

# Preface

Although the emergence and ever increasing diffusion of the cyberspace have most obviously significant implications for international politics, global economic activity, and transnational social relations, there is still a cloudy spot in research in terms of addressing these implications theoretically and empirically in one comprehensive and wide-ranging volume. Of course there is a vast number of articles and books on security-related issues of the cyberspace (cyber security, cyber warfare, cyber power, and so forth) as well as on the processes and the modalities of what we may call the digital transnationalization of social spaces and relations, but an inclusive volume on the implications of the process of “cyberization” of international relations (IR) has been missing until now. “Cyberization” of IR refers to the ongoing penetration of all different fields of activity of international relations by different mediums of the cyberspace on the one hand, and the growing dependence of actors in IR on infrastructure, instruments, and means offered by the cyberspace on the other hand. Because of the evolution of a “cyberization” of IR and due to the ever-increasing relevance of the cyberspace for contemporary international politics and global economic and social activities, there is profound need for political scientists and scholars of IR to identify, describe, and explain these developments, prospects, and emerging challenges theoretically and empirically in an accurate manner.

Therefore, this book brings together scholars and scientist as well as experts from cyberspace’s everyday practice, to provide elaborated and sophisticated answers as well as deep insights about how to cope conceptually, theoretically, and empirically with the relation of *Cyberspace and International Relations*.

Based on the observation that there is not only a considerable deficiency of knowledge on the topic in political science and IR, but also a significant lack of discussion and debate with scholars and experts from other fields of practical and academic work, the idea for a project came up that should tackle this “agonizing lightness” by combining the forces of scholars from different disciplines and practical experts alike. It was obvious from the beginning that a project that should equally address theoretical as well as empirical implications of the cyberspace for international relations would need an editorial team and authors who could rely on academic expertise as well as practical experience in the field. Consequently, the idea was born to invite scholars and practitioners from various fields of activity to join the effort of creating a collective volume that engages the relationship of

cyberspace and international relations from as many points of view as possible. The editors hope that this volume is able to contribute to supporting an interdisciplinary and sophisticated debate on the implications of the process of “cyberization” of IR.

To achieve this goal, Part I of the project brings together authors that present their thoughts on how to conceptually and theoretically enlighten the relationship of the cyberspace and international relations, to discuss implications for the discipline of IR and to present fresh and innovative theoretical approaches. By presenting approaches and frameworks that either deal with the general relation of IR and the cyberspace or that develop theoretical approaches to explain the dynamics of this relation in specific fields of activity (like cyber security, cyber warfare, diffusion of information and knowledge through the cyberspace, interconnectedness of economic and social activities through the cyberspace etc.) part I of the project enhances the theoretical and conceptual knowledge on the interaction of the cyberspace and IR. This opening part of the book brings together conceptual and theoretical contributions on the relation of the cyberspace and IR (in terms of actors, spaces, fields of activity etc.), to foster and improve our understanding of the consequences, effects, and implications of the process of “cyberization” for states’ security, power positioning, interest achievement, diplomatic activity among others, as well as for economic and civil actors that are likewise affected by the “cyberization” of IR.

The opening chapter of part I, “Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace” by Roxana Radu argues that the best way to grasp the impact of the cyberspace on IR is to study the reconfiguration of global governance techniques brought about by the virtual mediums. By applying the Foucauldian concept of governmentality to investigate the global discourses of security in the cyberspace, this chapter sheds light on a shift in the rationality of governing, and gives empirical evidence of the dominant discourse(s) of security in the cyberspace in the United Nations (UN) ambit. The chapter therefore delivers solid knowledge on how technologies and practices related to the cyberspace shape international politics and IR more generally.

In his chapter “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?” Craig B. Greathouse tackles the important question of whether or not classical theorist of IR can still be seen as a valuable source of explanation for understanding war, warfare, and conflict in the realm of the cyberspace. With a special emphasis on the strategic options available for states in the field the chapter offers a clear and distinctive typology to view issues of cyber conflict, based on the thoughts of some of our discipline’s most influential thinkers. Furthermore, it offers an examination of possible strategic choices for policy makers based on classic strategic thought. The chapter applies the ideas of Clausewitz, Sun Tzu, Jomini, along with more modern theorists such as Douhet and Warden to the idea of cyber war. In doing so the chapter convincingly elaborates the importance of classic and modern thinkers for explaining the implications of cyber warfare and cyber security.

In their contribution, “SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World” Jan-Frederik Kremer, and Benedikt Müller present a new framework to identify and evaluated challenges to states in relation

to the cyberspace. Based on the observation, that states and enterprises are increasingly faced with newly emerging threats made possible by interconnected digital infrastructures and that these threats pose different levels of risk to states and their citizens, the chapter identifies the different types of stakeholders, their actions and respective motives in the context of cyber security and introduces the so-called SAM-framework to estimate whether or not a challenge poses a severe risk to the security of the state.

Hanna Samir Kassab (“In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare”) focuses in his chapter on the possibility of a reliable cyber deterrence option. After a discussion of deterrence theory and the potential of its application for the realm of the cyberspace, Kassab discusses the argument of a virus wall as functional instrument of deterrence. In doing so Kassab’s chapter distributes to the theoretical debate on deterrence and its use in the area of cyberspace.

In her chapter “Offense–Defense Balance in Cyber Warfare” Salma Shaheen discusses the possible implication of a proliferation of cyber weapons. She argues that since, until now the cyber weapons are used in an offensive mode; therefore, the probability of more states developing offensive cyber weapons is increasing. The chapter reasons that the offensive nature of cyber weapons without having an adequate defensive character is destabilizing for the international security system. In this regard, her chapter examines the offense–defense balance in the cyber warfare, and how the offensive side does has the advantage in cyber warfare that can destabilize international security.

By linking power relations in the technologically dominated context of cyberspace to Hannah Arendt’s theoretical considerations of power and violence the chapter “The Utility of Timeless Thoughts: Hannah Arendt’s Conceptions of Power and Violence in the Age of Cyberization” by Katharina C. Below offers fresh perspectives on the importance of power in IR. It is argued that the structure of power and violence in cyberspace can be captured abstractly by dividing cyberspace into two parts that refer to Arendt’s conceptions of power as “power to” and violence as “power over”. Cyberspace is thus both, a modern space of appearance and political freedom and an unexplored context for Arendt’s conception of power as well as an anti-space of appearance, a space filled with Arendt’s conception of violence that denies the positive attributes of a space of appearance when filtering and control techniques are implemented. By looking at the cases of the Arab Spring protests, Weibo and the Fifty Cent Party as well as Denial of Service (DoS) attacks during elections or interstate conflicts Below underlines the empirical relevance of her thoughts.

Contributions of the Part II address emerging challenges and prospects for international politics and relations. By highlighting empirical findings in fields like peacekeeping, global governance, diplomacy, economy, cultural activity, transnational communication, cyber espionage, and social media, it explores the process of “cyberization” of IR. The chapters in this part of the book focus on specific empirical phenomena that make the process of “cyberization” of IR comprehensible and visible, while at the same time addressing the implications of their findings on their field of IR.

The first chapter of part II “Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War” by Sascha Knoepfel addresses the question whether the use of the Stuxnet computer worm can be seen as an “act of war” in the light of theory on the nature of war and acts of war. By presenting definitional criteria for an act of war in cyberspace the chapter sheds light on the ongoing debate and makes a solid contribution to a discussion on an empirical phenomenon which stands exemplary for a new type of virus worm used by well-equipped actors as instrument to achieve strategic goals.

In his piece of work “A New Way Of Conducting War: Cyberwar, Is That Real?” Hakan Mehmetcik contributes to the more general discussion on both the reality and impact of cyberwar. By discussing the applicability of Clausewitzian and other IR perspectives on war to cyberwarfare, this chapter broadens our understanding of cyberwarfare. Looking into the cases of Estonia and Georgia as defendant of cyberattacks Hakan’s contribution will also increase our empirical knowledge on different forms of occurrences of cyberwarfare.

The chapter “Peacekeeping 4.0: Harnessing the Potential of Big Data, Social Media, and Cyber Technologies” by John Karlsrud evaluates, by looking into various cases, the potentials that arise from big data, social media, and other cyber technologies for effective peacekeeping and peacebuilding. The chapter states that actors in the field are still lagging woefully behind when it comes to putting those new technologies and developments to use for peacekeeping and peacebuilding. The chapter shows further, that these tools are already well-known in the areas of humanitarian action, social activism, and development; and that the United Nations, through the Global Pulse initiative, has also begun to discover the potential of “Big Data for Development,” which may in time help prevent violent conflict. This chapter details some of the initiatives that can be harnessed and further developed to overcome this shortage, and offers policy recommendations for states, the UN Security Council, and UN peacekeeping at UN headquarters and at field levels. Thereby, the contribution by John Karlsrud delivers not only profound knowledge on the importance of cyber technologies for specific activities of international relations, but also solid and elaborated policy recommendations for future application.

Ryan David Kiggins’ chapter “US Leadership in Cyberspace: Transnational Cyber Security and Global Governance” examines US cyber security policy in the light of transnational cyber security, deterrence theory, and hegemonic stability theory. His chapter explores and discusses the problems of deterrence theory, as a state level theory of national security, related to the application on a medium which is per meaning transnational in form and characterized by diffusion of authority, control and leadership—the Internet. The chapter argues for a conceptualization of cyber security as a transnational security issue and that such a framing may assists political leader within the US to develop a comprehensive US cyber security policy that incorporates deterrence and US leadership. Furthermore, the chapter argues that from the standpoint of transnational security, the US should fulfill its role as leader of collective hegemony, by leading cyber space stakeholders to develop norms and rules for global cyber security governance regimes and institutions that will teach states the norms and rules necessary for a stable and

secure cyber domain through which global information and economic exchange will continue to flourish. By applying a strong empirical argument, the chapter contributes significantly to the arising debate on the necessity of leadership for a secure and stable Internet.

Starting with the reflection that networked governance is the default *modus operandi* in Internet governance Andreas Schmidt's contribution "Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security" analyzes the consequences for Internet security. The chapter argues that Internet security heavily relies on non-hierarchical, networked forms of organization and defines networked governance in this field as "a semi-permanent, voluntary negotiation system that allows interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority". His chapter analyzes the ability of traditional powerful actors such as state authorities and large enterprises to provide Internet security and exert power in the cyber-domain. The chapter furthermore outlines potential anchor points for traditional powerful actors to introduce more elements of hierarchy and control into Internet security provisioning networks. Empirically, the chapter describes emerging hybrids of networks and hierarchies in Internet security provisioning. In so doing, this contribution not only fosters our empirical knowledge on the importance of networked governance in IR, but also marks out the theoretical implication for IR of such developments.

Oliver Read's part ("How the 2010 Attack on Google Changed the US Government's Threat Perception of Economic Cyber Espionage") shows how the 2010s attack on Google changed the US authorities' perception of cyber threats. Through exploring the evolution of the case and perceptions of the US government and by applying an analytical framework called "threat politics" introduced by the author, this chapter profoundly increases our knowledge on how threat perceptions develop in the realm of cyberspace. The argument is substantiated in two main steps. In step one, it is shown how the American Government conceptualized the threat of economic cyber-espionage before and after the announcement. In step two, we trace how this perception-shift led to a series of countermeasures.

Stephen D. McDowell's, Zoheb Nensey's, and Philip E. Steinberg's chapter entitled "Cooperative International Approaches to Network Security: Understanding and Assessing OECD and ITU Efforts to Promote Shared Cybersecurity" looks into how states have undertaken efforts to increase cybersecurity by promoting network security in international organizations and examines the influence of these institutions in this regard (Organization for Economic Cooperation and Development (OECD), and the International Telecommunications Union (ITU)). The chapter examines existing perspectives on the desirability and feasibility of international cooperation on network security. It further discusses the international efforts to advance cooperative approaches to network security and cybersecurity. Additionally, it assesses these multilateral efforts in the light of states' recent moves to advance more strategic national approaches and thereby delivers profound insights into cyber-security-related bargaining and decision making among international organizations and evaluates the influence of the respective organizations for supporting security in the field.

The contribution of Matthew Crosston entitled “Phreak the Speak: The Flawed Communications within Cyber Intelligentsia” surveys a fundamental dichotomy that has developed within the academic, technical, and policy communities when it comes to understanding, advancing, and communicating work on cyberspace within global affairs. This dichotomy, so Crosston, not only exists as an intellectual barrier between scholars of the hard and social sciences, it impinges on progressive cooperation between the political and technical communities. Consequently, there is a gap weakening the scope and reach of theoretical and empirical work on cyberspace in general. The chapter argues that this problem has the potential to become exponentially larger in the immediate future: not only are real-world professionals and scholars having trouble building bridges between obvious mutual interests, but this ‘Chinese knowledge wall’ separates each group respectively. Just as phreaking involves a subculture of specialists who experiment and toy with telecommunication systems, the intellectual, technical, and governmental worlds need a new generation of ‘phreak-scholars’ who are adept at building connections between these diverse, inter-related knowledge bases.

The chapter “Reflections on Virtual to Real: Modern Technique, International Security Studies and Cyber Security Environment” by Marcial A. Garcia Suarez and Igor D. P. Acácio deals with the analysis of the phenomenon of modern technique by Martin Heidegger, especially the issue of information societies and the role that the virtual network has. It gives information about the political behavior of states, which affect the international security environment and estimates implications for IR theory.

The editors would like to express their deepest gratitude to Mrs. Barbara Fess and Mrs. Marion Kreisel (Springer) for their tremendous help and backing throughout the whole project and for their commitment to produce the project true to the editors’ visions. Working together with such proficient and pleasant people makes publishing a lot more easy. Furthermore, the editors would like to share their appreciation and admiration for all the participating authors: Without their magnificent chapters, this book would not be such a comprehensive and conclusive contribution to the field. Working together with such highly professional and prudential people makes the editing work most enjoyable. Additionally, the editors wish to express their appreciation to the organizers and respective panel chairs of the ISSS/ISAC Annual Conference 2011, ISA Annual Convention 2012, and the 2012 Joint BISA-ISA Conference for providing an excellent setting to present our ideas and to launch this project.

Jan-Frederik Kremer would like to express his deepest thanks to his friends, family, parents, and to his wonderful wife Katrin for their support and patience not only throughout this project, but throughout difficult times in his life. Without his wife’s, parents’, familys’ and his friends’ love and ever ongoing and unconditional support he would not have had the drive or inspiration to complete such a project. He also wants to share his special and deep gratitude for Prof. Dr. Xuewu Gu’s ever ongoing backing, mentoring, and his most enjoyable way of (academic) support, which by far exceeded any expectations. Additionally, he would like to thank Prof. Dr. Wilhelm Lowenstein (Ruhr-University) for his personal and

professional support throughout the years. Jan-Frederik also owes his gratitude to institutions like the DAAD, DFG, Ruhr-University Bochum Research School, Bonn University, University of Miami (FL), and ISA for grating him numerous grants, scholarships etc., which have made academic networking and project planning possible. Jan-Frederik wish to express his thankfulness also to the Friedrich-Naumann-Foundation for Freedom and especially to Dr. Gerhard Söltenfuß for the confidence and faith he have in me and for his backing and mentoring. Working for the indispensable idea of liberty and freedom is fulfilling and stimulating at the same time. Last but not least, Jan-Frederik would like to thank his co-editor and friend Benedikt Müller for all the enjoyment, support, and professionalism, which has made working together with him at this project truly inspirational.

Benedikt Müller would like to thank his family and friends, especially his wife Lara and his parents for their everlasting love and support. The most powerful force driving him to complete a project like this is having loved ones who believe in him. He is furthermore indebted to IBM and Accenture, two exceptional corporations offering environments full of inspiring people and challenging experiences. Beyond that, he wants to extend his gratitude to his co-editor Jan-Frederik Kremer who, besides being a true friend and his best man, helps a practitioner wander through the world of academics.

Bonn, Germany  
Essen, Germany

Jan-Frederik Kremer  
Benedikt Müller

Cyberspace and International Relations

Theory, Prospects and Challenges

Kremer, J.-F.; Müller, B. (Eds.)

2014, XXIV, 284 p. 2 illus., Hardcover

ISBN: 978-3-642-37480-7