Realism were clearly relevant during the Cold War while one could argue that the global political realities of that period could only be understood through the 'Realist' concept of International Security. The major competition between the two superpowers of the international system, the arms race, and the fear of a potential nuclear war were some of the main features that characterized the Cold War and influenced the foreign policy-making of the USA, the Soviet Union, and their allies. In that sense, the most cherished value during the Cold War was—national and international—peace as it was the most threatened value.

As noted earlier, the prevalent understanding of security during the Cold War was seriously challenged after the end of bipolarity. The collapse of the Soviet Union gave an end to the narrow idea of strategy and military as the main security concept and made room for new threats to enter the debate of how security should be addressed and conceptualized. A small taste of how broad this discussion became is not only the inclusion of new threats that emerged in the post-Cold War era but also the emergence of a debate about whether security is a sub-field of International Relations and vice versa.[4] Regardless of the relationship between Security Studies and International Relations, strategy is today perceived only as a sub-field of security and not as a synonym to it. What broadened the field of security after the Cold War were factors that concern demilitarization, the spread of democracy, the evolution of technology and communications and, therefore, the 'increasing globalization'.[5]

This essay adopts Williams's proposed understanding of security as the most relevant and valid one: "security is most commonly associated with the alleviation of threats to cherished values; especially those which, if left unchecked, threaten the survival of a particular referent object in the near future."[6] We also accept that given

[2] Stephen M. Walt, "The Renaissance of Security Studies," *International Studies Quarterly* 35, no. 2 (1991): 213–14.

[3] Paul D. Williams, "Security Studies: An Introduction," in *Security Studies*: *an Introduction* ed. Paul D. Williams (New York: Routledge, 2010), 3.

[4] Terry Terriff et al., *Security Studies Today* (Cambridge: Polity, 2006). 12.

[5] Iztok Prezelj, "Challenges in Conceptualizing and Providing Human Security," *HUMSEC Journal* no. 2 (2008): 2.

[6] Williams, "Security Studies: An Introduction," 5. Williams' definitions draws upon similar previous definitions such as Wolfers'; see, Arnold Wolfers, "National Security' as an Ambiguous Symbol," *Political Science Quarterly* 67, no. 4 (1952): 485.

the changes in the international system after the Cold War, a wider security agenda is justified and rather helpful to our understanding of new threats, such as cyberthreats; yet the military and the 'Realist' dimensions of security should not be entirely supplanted. Drawing upon the literature on security studies there are certain questions that we could ask in order to narrow down what the "cherished values" and "threats" are, as well as how to "alleviate" these threats. These could be concisely expressed in the following four questions[7]:

(a) What is the referent object of security?
(b) What is the security threat?
(c) Who is responsible for providing the security?
(d) Which are the best ways to provide security?

Answering these questions can help us understand the importance of cybersecurity and the ways in which a security culture of multileveled cybersecurity could be formulated.

13.2.1 Referent Object(s) and Cherished Values

The referent object of security during the Cold War, as we have already seen, was the state. In other words the "state" was the object that was primarily threatened and had to be secured. Later, within the framework of the widening security agenda, the security of the individual and its well-being had become increasingly important. Further, the significance of the strong relationship between the state and the individual has been underpinned by a large body of literature creating a whole new dimension of security and human security in particular.[8] As such it has been argued that the security of individuals is directly linked to national security and therefore it should be prioritized "since without reference to individual humans, security makes no sense."[9] Emphasis has been given on many other referent objects as well; after all, as Baldwing states, "the choice depends on the particular research question to be addressed"[10] and, as one could argue, on who sets the security agenda. What would then the referent object of a multileveled cybersecurity be?

[7] Wolfers, "'National Security' as an Ambiguous Symbol."; David A. Baldwin, "The Concept of Security," *Review of International Studies* 23(1997): 13–17; Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2010). 10–13; Williams, "Security Studies: An Introduction," 5–10.

[8] Richard H. Ullman, "Redefining Security," *International Security* 8, no. 1 (1983): 130–31.

[9] Williams, "Security Studies: An Introduction," 7. Williams cites, Ken Booth, "Security and Emancipation," *Review of International Studies* 17, no. 4 (1991); and, Bill McSweeney, *Security, Identity and Interests*: *A Sociology of International Relations* (Cambridge: Cambridge University Press, 1999). 45–68.

[10] Baldwin, "The Concept of Security," 13.

We argue here that in order for a security culture of multileveled cybersecurity to be possible, multiple referent objects need to be taken into account. In this context cyber(in)security should be addressed at the individual/societal, national/state, regional, and international level. All these—often interlinked—levels constitute our security referent objects. As cyberspace has created a "parallel universe" in which all these levels coexist at all times and in relation to all aspects of social, political and economic life, then, it is against this background that cyber insecurity should be addressed. At this point one could argue that Nye may indeed be right in that "cyberspace is not a [global] commons like the high seas because parts of it are under sovereign control."[11] But in a globalized world, where there is increasing interconnectedness on every level, a legitimate argument could be made that cyberspace should become a single—though multileveled—referent object. Accordingly, cyberspace should be protected on every level as the cherished values (interests) at stake are not only individual but collective as well. This levels-of-analysis approach is similar to that of Choucri: drawing upon the "fourth image"/global level put forward by Robert North,[12] Choucri suggests that "Cyberspace allows both the constrains and the opportunities rooted at the local level to extend within and across levels of analysis nearly unimpeded and to circulate through the global system."[13]

13.2.2 Cybersecurity Threat(s)

Having established the referent object of (cyber) security and its relationship to cherished values, the next step is to decide what constitutes a threat. According to the referent object (e.g., states, individuals, social groups), cherished values vary[14] and, therefore, we should decide which of these "values are threatened and by what or whom."[15] In other words, security threats are—and arguably should be—mainly perceived according to what one considers the referent object to be. It should also be kept in mind that (human) "security is directly related to the concept of international peace and security;"[16] as such, some threat agendas are more important than others in terms of their political significance, or depending on the significance of the one who sets the agenda.[17] For example, the threat agenda of the UN High-Level Panel on Threats, Challenges and Change is probably more significant than any other

[11] Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011). 143.

[12] Robert C. North, *War*, *Peace*, *Survival*: *Global Politics and Conceptual Synthesis* (Boulder, CO: Westview Press, 1990).

[13] Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge: The MIT Press, 2012). 46, 44–48.

[14] Baldwin, "The Concept of Security," 13–14.

[15] Williams, "Security Studies: An Introduction," 8.

[16] Prezelj, "Challenges in Conceptualizing and Providing Human Security," 9.

[17] Williams, "Security Studies: An Introduction," 8.

agenda in international politics.[18] Also the threats presented in it are undoubtedly the ones that the international community will care the most about—albeit their ranking is debatable.

Importantly enough cyberthreats were not included in the list of the 2004 UN High-Level Panel, although one could categorize them under "Terrorism." Yet cyberthreats vary in nature and cannot be limited to cyberterrorism. Choucri identifies "three broad types of cyber contentions and conflicts: contentions over the architecture of the internet and the management of cyberspace, conflicts in the pursuit of political advantage and economic gain (legal and illegal), and cyber threats to national security." Under these broad types fall, for example, cyberthreats to infrastructure (e.g., communications and information), to national security, and political or commercial cyberthreats to individuals, firms, governments, and states.[19] Nye focuses on national security and sees four main cyberthreats: "economic espionage, crime, cyberwar, and cyberterrorism."[20] On the other hand, Rosenfield argues that "cybernetic warfare and the threat it poses to modern society" needs to be redefined. He goes on to emphasize that the "disruptive potential of cybernetic attacks" is more threatening than their "destructive potential" while he divides cyberattacks into "two principal forms: those targeting data and those targeting control systems." Rosenfield adds that most cyberattacks are related to data targeting, "from online credit-card fraud to Web site vandalism to large-scale denial-of-service (DOS) assaults."[21]

It is clear that every day-life practices are not only as threatened as national security but perhaps even more so. In this context the various types of cyber-threats could directly or indirectly affect multiple aspects of social, political, and economic life through the "disruption" or "destruction" of critical infrastructures. A paper of the European Commission, in 2005, clearly stated that "Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments."[22] From that perspective cyber-threats are directly associated with human, national, international and, therefore, global (in) security as they are essentially converted into other types of threats once they take place; such threats include economic, food, health, environmental, community, personal, and demographic threats, among others.[23] In Davies's words "The informa-

[18] Panyarachun A et al., "A More Secure World: Our Shared Responsibility," (High-Level Panel on Threats, Challenges and Change: United Nations, 2004), 21–59. The ten main security threats identified were: poverty, infectious disease, environmental degradation, interstate war, civil war, genocide, other—war related—atrocities, weapons of mass destruction, terrorism, and transnational organized crime.

[19] Choucri, *Cyberpolitics in International Relations*: 126, 25–53.

[20] Nye, *The Future of Power*: 144.

[21] Daniel K. Rosenfield, "Rethinking Cyber War," *Critical Review* 21, no. 1 (2009): 77–78.

[22] EC, "Green Paper: On a European Programme for Critical Infrastructure Protection," *Commission of the European Communities* COM(2005) 576(2005): 20.

[23] Prezelj, "Challenges in Conceptualizing and Providing Human Security," 8, 17.

tion technology infrastructure is at risk not only from disruptions and intrusions, but also from serious attacks."[24] Such attacks, intrusions and disruptions could have a great negative and costly impact on areas such as international banking, military systems, governmental systems, local businesses, communications, transportation, and many others. It is thus clear that cybersecurity is of the essence for literally everyone—even if they do not own a personal computer—as the cherished values of any given referent object are potentially under threat.

13.2.3 Security Provider(s) and Policies

The last two questions to be answered are rather interlinked as the ways (policies) of providing security are not only directly related to the referent object and the security threats but to the security provider as well. Security providers may vary in size, influence and importance, especially within the framework of international relations and global politics. In that light, the security provider could be the state, an international organization, a non-state actor or even individuals with certain power capabilities and in certain situations.[25] To be sure, depending on the security threat, some security providers are more capable of managing certain threats than others. On the other hand, a particular agent might not care for a security threat as much as another agent would[26]; therefore, as a broadened threat agenda becomes gradually necessary the need for different actors or agents to address particular threats arises as well.

As today's threats are more—and in many ways different—than the traditional ones, security providers as well as the policies and mechanisms established to face those threats should be adjusted accordingly. Additionally, the increasingly globalized nature and interconnectedness of the international system, challenges state sovereignty and transnationalizes threats thus rendering the adoption of common (international) policies necessary. As Aravena puts it:

> coordinating policies, establishing regulations and generating international regimes based on shared values are essential points in designing a new international system for the twenty-first century. Only the ability to act jointly will enable states to recover their abilities to generate, together with other actors, a legitimate order capable of building a world free from threats and fear.[27]

It is true that such an approach is embedded in a neoliberal understanding of world politics and it could thus be criticized on many levels by advocates of different approaches. For example, given that most of the times security policies depend on who the security provider is, particular threats which are considered to be important to certain individuals, states, or non-state actors, might be given less attention than

[24] Barry Davies, *Terrorism*: *Inside a World Phenomenon* (London: Virgin Books, 2003). 253.

[25] Williams, "Security Studies: An Introduction," 9–10.

[26] Baldwin, "The Concept of Security," 16.

[27] Francisco R. Aravena, "Human Security: Emerging Concept of Security in the Twenty-First Century," *Human Security in Latin America* 2, no. 1 (2002): 7.

those actors would like if the only security agents were the international institutions. But in the case of a multileveled cybersecurity the logic regarding the security provider is different in that it is not limited to national or international policies of security management. Rather, the aim is to incorporate all concerned levels and actors into a common and collective multileveled framework, through which they would be able to produce multileveled, and globally oriented, policies of cybersecurity and cyber-defense. What are the implications of these conclusions for our definition of cyber-security and how could we go about establishing such a framework?

Cybersecurity has been defined as "a state's ability to protect itself and its institutions against threats, espionage, sabotage, crime and fraud, identity theft, and other precedents, and other destructive e-interactions and e-transactions."[28] Based on what we have examined so far and considering our aim of putting forward a multileveled cybersecurity, this definition seems rather narrow. In the context of this essay cybersecurity is the collective ability of individual, non-state, national, and international actors to protect each one of these levels against any type of disruptive or destructive cyberthreats, through a multileveled framework of cooperation, to the end of providing a secure and stable globally managed cyberspace. It is proposed that in order to accomplish the establishment of such a framework of multileveled cybersecurity, a certain security culture needs to be developed. The way in which we could develop a security culture that would correspond adequately to the challenge of such an understanding of cybersecurity is elaborated below.

13.3 International Cybersecurity Cooperation and Capabilities

Although the literature on international cooperation and institutionalism is extensive, there have not been made many concise efforts to approach international cooperation on cybersecurity. At the same time, whereas there is abundance of political and legal frameworks on perhaps every aspect of human life, the agreements and treaties with regard to cyberspace, and cybersecurity more specifically, are limited.[29] The few such treaties and agreements include the 2001 Convention on Cybercrime, by the Council of Europe, and the 2012 World Conference on Information Technology (WCIT-12). The latter was meant to revise the 1988 International Telecommunications Regulations treaty, and was led by the United Nations International Telecommunication Union (ITU).[30] Although WCIT-12 was an important step toward an international framework on cyberspace, the USA and other allies did not sign the final document over fears that governments would acquire control

[28] Choucri, *Cyberpolitics in International Relations*: 39.

[29] See, for example, Rex Hughes's call for a treaty on cyberspace, Rex Hughes, "A Treaty for Cyberspace," *international Affairs* 86, no. 2 (2010).

[30] Choucri, *Cyberpolitics in International Relations*: 168.

of the Internet. Eighty-nine other nations signed the final document[31] of the Conference but it has been argued that the refusal of many important Western states (e.g., the USA, Canada, and the UK) limit to a great extent the applicability of the agreed additions and revisions in the Convention of the ITU.[32]

Apart from international agreements and treaties, a number of various entities play a role in the "international institutional security ecosystem," at the international, national, and local level—including the private sector and nonprofit entities.[33] The North Atlantic Treaty Organization (NATO) and the European Union (EU) are two of the most important entities as they combine the local and regional levels while also having proceeded to the adoption of cybersecurity and cyber-defense policies.

NATO's commitment to the development of cyber-defense was evident as early as 2002 during the Prague Summit. Consequent Summits emphasized even more on the notion of a common cyber-defense while the new Strategic Concept of 2010 states that the Organization needs to have the necessary capabilities "to prevent, detect, defend against and recover from cyberattacks" as well as "enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations."[34] NATO's Cyber Defense Management Board, which has supplanted Cyber Defense Management Authority, makes a bold move toward bringing together key actors and centralizing the capabilities of the alliance with regard to cybersecurity and cyber-defense. At the same time, the Organization's cooperation with non-NATO nations in recent years has expanded its capabilities and cybersecurity management potentials.[35]

For its part, the EU has made its own efforts for the development of cybersecurity policies, most notably, by publishing its cybersecurity strategy, early in 2013. The five priorities of "Cyber Security of the European Union" are: the achievement of cyber resilience, the reduction of cybercrime, the development of a cyber-defense policy within the framework of the Common Security and Defense Policy (CSDP),

[31] ITU, *Final Acts*: *World Conference on International Communication* (Dubai: International Telecommunications Union, 2012).

[32] Cyrus Farivar, "The UN's telecom conference is finally over. Who Won? Nobody Knows.," ars technica, http://arstechnica.com/tech-policy/2012/12/the-uns-telecom-conference-is-finally-over-who-won-nobody-knows/.

[33] See a list of major entities at all these levels in, Choucri, *Cyberpolitics in International Relations*: 161–66.

[34] NATO, *Active Engagement*, *Modern Defence. Strategic Concept for the Defence and Security of the Members of th North Atlantic Treaty Organization* (Lisbon: NATO, 2010). 16–17; Marios P. Efthymiopoulos, "NATO's Security Operations in Electronic Warfare: the Policy of Cyber-Defence and the Alliance's new Strategic Concept," *Journal of Information Warfare* 8, no. 3 (2009): 64–66.

[35] Victoria Ekstedt, Tom Parkhouse, and Dave Clemente, "Commitments, Mechanisms & Governance," in *National Cyber Security*: *Framework Manual*, ed. Alexander Klimburg (Tallinn: NATO CCD COE Publication, 2012), 185; Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," *Atlantic Council* IssueBrief(2011): 4.

the development of "industrial and technological resources for cyber security," and the establishment of "a coherent international cyberspace policy" for the Union.[36] These strategic priorities are also based on a number of principles; yet two of those principles stand out as they are particularly important for the future of cybersecurity as put forward in this essay: (1) "Democratic and efficient multi-stakeholder governance," and (2) "A shared responsibility to ensure security." The former acknowledges the importance of multiple stakeholders—e.g., commercial, nongovernmental, and governmental entities—and supports their role in a "multi-stakeholder governance approach" for the EU, while the latter calls for "shared responsibility" and "coordinated response" by all relevant actors, at all levels, for a stronger cybersecurity.[37]

The examples of both the EU and NATO demonstrate recent, yet significant, efforts toward a coherent and broader cybersecurity framework. Even more essential for the accomplishment of this end seem to be the established and developing frameworks of cooperation between the EU and NATO. The two Organizations have been cooperating closely particularly since 2003 within the framework of the "Berlin Plus" agreement, while NATO has been also cooperating with the European Defense Agency (EDA), which has prioritized cyber-defense. Despite a number of existing agreements that regulate the NATO–EU cyber cooperation, there are still problems with its expansion to other sectors due to data protection concerns, the different perceptions of EU non-NATO states, as well as different perceptions between the two Organizations.[38]

The disagreements—no matter how minor—between two Organizations with such a similar security culture—given the big overlap with regard to their members—and history of cooperation, brings us to a common problem in international relations and politics, the one of conflicting (national) interests. Deibert and Rohonzinski, while acknowledging the growing international consensus on cybersecurity, they argue that this is not always the case, especially "when it comes to risks *through* cyberspace." In specific, they maintain that, "While states do collaborate around some policy areas where consensus and mutual interests can be found (for example, 'piracy,' and to a lesser degree child pornography), cooperation declines as the object of risk becomes politically contestable and where national interests can vary widely."[39] This, in turn, brings us to the realization that as long as individual nations have their own interests and maintain their own offensive and defensive (cyber) capabilities, full cooperation with regard to cybersecurity can only be limited. After all there have been many incidents over the past decade of cyberattacks from one

[36] EU, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," JOIN(2013) 1 final(07/02/2013): 4–5.

[37] Ibid., 3–4.

[38] Ekstedt, Parkhouse, and Clemente, "Commitments, Mechanisms & Governance," 186–87.

[39] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4(2010): 17.

country to another, such as China's attacks against the USA.[40] In this light, a need emerges for finding the ways in which the international community and global civil society could join forces in establishing a multileveled management of cybersecurity. One such way could be the development of a security culture that would foster multileveled cooperation on cybersecurity.

13.4 Security Culture and Global Capacity Building

Security culture has been related, among others, to organizational and (national) strategic culture and it is in many ways based on cognitive psychology and ideational understandings of security. In this essay we draw upon strategic culture definitions to shape our own definition of cybersecurity culture in the context that has been analyzed above.[41]

Jack Snyder was the first to examine the concept of strategic culture which he defined as "the body of attitudes and beliefs that guides and circumscribes thought on strategic questions, influences the way strategic issues are formulated, and sets the vocabulary and the perceptual parameters of strategic debate."[42] Kupchan's narrower view focuses on how elites make strategic decisions, and argues that "deeply embedded conceptions of security and notions of empire take root among elites and masses alike" while stressing that "strategic culture is distinguishable from elite beliefs [because]…it is based on images and symbols, not on logic and causal inference."[43] Johnston also emphasizes the importance of "symbols" while he maintains that two basic elements constitute strategic culture: "a central paradigm" which has answers regarding symbols, like "the nature of conflict in human affairs, the nature of the enemy, and the efficacy of violence; and "a ranked set of strategic preferences logically derived from these central assumptions."[44]

Even broader are the definitions by Booth and Gray. Booth suggests that "strategic culture refers to a nation's traditions, values, attitudes, patterns of behaviour, habits, customs, achievement and particular ways of adapting to the environment and solving problems with respect to the threat or use of force."[45] A similar, though shorter, definition is the one by Gray: "Strategic culture is the world of mind, feeling,

[40] Nigel Inkster, "China in Cyberspace," *Survival*: *Global Politics and Strategy* 52, no. 4 (2010): 55–56.

[41] Alexander W. Vacca, "Military Culture and Cyber Security," *Survival* 56, no. 6 (2012): 160.

[42] Jack L. Snyder, *The Strategic Culture*: *Implications for Nuclear Options* (Santa Monica: RAND, 1977). 9.

[43] Charles A. Kupchan, *The Vulnerability Of Empire* (New York: Cornell University Press, 1994). 21–22.

[44] Alastair I. Johnston, *Cultural Realism*: *Strategic Culture and Grand Strategy in Chinese History* (New Jersey: Princeton University Press, 1995). 50–51, viiii-x.

[45] Ken Booth, "The Concept of Strategic Culture Affirmed," in *Strategic Power*: *USA/USSR*, ed. Carl G. Jacobsen (New York: St. Martin's Press, 1990), 121.

and habit in behavior."[46] In this context, ideas matter and should be taken into account when examining or developing policies as well as when we try to develop frameworks of cooperation. As the above definitions show, strategic culture explanations mostly concern the national level and the distinct characteristics that shape the ways nations act on or react to strategic and security matters. Yet strategic culture has also been used to refer to different levels such as the military level or even the international level, i.e., strategic culture of a collective security organization. With regard to cybersecurity Paul and Porche III define an Army cybersecurity culture as "A pattern of shared basic assumptions that supports information security becoming a natural aspect of the daily activities of all Army personnel who operate in cyberspace."[47]

The security culture that this essay suggest is much broader and even though it goes beyond national strategic cultures, it does not disregard their existence; contrarily, it takes the variety of strategic cultures seriously into account as that is the only way the appropriate common features could be identified for the development of a new, collective, security culture of multileveled cybersecurity. After all, it has been argued that strategic culture could also be applied to non-state or transnational actors like the EU.[48] In this instance we refer to a culture of security instead of strategy as what we do not want to trace the ideas and norms that shape the strategic behavior of an actor but rather find ways to socialize different (national) ideas and norms—whatever they may be—into a global security culture of cybersecurity. A cybersecurity strategy therefore is the outcome we are interested in, not our object of analysis; but for such a strategy to be adopted a security culture needs to be developed first. Drawing upon the above-mentioned definitions, a security culture of multileveled cybersecurity would be a body of collective—i.e., non-state, sub-national, and national—attitudes, patterns of behavior, beliefs, as well as conceptions of (cyber) security, shaped based on the need to secure multiple referent objects against various cyberthreats, which would influence cybersecurity strategies.

It has been argued before that institutions have the power to shape common ideas and interests. As far as cybersecurity is concerned we do agree with the view that "institutions may well be the precursors for formalizing norms and principles that, in turn, might consolidate and strengthen the institutions themselves."[49] But because, as we have shown, many issues are subjects to political contestation among nations, the starting point of cooperation should be one that is valued by all actors involved. For example, it would be fairly difficult to integrate multiple national or military security cultures within a broader security culture framework. That is also the case

[46] Colin S. Gray, "Strategic Culture as Context: The First Generation of Theory Strikes Back," *Review of International Studies* 25(1999): 58.

[47] Christopher Paul and Isaac R. Porche III, "Toward a U.S. Army Cyber Security Culture," *International Journal of Cyber Warfare & Terrorism* 1, no. 3 (2012): 71.

[48] Perm M. Norheim-Martinsen, "EU Strategic Culture: When the Means Becomes the End," *Contemporary Security Policy* 32, no. 3 (2011): 535.

[49] Jeremy Ferwerda, Nazli Choucri, and Stuart Madnick, "Institutional Foundations for Cyber Security: Current Responses and New Challenges (revised)," *Composite Information Systems Laboratory*, *MIT* Working Paper CISL# 2011-05(2011): 4.

Table 13.1 Recent cyberthreat perceptions and cyberattacks

Actors	Incidents	Month/year	Type
Iran against West	Iran carries out cyber-drills	December, 2012	State vs. State (*Political*)
China against USA	USA asks China to halt corporate cyberattacks	February, 2013	State vs. State/Corporations (*Commercial*)
"Anonymous" against Governments, e.g., Israel	"Anonymous" launch attack on Israel	April, 2013	Transnational entity vs. states/governments (*Political*)
Anti-Western hackers (Syria) against West	Syria-based pro-Assad hackers (Syrian Electronic Army) attack Western media	April, 2013	Non-state/individual actors vs. non-state Organizations (*Political*)
Anti-Western hackers (Iran) against USA	Iranian-based hackers attack US company	May, 2013	State vs. State (*Political*)
China against USA	USA accuses China of cyber-spying	May, 2013	State vs. State (*Political*)

with cybersecurity as each nation—especially great powers—have related their cybersecurity and cyber-defense with their military and national strategies. The domain of cyberspace is, arguably, much more important than any other domain of international cooperation because of the multiple referent objects to be secured and the global implications of cyberthreats, as analyzed above. This reality—if we may call it that—could constitute the perfect starting point for cooperation on cybersecurity and the eventual development of a corresponding security culture.

In order for that to be achieved, two parallel tactics should be considered/undertaken: cooperation on all and through levels (horizontal and vertical cooperation); and cooperation on common cybersecurity threats—i.e., shared threats, common individual threats, and threats with potentially global impact. Starting with the latter we need to identify some serious cyberthreats with global or international concern. Table 13.1 briefly articulates a few cyberthreat perceptions or actual cyberattacks of different kinds in recent of years. It is important to note that threat perceptions do matter as they influence policy-making. By looking at the table one can identify the different types of cyberthreats, the different actors involved and, therefore, the multiple referent objects that need to be secured. It is important to note that the table is by no means exhaustive.

It is clear that there are differences between states which are expressed in cyberspace as well. Most notable cyber rivalries—at least as far as the table is concerned—are between the USA and China, the USA and Iran, and Israel and Iran. Cyberattacks were also carried against Iran from the USA and Israel in 2009.[50] From that perspective, cooperation could not be initiated based on politically sensitive issues like the cybersecurity of Iran's nuclear program, or the US government

[50] Shaun Waterman, "U.S.-Israeli Cyberattack on Iran was 'Act of Force,' NATO Study Found," The Washington Times, http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all.

cybersecurity vis-à-vis Chinese cyberthreats. The best starting point for multileveled and international cooperation on cybersecurity would be the common threats that all levels and governments face from individuals, non-state, and transnational actors—provided that they do not have state-sponsored political aims. Then more important issues could be gradually added to the agenda.

A multileveled cooperation and security culture could only be developed if efforts were made to bring together different actors on each level as well as built efficient communication lines between levels. As such, the sought collective cybersecurity culture would be informed by all levels through a top-down/bottom-up approach with no imposition of rules, regulations, or policies by one level on another. On a sub-national level, non-state actors such as banks, different firms, multinational companies and corporations, transportation and communication companies, would be easier to collaborate rather than governments. Therefore, existing domestic, regional, and international frameworks of cooperation need to be further developed in order for a global network to be created; a network, which would deal with—mainly commercial–cybersecurity concerns of private non-state entities. Such concerns could be cyber disruptions as well as data or intelligence theft by individuals or other private entities.

On a national level states should develop—as many have already done—their own cyber-defense not only for military purposes but for the security of their administrative (cyber) infrastructures as well. However, the know-how of each state should be shared as much as possible with other states, within the framework of global cooperation. Regional organizations could play an instrumental role to that end. Entities such as NATO, the EU, the Organization for Security and Cooperation for Europe (OSCE), the Association for Southeast Asia Nations (ASEAN), the African Union (AU), and the Union of South American Nations, among others, could facilitate an international dialogue on cybersecurity at the regional level as a first step. Understandably some of these institutions are more focused on trade and economic cooperation; yet a focus on cybersecurity would be an opportunity for further integration. In the meantime, at the national level, non-state actors should be in coordination both with the government and with the relevant regional institution.

The key for a global integration of different entities and different cybersecurity concerns is interregional/organizational dialogue. That would be the last step for the completion of the multileveled and globally oriented scheme of cooperation (see Fig. 13.1 for a depiction of the proposed framework). In sum, horizontally, non-state actors based in different states should cooperate among them, states should also cooperate on a (bilateral or multilateral) government level, states should participate in international institutions of their region, and regional institutions should participate in interregional coordination. Vertically, all levels should maintain effective communication lines and coordination between them. The non-state level should communicate with the state and regional level and vice versa, the state level should communicate with the non-state level as well as with the regional institutional level and vice versa, while the regional institutional level should coordinate with other regional institutions at the interregional—and ultimately global—level. Further, in terms of the agenda, the issues to be addressed and dealt with should be

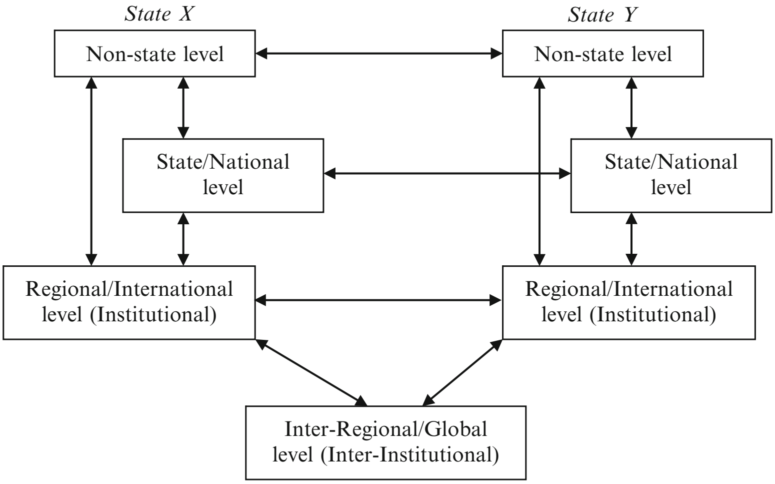
State X
State Y
Non-state level
Non-state level
State/National level
State/National level
Regional/International level (Institutional)
Regional/International level (Institutional)
Inter-Regional/Global level (Inter-Institutional)

Fig. 13.1 Multileveled cybersecurity cooperation

gradually more important and politically sensitive. Cooperation should start from commercial, everyday life, and notably non-state, matters only to gradually proceed to national, governmental and military issues. Thereby, the development of a global security culture of multileveled cybersecurity would be more possible and with greater potentials not only for cybersecurity but for international peace as well.

13.5 Conclusions

This essay has demonstrated the impact of cyberspace in everyday life and therefore the great insecurity that stems from cyberthreats at all levels—the local, national, and international. Against this background, and given that cybersecurity is in every actor's interest, there has been suggested that in order for global and effective cybersecurity and defense to exist a security culture of cybersecurity should be gradually developed through horizontal and vertical multileveled cooperation by starting with "low-politics" or non-politically sensitive cybersecurity matters. We have accepted that there may be many reasons for states not to cooperate, and states may indeed be the actors which would pose the biggest challenge in the context of a multileveled cybersecurity. However, cyberspace might be the one thing with the potential of effectively going beyond the notion of state-centric power struggle and that is because of its increasing and essential role in interconnecting all kinds of interests of all kinds of actors within the global system. In fact, we could go so far as to suggest that a multileveled framework of cybersecurity with successful communication lines through and between all levels may even provide a good platform for cooperation in other domains as well—through the socialization of norms and ideas—thus marking the beginning of further integration and interconnectedness of interests.

Yet this idea needs to be further developed and researched based on the already existing frameworks of cooperation at all levels in order for specific guidelines to be suggested and ways through which these frameworks could be integrated to be found.

Bibliography

Aravena FR (2002) Human Security: Emerging concept of security in the twenty-first century. Human Security in Latin America 2(1):5–15

Baldwin DA (1997) The concept of security. Rev Int Studies 23:5–26

Booth K (1990) The concept of strategic culture affirmed. In: Jacobsen CG (ed) Strategic power: USA/Ussr. St. Martin's Press, New York, NY, pp 121–128

Booth K (1991) Security and emancipation. Rev Int Studies 17(4):313–326

Buzan B, Hansen L (2010) The evolution of international security studies. Cambridge University Press, Cambridge

Choucri N (2012) Cyberpolitics in international relations. MIT, Cambridge

Davies B (2003) Terrorism: Inside a world phenomenon. Virgin Books, London

Deibert RJ, Rohozinski R (2010) Risking security: Policies and paradoxes of cyberspace security. Int Polit Sociol 4:15–32

EC (2005) Green Paper: On a European Programme for Critical Infrastructure Protection. Commission of the European Communities COM(2005) 576

Efthymiopoulos MP (2009) Nato's security operations in electronic warfare: The policy of cyber-defence and the alliance's new strategic concept. J Inform Warfare 8(3):61–70

Ekstedt V, Parkhouse T, Clemente D (2012) Commitments, mechanisms & governance. In: Klimburg A (ed) National cyber security: Framework manual. NATO CCD COE Publication, Tallinn, pp 146–191

EU (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final (07/02/2013)

Farivar C (2012) The Un's Telecom Conference Is Finally Over. Who Won? Nobody Knows.ars technica,http://arstechnica.com/tech-policy/2012/12/the-uns-telecom-conference-is-finally-over-who-won-nobody-knows/

Ferwerda J, Nazli C, Stuart M (2011) "Institutional Foundations for Cyber Security: Current Responses and New Challenges (Revised)." Composite Information Systems Laboratory, MIT Working Paper CISL# 2011–05, http://web.mit.edu/smadnick/www/wp/2011-05.pdf.30/04/2013

Giddens A (1990) The consequences of modernity. Polity, Cambridge

Gray CS (1999) Strategic culture as context: The first generation of theory strikes back. Rev Int Studies 25:49–69

Healey J, van Bochoven, L (2011) Nato's Cyber Capabilities: Yesterday, Today, and Tomorrow. Atlantic Council IssueBrief

Hughes R (2010) A treaty for cyberspace. Int Affairs 86(2):523–541

Inkster N (2010) China in cyberspace. Survival: Global Politics and Strategy 52(4):55–66

ITU (2012) Final Acts: World Conference on International Communication. International Telecommunications Union, Dubai

Johnston AI (1995) Cultural realism: Strategic culture and grand strategy in Chinese history. Princeton University Press, Princeton, NJ

Kupchan CA (1994) The vulnerability of empire. Cornell University Press, New York, NY

McSweeney B (1999) Security, identity and interests: A sociology of international relations. Cambridge University Press, Cambridge

NATO (2010) Active engagement, modern defence. Strategic concept for the defence and security of the members of the North Atlantic Treaty Organization. NATO, Lisbon

Norheim-Martinsen PM (2011) Eu strategic culture: When the means becomes the end. Contemporary Security Policy 32(3):524–541

North RC (1990) War, peace, survival: Global politics and conceptual synthesis. Westview Press, Boulder, CO

Nye JS (2011) The future of power. Public Affairs, New York, NY

Panyarachun A et al (2004) A More secure world: Our shared responsibility. High-level panel on threats, challenges and change: United Nations, Manhattan

Paul C, Porche IR III (2012) Toward a U.S. Army cyber security culture. Int J Cyber Warfare Terrorism 1(3):70–80

Prezelj I (2008) Challenges in conceptualizing and providing human security. HUMSEC J 2:1–22

Rosenfield DK (2009) Rethinking cyber war. Crit Rev 21(1):77–90

Snyder JL (1977) The strategic culture: Implications for nuclear options. RAND, Santa Monica

Terriff T et al (2006) Security studies today. Polity, Cambridge

Ullman RH (1983) Redefining security. Int Security 8(1):129–153

Vacca AW (2012) Military culture and cyber security. Survival 56(6):159–176

Walt SM (1991) The renaissance of security studies. Int Studies Quarterly 35(2):211–239

Waterman S. U.S.-Israeli Cyberattack on Iran Was ‘Act of Force,’ Nato Study Found. The Washington Times, http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all

Williams PD, Studies S (2010) An Introduction. In: Williams PD (ed) Security studies: An introduction. Routledge, New York, NY, pp 1–10

Wolfers A (1952) 'National security' as an ambiguous symbol. Polit Sci Quarterly 67(4):481–502