Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Cyberpolitics

Nazli Choucri

Professor, Political Science Department
Massachusetts Institute of Technology

May 15, 2014

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Citation: Choucri, N. (2014). Cyberpolitics. In J. Krieger (Ed.), *The Oxford companion to international relations* (pp 267–271). Oxford University Press.

Unique Resource Identifier: ISBN: 9780199738878. https://global.oup.com/academic/product/the-oxford-companion-to-international-relations-9780199738878?cc=in&lang=en&

Publisher/Copyright Owner: © 2014 Oxford University Press.

Version: Final published version.

MacFarquhar, Roderick. *The Origins of the Cultural Revolution.* 3 vols. (New York, 1974–1997). The magisterial work by the recognized dean of Cultural Revolution studies covering the period 1956–1966, when the seeds of the Cultural Revolution were planted in Mao's mind and in the Chinese Communist Party state he created.

MacFarquhar, Roderick, and Michael Schoenhals. *Mao's Last Revolution.* (Cambridge, Mass., 2006). Widely regarded as the best single-volume history and analysis of the Cultural Revolution.

William A. Joseph

CYBERPOLITICS

Almost everyone, and almost everywhere, has access to the Internet and makes use of cyber venues in one way or another. Until recently, cyberspace was considered largely a matter of *low politics*—background conditions and routine decisions and processes. In recent years, issues connected to cyberspace and its uses have catapulted into the highest of high politics. A newly coined term, "cyberpolitics," refers to the conjunction of two processes: those pertaining to politics surrounding the determination of who gets what, when, and how, and those enabled by the uses of cyberspace, a new arena of virtual interactions.

Space and Its Realities All forms of space in traditional conceptions of international relations provide opportunities for expanding power and influence in world politics. The term "space" often refers to areas of interaction that create potential sources of power; provide for the expansion of influence and leverage; enable new services, resources, or markets; and realize further potentials when reinforced and sustained by technological advances. Traditionally, the notion of space was closely coupled with territoriality. Clearly, this connection is loosening rapidly.

The fundamentals of space revolve around the characteristics of the playing field—that is, who can play, how, and why. Among the most familiar notions of space are those wrought by traditional forms of colonialism and imperialism, modes of expansion and control of foreign territories that are driven by economic, strategic, and political motivations for control and domination.

Advances in science and technology, buttressed by scientific innovation, have allowed for conceptualization, construction, and access to new forms of space. Notable among these is nanospace, where microminiaturization affords activity in a previously inaccessible domain. The area of genetic space, greatly expanded with the charting of the human genome, is another example.

Cyberspace is yet another arena. Created through technological innovation, it is a venue that allows users to engage in activities conducted over electronic fields whose spatial domains transcend traditional territorial or sovereign constraints. In the twenty-first century, access to cyberspace has become available to more and more people around the world. As of 2011 an estimated 2 billion people had accessed the Internet. Access to cyberspace offers new opportunities for competition, contention, and conflict—all fundamental elements of politics and the pursuit of power and influence.

Cyberspace. The historical and philosophical roots of the term "cyber" are often considered to lie in Plato's allegory of the cave in the *Republic.* In the twentieth century its semantic identity was derived from the term "cybernetics," the study of communication and control rendered famous by Norbert Weiner in *Cybernetics: Or Control and Communication in the Animal and the Machine* (1948). Weiner's exposition influenced Karl W. Deutsch's *The Nerves of Government* (1963), which remains the single most important entry point into political science and political inquiry. William Gibson's *Neuromancer* (1984) connected the notions of cybernetics and spatial domain and is generally regarded as providing the first formal designation for the new arena of interaction we now know as cyberspace. A range of metaphorical meanings now attached to "cyber" is associated with a panoply of immersive environments, the possibility of interacting with synthetic entities, and a variety of gaming experiences. Many, if not all, reflect modes of expanding the frontiers of virtual space and human imagination.

Cyberspace is a domain of human interaction created through the interconnection of millions of computers provided by a core global network, such as the Internet. The Internet is a layered system that enables processing, manipulation and use of information, and facilitates the expansion of human communication as well as interaction of humans and information. All of these features are relevant to cyberpolitics in international relations, but to different degrees and in different ways.

Cyberpolitics. The laws of politics, though subject to debate among some political scientists, generally refer to regularities of human behavior across time and space. With the creation of cyberspace, a new arena for the conduct of politics is taking shape, and we may well be witnessing a new form of politics. There is, as yet, no decisive account or description of cyberpolitics; the language and concepts we use are the familiar ones of politics in real domains. Combining a definition of politics as the authoritative allocation of values in society with the notion of who gets what, when, and how, leads us to the most generic and appropriate view of politics, relevant in all contexts, times, and places. These dual insights into the nature of politics, while initially articulated for the individual polity or the nation-state, carry a powerful meaning that is readily transferable to various political contexts, national and international. They also draw attention to areas dominated by the politics of ambiguity, areas where the domain is unclear and the stakes are not well defined.

All politics, in the cyber and real arenas, involves conflict, negotiation, and bargaining over the mechanisms, institutional or otherwise, to resolve in authoritative ways the contentions over the nature of particular sets of core values. While it is not possible to delineate the full implications of cyberspace for politics and political behavior, the conduct of cyberpolitics across a wide set of issues, along with commensurate changes in political discourse and interactions, has generated worldwide effects and has led to the articulation and aggregation of new interests, as well as new patterns of international relations and new modes of institutional responses and global accord. The essence of the virtual state—characterized by expansion of, and dependence upon, its cyber capabilities—lies in its ability to garner the power of finance and ideas and to transform them into sources of global influence.

Cyberspace has created new conditions for which there are no clear precedents. There is as yet, little consensus, if any, on the "next steps" to take to incorporate cyber venues into contemporary discourse on sovereignty, stability, and security. However, some contending positions are already discernible.

Theory Matters. All things considered, we cannot assume that international relations theory of the twentieth century can be readily imported into the cyber world of the twenty-first century. Consider *realism* (and its variants), for example, which focuses on national security, power politics, and conflict. It is not yet fully clear what cybersecurity actually entails or what "might" may signify in the cyber domain. Or consider *institutionalism*, concerned with cooperation, coordination, and formal and informal collaborations, which may have some direct implications for the management of cyber venues. However, institutionalism is a state-based logic for regulating interstate interactions. Cyberspace has been constructed by the private sector, and its operations are managed by the private sector. The state is a latecomer to this domain. There are more obvious possibilities were we to consider *constructivism*, the perspective focusing on perceptions, cognition, beliefs, values, symbols, and similar variables, which emphasizes the subjective. The interface of constructivism with some uses of cyber access for purposes of expression and communication is among the most obvious connections with international relations theory.

A major challenge is to develop a powerful logic to guide our understanding of cyberpolitics in international relations, other than to say that individual voices matter now more than ever before. Adjustments to all three theoretical perspectives must take place if the new cyber realities are to be effectively taken into account in evolving understanding of international relations. The same challenges may well hold for theory in different areas of politics and political behavior.

In light of the changing and ever expanding global connectivity, it is tempting to ask, What are some of the major patterns of cyber access? How extensive is cyber participation worldwide? Are these empirical questions that can generate data-based responses? At the same time, however, cyber access per se provides little insight into the content or the substance of cyber interactions and even less information about leveraging cyber venues to enhance power, capability, and performance—the substance of interactions. With the increased politicization of cyber-based interactions, there are growing efforts to control access as well as content, and these efforts threaten the "open communication" vision of cyberspace supported by the United States and other Western countries.

Levels of Analysis. To improve any effort to understand of these new realities, it is useful to look at cyberpolitics at four levels of analysis: the individual level, the state level, the international level, and the global level. All these activities may challenge traditional concepts of sovereignty.

The evidence so far suggests that cyberspace empowers and enables *individuals* in ways that were previously not possible. This empowerment is manifested through communication, expressed perceptions, organization, and preparations and, most important, access to knowledge. At the same time, there is variation in the degree of power wielded by individuals in different states. Different parameters of action are possible in cyber venues, and these cannot always be ignored by the state.

To date, the technology of cyberspace privileges the individual relative to the state in one important way: it is not always possible to assign responsibility to a specific individual for the transmission of a cyber message. If this situation persists, then the individual level of analysis in international relations theory assumes a new importance, greater than anticipated in traditional theory. The aggregative powers of cyber access, which allow individuals to combine to form various types of entities that transcend territorial boundaries, provide a strong reinforcing mechanism. Some of the newly aggregated entities can be seen as "normal," non-state actors, others may lack a label or description, and still others may operate behind a veil of secrecy. But they all affect states in one way or another.

At the *state level,* cyberspace provides new venues for the exercise of power in all the usual ways, as well as some additional ones, and allows a focus on sovereignty and territoriality as the ultimate principles on which to justify moves of choice in cyberspace. It has also given states new points of control. But the state is no longer the only actor wielding this power—perhaps not even the most dominant one in cyberspace. One line of thinking holds that cyber realities undermine state sovereignty in notable ways. Another line is that despite the emerging power of virtual reality, the fundamentals of state sovereignty remain robust, as revealed in various successful efforts in democratic as well as authoritarian states to regulate the transmission of content. This view suggests that the new arena is neutral with respect to impacts on sovereignty. Yet another holds that cyberspace is fundamentally generative in both technological and social terms and, as such, contributes to reframing conceptions of sovereignty and the role of the state, most notably in the provision of public goods.

Cyber access notwithstanding, states are far from equal in attributes and capabilities or in power and influence. Drawing on the constitutive power of the master variables core features of states — population, resources and technology—the evidence shows that different combinations of these fundamental features capture the major differences among them. Despite variation in master variables, almost all states, rich and poor, are already adjusting to the cyber realities, are engaged in various forms of e-governance, and continue to reinforce the conditions required for effective performance. Closely connected to e-governance is e-participation. While the evidence points to more rather than less e-participation by states, more important is the impact. How effective is e-governance? What is the impact of e-participation?

At the *international level,* the system as a whole consists of sovereign states (the key entities), as well

as nonstate actors and intergovernmental institutions. They all operate in a world that is increasingly connected via cyberspace—often in tightly coupled ways. While there is much in this new world that challenges the state system at the individual, national, and international levels, in the cyber domain boundaries are permeable and information, ideas, interests, and the like can circulate with little regard for territory or jurisdiction. This means that the usual international instruments of states are not always readily transferable, available for use in the cyber arena, but the state system is adapting. Its members are developing and deploying new instruments of control, and in many cases, they clearly aspire to become the major players in the cyber domain.

At the *global* level, the construction of cyberspace has created a new dimension of interaction of overarching scale and scope. As such, cyberspace is becoming a close companion of the social system in its global proportions. Since all human interactions are embedded in the natural environment, the cyber domain is inevitably interconnected with the life-supporting properties of the natural environment. The global system as a whole is increasingly vulnerable to a broad range of hazards created by human activities. Such arguments point to the potential synergy between cyberspace (a new arena of interaction) and sustainability (a new imperative for theory and policy). There may well be some powerful synergy or mutually reinforcing dynamics between cyberspace as a new arena for human interaction, on the one hand, and the worldwide efforts to explore transitions to sustainable development, on the other. These two initially independent processes may well be converging, with potentially powerful impacts at the international, state, and individual levels.

Conflicts and Cooperation. Conflict and cooperation are two, often interdependent, modes of political activity at all levels of analysis. Cyberspace enables various types of conflict and of cooperation, what may or may not be the mirror image of their respective manifestations in traditional international relations.

Despite the variety of contentions and disputes and the incompleteness of information, we are nonetheless able to identify three general types or clusters of cyberconflicts. First are contentions over the management of cyberspace and the operational features of the Internet. Second are the uses of cyber venues for strategic advantage and leveraging political control to regulate cyber access or deny access to content deemed undesirable. And third is the militarization of cyberspace, including the conduct of cyber warfare, cyber threats to critical infrastructures, and various types of cyber crimes and espionage, among others. Each of these three reflects a modal type with many variations. Some are about claiming the future, while others are about managing the present, all with different manifestations and varying degrees of intensity, and varieties of manifestations.

The other side of the ledger is no less complex: the construction of cyberspace has already required new mechanisms of coordination and collaboration to develop norms and standards. First are the collaborative activities surrounding the governance of cyberspace. To date, cyberspace has been managed by the private sector, but traditional international institutions now seek to influence the management of the new arena and use it for a wide range of mission-oriented purposes. Some new forms of collaboration may be in the making. Second are the cyber collaborations that revolve around the quest for global norms and agreements on the provision of cyber-related public goods. The players, state and nonstate, involved in shaping the evolving global agenda are increasingly drawing on cyber venues to reinforce the central trajectories of that agenda. The third and most comprehensive form of cooperative cyberpolitics involves the formation of the twenty-first-century global agenda, broadly defined. An important aspect of the global agenda is to support the technological bases of cyberspace and ensure its sustainability.

Conclusion. In the cyber domain, as in the traditional domain, politics is fundamentally about control over the authoritative allocation of value in terms of who gets what, when, and how. Cyberpolitics

represents a new dimension of political activity that: (1) expands both "voicing" and participation in interactions, communication and networking; (2) facilitates the development of new content, notably knowledge; (3) helps to consolidate political discourse and the formation of cyberpolitics in the pursuit of norms, goals, and modes of behavior at all levels of social organization and over time; (4) provides new venues to organize and articulate demands for collective responses to shared problems; and (5) eventually helps institutions to construct strategies for managing responses.

These are only a few of the key features of cyberpolitics. They reflect an emergent form of politics that is becoming sufficiently pervasive to constitute a fundamental feature of the changing international landscape of power and influence. At least two overarching processes will continue to shape the future of cyberpolitics: one is the use of cyber venues for shaping politics in the physical domain, and the other pertains to uses of cyber venues for shaping the configuration of cyberspace itself. And both processes influence, if not shape, how the international "landscape" of actors, actions, technology, and power relations is rapidly changing.

[*See also* Censorship; *and* Political Science.]

BIBLIOGRAPHY

Choucri, Nazli. *CyberPolitics in International Relations.* (Cambridge, Mass., forthcoming).

Choucri, Nazli.and Daniel Goldsmith "Lost in Cyberspace: Harnessing the Internet, International Relations and Global Security." *Bulletin of the Atomic Scientists*, 68, 2: 70–77, (2012).

Choucri, Nazli, ed. "Introduction: CyberPolitics in International Relations," in *International Political Science Review*, Issue Title *CyberPolitics in International Relations*, 21, 3: 243–265. (2000).

Deutsch, Karl W. *The Nerves of Government: Models of Political Communication and Control.* (New York, 1963).

Easton, David. *The Political Science System: An Enquiry into the State of Political Science.* (New York, 1963).

Gibson, William. *Neuromancer.* (New York, 1984).

Lasswell, Harold D. *Politics: Who Gets What, When and How.* (New York, 1958).

Rosecrance, Richard. *The Rise of the Virtual State.* (New York, 1999).

Weiner, Norbert. *Cybernetics: Or Control and Communication in the Animal and the Machine.* (Cambridge, Mass., 1948).

Nazli Choucri

CZECHOSLOVAKIA

See Slovakia.

THE OXFORD COMPANION TO COMPARATIVE POLITICS

Joel Krieger
EDITOR IN CHIEF

VOLUME 1

Abortion–Korea, Republic of

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS
Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trademark of Oxford University Press
in the UK and certain other countries.

Published in the United States of America by Oxford
University Press, 198 Madison Avenue, New York, NY 10016
www.oup.com

Copyright © Oxford University Press 2013

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior permission in writing of Oxford University Press, or as expressly permitted by law, by license, or under terms agreed with the appropriate reproduction rights organization. Inquiries concerning reproduction outside the scope of the above should be sent to the Rights Department, Oxford University Press, at the address above.

You must not circulate this work in any other form and you must impose this same condition on any acquirer.

Library of Congress Cataloging-in-Publication Data
The Oxford companion to comparative politics / Joel Krieger, editor in chief.
p. cm.
Includes index.
ISBN 978-0-19-973859-5 1. Comparative government—Handbooks, manuals, etc. I. Krieger, Joel, 1951–
JF51.O93 2012
320.3—dc23 2012006696

9 8 7 6 5 4 3 2 1
Printed in the United States of America
on acid-free paper