Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences

Nazli Choucri

Professor, Political Science Department
Massachusetts Institute of Technology

October 13, 2013

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.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Co-Evolution of Cyberspace and International Relations:

New Challenges for the Social Sciences

Nazli Choucri
Professor of Political Science
Massachusetts Institute of Technology
nchoucri@mit.edu

Prepared for World Social Science Forum (WSSF) 2013
Montreal, Canada

October 13-15, 2013

Acknowledgement: This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Table of Contents

I. Introduction

Created by human ingenuity, cyberspace is a fact of daily life. Until recently, this arena of virtual interaction was considered largely a matter of *low politics*—the routine, background, and relatively non-contentious. Today cyberspace and its uses have vaulted into the highest realm of *high politics* – the most salient and contentious forms of interaction. We now appreciate that cyber capabilities are also a source of vulnerability, posing potential threats to national security, and disturbing the familiar and traditional international order. The expansion of cyber access has already influenced the Westphalian-anchored international system in powerful ways.

This paper argues that the construction of cyberspace is creating new challenges for the social sciences, the full nature of still remains to be fully understood -- perhaps even calling into question some of its most basic assumptions. We frame these challenges with reference to co-evolution of the new cyber domain and the traditional international system, and then focus more specifically on the emergent synergy between two independent features of the contemporary world order -- cyberspace (an arena of interaction) and sustainability (a policy imperative), and their convergence on the global policy agenda It is no surprise that sustainability is closely connected to security – or alternatively that security is contingent on sustainability. By extension, cyber security is derivative, in that is refers to security in the cyber domain.

II. Cyberspace and International Relations

Many features of cyberspace challenge traditional understandings of contemporary international relations theory, policy, and practice. Most notable are the following specific features of cyberspace (based on Choucri. 2012:4).

- *temporality* (replaces conventional temporality with near instantaneity)
- *physicality* (transcends constraints of geography and physical location
- *permeation* (penetrates boundaries and jurisdictions);
- *fluidity* (sustains shifts and reconfigurations);
- *participation* (reduces barriers to activism and political expression);
- *attribution* (obscures identities of actors and links to action); and
- *accountability* (bypasses mechanisms of responsibility).

Individually, each factor is at variance with our common understanding of international realities. Jointly, they create powerful disconnects that impinge upon, if not contradict, the concept of sovereignty and the vertical structures of power and influence. So too, the traditional systems of international relations generally framed in hierarchical power relations—bipolar, multipolar, unipolar and the like—may not be congruent with these new features of the virtual system of international relations. This is a system with increasing diversity of individual, groups, and non-state actors – all expressing *voice* and exerting *influence* in a context of decentralization, localization, and asymmetry in modes of advantages, power, and influence.

Together, the increase in cyber access worldwide, the growth in voicing, global civil society, and the new economic and political opportunities afforded by cyberspace are critical drivers of ongoing realignments in power and politics. Most importantly, they have already assumed constitutive influence of their own. At the same time, as the sovereign state seeks to exert influence and extend power and control over the cyber domain, it seeks it seeks to reproduce the traditional and familiar ecology and its attendant demography and systems of authority.

2.1 Cyberspace – New Domain of Interaction

From a social science perspective, cyberspace is a constructed context of interaction. Elsewhere, we explore the cyber domain in greater depth (Choucri, 2012); here we note only that, with the Internet at its core, cyberspace is:

- Created through the interconnection of millions of computers by a global network such as the Internet.
- Built as a layered construct, where physical elements enable a logical framework of interconnection that
- Permits the processing, manipulation, exploitation, augmentation of information, and the interaction of people and information.
- Enabled by institutional intermediation and organization, and
- Characterized by decentralization and interplay among these actors, constituencies and interests.

The figures that follow help illustrate salient features of cyberspace in terms of ecology, demography, and modes of behavior. For the most part they reflect basic parameters and evolution of time. They also reveal some notable background conditions.

In Figure 1 we present the global trends of enabling devises and technologies from 2001-2011 – the first full decade of the 21st century – and shows the dramatic growth of mobile cellular subscriptions. (Note the trend for fixed telephone service, a major technology of the 20th century).

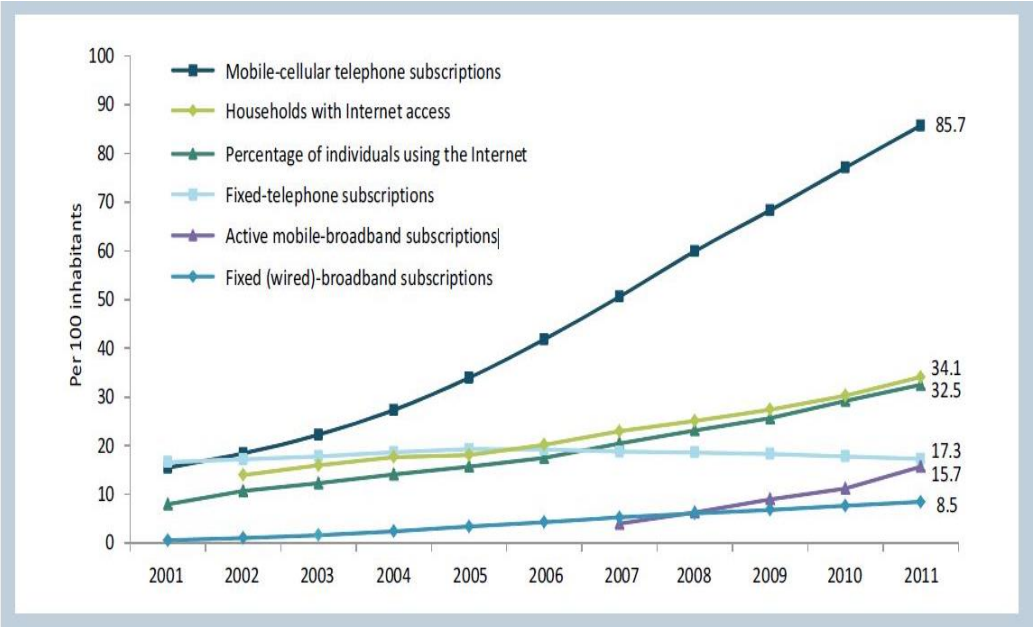


Figure 1: Global ICT developments, 2001 – 2011.
Source: International Telecommunication Union. 2012. *Measuring the Information Society: Executive Summary.*

A closer look at the trends in mobile cellular subscriptions, in Figure 2, signals both distribution and rates of change.

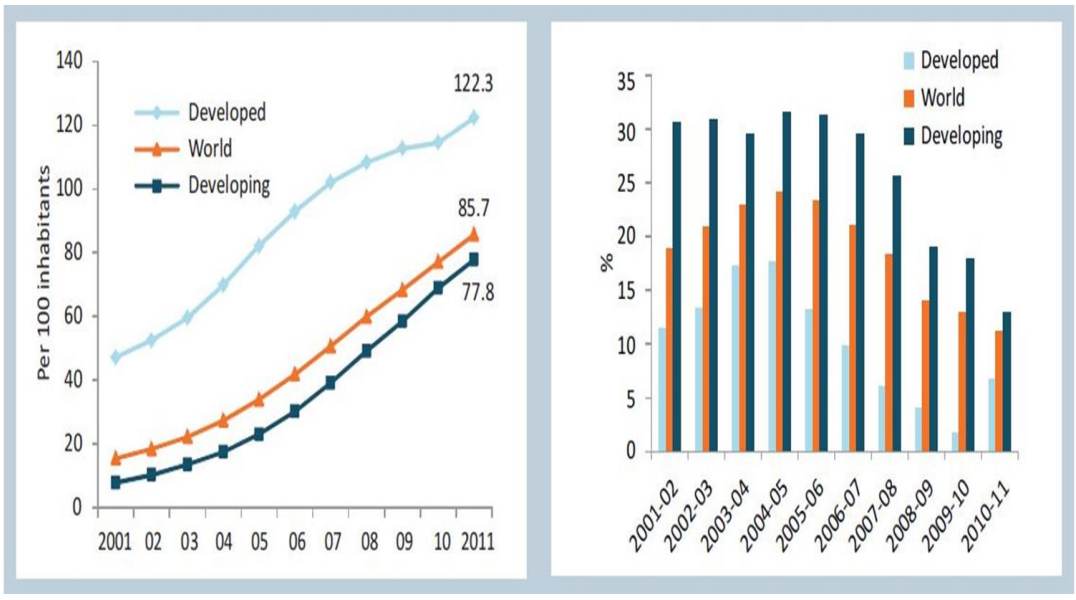


Figure 2: Mobile-cellular subscriptions, 2001-2011, world and by level of development, penetration (left) and annual growth (right).
Source: International Telecommunication Union. 2012. *Measuring the Information Society: Executive Summary*

Far more impressive are the trends in Figure 3 that shows the dominance of the developing countries in their adoption of mobile cellular communication devises. At a minimum, these trends can be seen as a reduced gap between developed and developing societies.

Figure 3: Percentage of individuals using the Internet, 2001-2011, world and by level of development, penetration (left) and annual growth (right).
Source: International Telecommunication Union. 2012.
Measuring the Information Society: Executive Summary

Figure 4 shows four different views of the cyber domain, at least three of which reflect more 'behavioral' features rather than attributes or characteristics. They show different levels of cyber access, as well as different modes of participation. Captured in Figure 4 is information that is at variance with the traditional power calculus of international system – and points to asymmetries in the physical as well as the cyber domains.

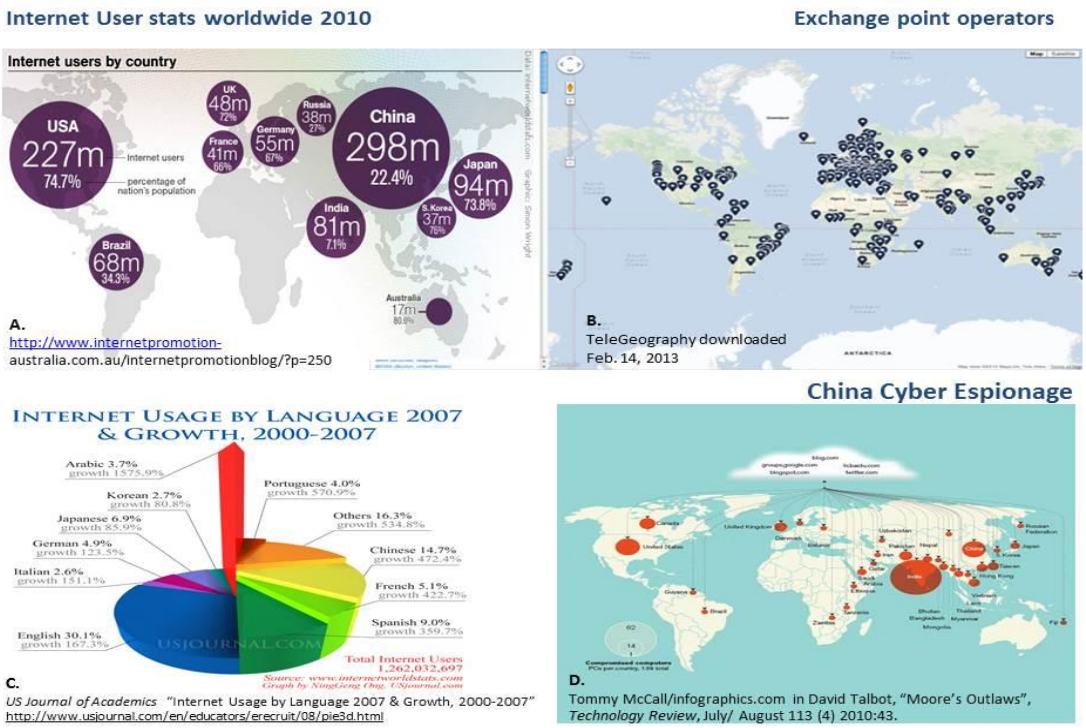


Figure 4: Four Views of the Cyber Domain

Sources: A. http://www.internetpromotion-australia.com.au.internetpromotionblog/?p=250

B. TeleGeography. Downloaded Feb 14, 2013

C. *US Journal of Academics*. "Internet Usage by Language 2007 & Growth, 2000-2007". http://www.usjournal.com/en/educators/erecruit/08/pie3d.html

D: Talbot, David. (2010). "Moore's Outlaws." *Technology Review*, 113 (4) pp. 36-43.

While quadrant D in Figure 4 shows the features attributed to Chinese cyber espionage, this quadrant does little justice to the emergence of various forms of threats to cyber security -- by many actors and contexts -- coupled with increasingly diverse types of cyber-based conflicts. Accordingly, we show in Figure 5 select features of cyber malevolence on a global scale.

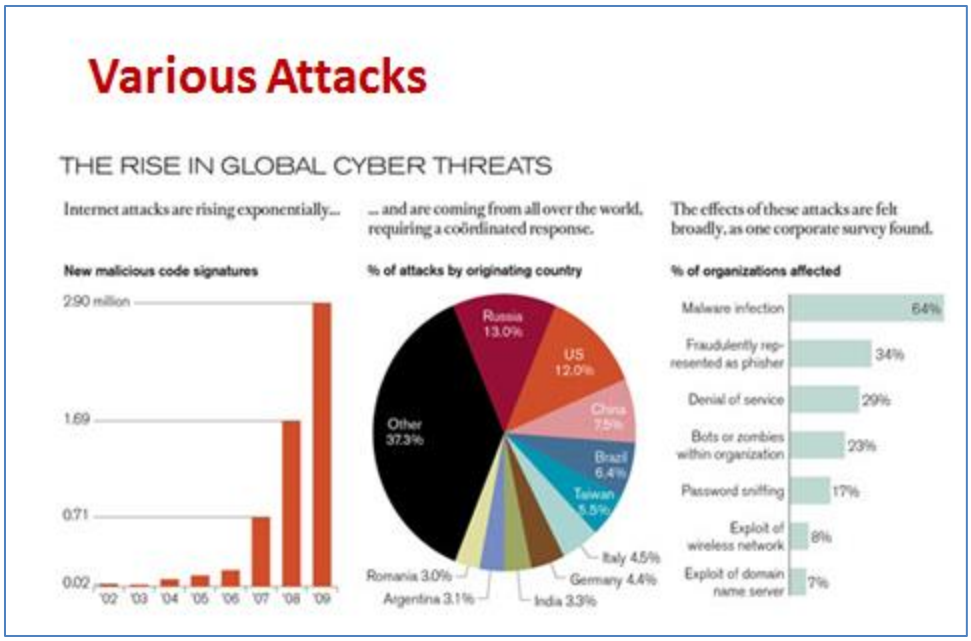


Figure 5: Various Attacks: The Rise in Global Cyber Threats.
Source: McCall, Tommy/Infographics.com in Talbot, David. 2010. "Moore's Outlaws." *Technology Review*, 113(4): 43.

2.2 Cyber Impacts on International Relations

The expansion of cyber access has already influenced the Westphalian state and its international system in powerful ways. Here we select ten of the most notable impacts distributed across three major trajectories of change (adapted from Choucri, 2013).

New Actors – New Threats – New Conflicts

***One*:** Empowerment of *new actors*—some with clear identities and others without—but all with opportunities for growth. Among these are national entities that exercise access control or denial, non-state commercial entities with new products and processes, agents operating as proxies for state actors, new novel criminal groups often too varied to track and too anonymous to identify—over and above the emergence of new and unregulated markets.

Two: Novel types of *asymmetries* shift traditional power relations and create new opportunities for weaker actors to threaten stronger ones, for various uses of cyber-anonymity, for new cyber venues of political, industrial or military activity, and for expansion of criminal activities—to note only a few examples.

***Three*:** New challenges to *national security*, from sources of vulnerability without precedent (cyber threats), new dimensions of national security (cyber security) coupled with uncertainty, fear, and threat from unknown sources (attribution problem).

Four: Diverse forms of *cyber conflicts* and *contentions* create new challenges to the stability and security of the state system, such as the militarization of cyberspace, the conduct of cyber warfare, threats to critical infrastructures, undetected cyber espionage and so on.

New Institutions -- New Decision-Actors – New Demand for Cooperation

Five: Unprecedented growth and power of *institutions for cyber management*, largely private entities created specifically to enable and manage cyber interactions (such as Internet Corporation for Assigned Names and Numbers and Internet Engineering Task Force), or to help support cyber security (such as Consortium for Electric Reliability Technology Solutions).

Six: Significant push-back by *traditional international institutions* (such as the International Telecommunications Union) who question the legitimacy of the new institutions for the management of cyberspace.

Seven: Increased *density of decision makers* for cyber domain with unclear mandates and overlapping job descriptions create new ambiguities that obscure responsibility, question legitimacy, and enhance uncertainty.

Eight: New demand for *cyber cooperation* to contain the growth of cyber conflicts further reinforced by a growing push for framing global cyber norms.

Emergent Dynamics – Global Transformation – Coupling of Cyber and "Real"

Nine: The *new coupling* of politics in the traditional and cyber domains shape new strategies based for cross-domain leverage and bargaining that are seldom consistent with conventional practice (such as the Stuxnet—the computer worm that attacked Iran's nuclear reactor).

Ten: *The transformative effects* of cyber access permeate all levels of analysis in international relations—the individual, the state, the international system, and the global system—including transnational and non-state actors, for profit and not for profit.

Given these are all aggregate trends, what can be said about the implications of cyberspace at different levels of analysis in international relations?

2.3 Revisiting "Levels of Analysis"

Given the above, it should be no surprise that the cyber impacts are already apparent at all levels in international relations – along the same general trajectories highlighted above. To note the most obvious (summarized from Choucri 2012):

The Individual: New Power—New Possibilities

Cyberspace enables and empowers the individual in unforeseen and diverse ways. Cyber interaction facilitates formal self-definition as well as the individual framing of political stances.

By participating in cyber venues, individuals pursue and may even achieve new freedoms. The individual—alone or in groups—can seriously threaten established authority in unprecedented ways (as in early phases of the 2011 Arab revolts).

Clearly, cyber-based interactions do not replace traditional forms of interest articulation and aggregation, nationally or internationally. However, they serve as effective conduits to challenge the established order. Note the recent Wikileaks episode, for example. The state is not likely to accept, or even accommodate, such trends.

The State System: New Challenges—New Opportunities

The state remains the basic unit of organization for the international system—the major actor in international politics. While the creation of cyberspace provides new opportunities, it also creates uncomfortable situations often seen as sources of threat.

On the one hand, states have not hesitated to use cyber venues for the delivery of social services—with varying degrees of success that depend on the reliability of cyber access, the clarity of purpose, and the specificity of operations. While we would expect industrial states to excel in the use of cyber venues, we already observe leapfrogging initiatives by the other states. In addition, the relatively strong positive relationship between the performance of e-government and the perceptions of government effectiveness signals that something is indeed happening on the ground (Choucri, 2012).

On the other hand, states have not been slow to control access to cyber venues and, when possible, to prosecute presumed offenders. Many governments have used cyber venues to exert their influence and pursue their own security by increasing the insecurity of their critics or detractors. Some go to great lengths to limit the exposure of their citizens to messages deemed undesirable. In response, we have seen the construction and growth of anonymous proxy networks to provide structural intermediation of routing mechanisms that mask the identity of sender and receiver, such as the TOR system with its software that enables anonymity and inhibits surveillance (Rady, 2013).

From a social science perspectives , these various trends points to the need for new view of national security—one that extends beyond conventional concerns of protecting borders against unwanted military intrusions and takes into account security threats from the cyber domain. The state must now protect the security of its own cyber systems and capabilities, as well as defend against uses of cyberspace to undermine its overall security, stability, and sustainability. Recognizing that cyberspace has become a is a war-fighting domain, the world's major power, the United States, has centralized command of cyberspace operations and coordinate defense military networks by creating the U.S. Cyber Command. Several other countries have followed suit.

The International System: Density, Diversity, and Decision

A major challenge to traditional international relations, theory, practice, and policy lays in the fact that cyberspace—with its ubiquity, pervasiveness, and global reach—is managed almost entirely by the private sector. This reality can only be understood in the historical moment when the dominant power, the United States, delegated to the private sector the operational

management of cyberspace. The decision was made by the sovereign that initiated, conceived, designed and constructed cyberspace. We are now observing some push-back from different actors and agents around the world. This too may be anticipated by traditional theory, but with little insight about the potential outcome.

Almost all international institutions have extended their reach and performance by using cyber tools and capabilities. Little in this trend is surprising, except perhaps the speed at which the use of cyber access is taking shape. With the growth of international organizations and trends in the new global agenda (notably the *Millennium Development Goals*), institutional linkages within and across both state and non-state bureaucracies and agencies have assumed increasingly greater complexity. Although states are the stockholders in international governance, non-state actors and other stakeholders resort to cyber venues for interest articulation and aggregation decision forums. Various non-state groups have been accorded observer status or otherwise allowed to participate in international forums, with no decision-making capacity, but may well influence the outcomes.

What does international relations theory have to say about this? U.S. dominance in the Internet's construction and management is entirely consistent with *realist theory*, which focuses on state power and national security, as is the challenge from ascending states. The push-back is consistent with *institutional theory*, which concentrates on coordinated and routinized international behavior. *Constructivists* might say that all of this is in the eye, and interpretation, of the beholder.

None of these theories address dynamics of change head on, however, consistent with the logic proposed by Gilpin (1987). We expect that, in the short run, uneven patterns of cyber access will continue to reflect the distribution of power in the international system. Over time, the diffusion of cyber capabilities worldwide will expand political participation, enhance politicization of both idiom and action, and increase competition for influence and control over the management of cyberspace. In the long run, these pressures will shape new ways of exerting power and leverage, create new structures and processes, and frame new demands for cyber norms—all of which will reflect the demography, capability, and values of the emergent cyber constituencies.

The Global System: All-Encompassing Commons

In principle, the global system refers to the Earth, its population, geological and geopolitical features, all life-supporting properties, and, now, to cyberspace as well. We have already seen the politicization of both the natural environment and the manmade cyber arena. We hardly expect that to change on short order. More to the point, however, we already see the emergence of a global civil society whose concerns and interests transcend the traditional levels of analysis and addresses the global system and its contours.

What is also novel for international relations theory, policy, and practice is the provision of public goods at the global level, a trend that is not created by cyberspace. An immediate follow-up concern, then, pertains to the rules and institutional mechanisms for such provision. However, when cyber venues are used to pursue global objectives via international institutions, a

whole new set of challenges emerges. Yet to be seen is the extent to which this shapes *who gets what, when,* and *how*—as well as who decides on each of these issues.

All of this rests upon, and strengthens, the vertical linkages—connecting global and local—transmitting information, communication, and knowledge building to and from the grass root. Some of these linkages are converging to reinforce the notion of a global civil society. Not surprising, this reinforces nascent calls for global accord on operational goals and cyber norms.

III. New Imperatives of the Global Agenda

In the most general terms, the global agenda in the early decade of the 21st century refers to the institutional priorities of the international community and the proposed actions to be undertaken in order to meet agreed upon goals. Such goals pertain to the improvement of the human condition, the enhancement of security for individuals and societies, and the reduction of threats to the global system and all of its constituent elements.

Over the past decades, the global agenda has concentrated increasingly on the quest for sustainability -- a new policy trajectory that departs from the traditional theories, models, and practices of economic growth that dominated the twentieth century. The global burden of growth in itself constitutes the empirical basis of the sustainability imperative. The politics—and the cyberpolitics—of sustainability revolve around achieving greater clarity and understanding of effective ways of meeting social needs. In the course of this process, the international community is revisitng the conventional parameters shaping *who gets what, when, how, and why.*

3.1 Cyberspace and Sustainability

The separate processes shaping cyberspace and the imperatives of sustainable development all converged early in the twenty-first century. This convergence, unexpected as it is, results mainly from the properties of cyberspace (as we know it) and those of sustainability (as we seek to frame it); it has been reinforced by the role of knowledge in international forums. Interestingly, both cyberspace and sustainability are relative newcomers to international relations theory, policy, and practice. They are also the subject of debates over uncertainties. Above all, they are powerful manifestations of the sources and consequences of growth, expansion, and globalization.

The logic for exploring the synergy between cyberspace and sustainability can be described in the terms of inquiry in *The Social Life of Information* (2000), by John Seely Brown and Paul Duguid. In this book, Brown and Duguid identify six forces unleashed by advances in information technology (IT) which they consider to be fundamental correlates of cyber venues that altered the social fabric in new and powerful ways. These consist of:

- demassification,
- decentralization,

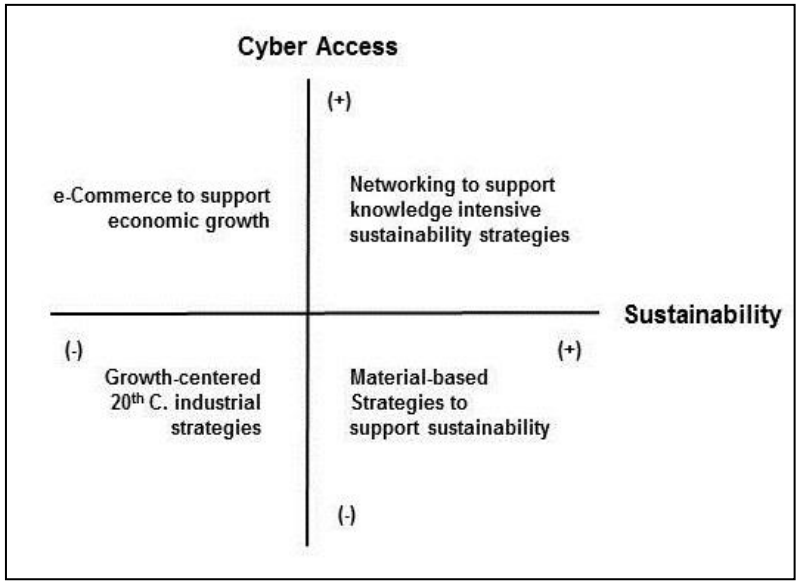
- denationalization,
- despatialization,
- disintermediation, and
- disaggregation

Brown and Druid argue that these forces, we call here the "6 D's," are critical and distinct properties of the cyber context. Although they do not address growth, development, or sustainability, it is not too much of a stretch to assign these same forces central roles in the nascent domain of sustainable development. At the very least, massification, materialization, spatialization, and centralization reinforce the ways in which human beings continue to stress and damage the natural environment. None of the stresses or impacts is intentional; rather, they are largely the by-products of routine human activities. These are also six features of social systems that support the sustainability agenda.

Of course, neither cyberspace nor sustainability can be reduced to the 6 D's; nonetheless, while any alternative to continued growth will involve a great deal of dematerialization, we cannot yet argue that an expansion of cyberspace will also have the same effect. As a practical matter, the 6 D's, individually and jointly, are currently located at the periphery of contemporary theory in terms of social relations, political behavior, power politics, and economic growth.

To illustrate the synergy – in theory and in practice -- we identify in Figure 6 four cases across the issues of cyber access and the sustainability *problematique*. Each entry shows different situations in policy and practice and different modalities of the synergy at hand.

Figure 6 Modes of Synergy – Cyberspace and Sustainability



Source: N. Choucri *Cyberpolitics in International Relations* MIT Press, 2012: 207

Sustainability is understood to be of relevance to all societies everywhere, and the new international initiatives surrounding transitions toward sustainability are being supported by efforts to expand cyber access. As an arena of interaction, cyberspace has created greater potential for a world of reduced material use, greater efficiencies in all activities, and improved environmental conditions. International institutions have taken the lead in arguing for the deployment of cyberspace in support of sustainability strategies.

3.2 Convergence on the Global Agenda

With the convening of the World Summit on the Information Society (WSIS), a clear connection was forged between sustainability issues and the pursuit of information-related objectives. This connection reinforces and is reinforced by *the Millennium Development Goals* promulgated by the United Nations.

The WSIS is especially relevant for our purposes as it was established to bring information technologies and cyber functionalities to bear on the challenges of development, specifically strategies to reduce poverty. The conference became a major landmark in the establishment of global accord, and with its explicit mandate for facilitating developmental strategies, the synergy between cyberspace and sustainability took on an institutional form. It will be remembered more for its introduction of a new issue on the evolving agenda for international collaboration than for its immediate effects. That the virtual is now formally recognized as a domain for institutionalized international collaboration is itself evidence of the salience of the critical nexus at this point in time.

At the same time, the WSIS exemplifies cyberpolitics in international relations par excellence. The WSIS focused on the broad use of IT, with the assumption that greater use of available technologies would enable increased access to content worldwide. In practical terms, it established a direct connection between advances in information and communication technologies, especially the forging of cyberspace, and the new global priorities focusing on transitions toward sustainable development. An important WSIS target is to render half the world's population cyber accessible by the year 2015.

The Declaration of Principles formally tied the WSIS initiative to the UN's Millennium Development Goals. What appeared initially as a technologically oriented summit rapidly took on many features of cyberpolitics. For example, the summit contributed to the mobilization of civil rights groups that did not feel the digital divide was of particular salience and argued that by bringing the Internet and technological advances to less-developed countries, the UN would be denying the rights of citizens to live as they always had, without that technology. Similarly, participants could not agree on the role of Internet technology in governance within states (i.e., e-governance).

The second phase of the WSIS took place in Tunis, Tunisia, on November 16–18, 2005. The official goals were to create an ongoing strategy for resolving the critical differences in cyber access worldwide and to develop a plan to provide affordable Internet access to 50 percent of the world's population by 2015. This segment of the WSIS undertaking, too, was not

devoid of political contentions. Nonetheless, The international community agreed that the progress of each country should be evaluated periodically to ensure that each country was reaching its goals as agreed upon at the summit. Phase 2 concluded with the Tunis Commitment and the Tunis Agenda for the Information Society. The Tunis Commitment (that affirmed a commitment to building an information society) and The Tunis Agenda for the Information Society (that focused on specific actions and endorsed increasing multilingualism online to facilitate the retrieval of information and knowledge by anyone and anywhere)..

In sum, the two segments of the WSIS provided the mechanism through which information technologies and cyber venues were jointly embedded in a common institutional fabric and international processes shaping the future of the global agenda.

3.3 Millennium Development Goals

The WSIS process was designed to address the Millennium Development Goals, thus reinforcing the connection between development challenges and applications of information technology. The MDGs provide institutional connection between the vision in *Agenda 21* and the goals of the WSIS initiative.

As with the UN's *Agenda 21,* the MDGs are statements of general principles, intents, and directions of action. They illustrate a gradual shift away from problem definition to shared responsibility. But they are not legally binding. Rather, they express specific goals, with reference to targets for attainment by 2015. Interestingly, the MDGs reflect the view of the global *problematique* from the perspective of the disadvantaged populations. Achievement of the goals would result in the eradication of extreme poverty, universal private education, increased gender equality for women, reduced child mortality, better maternal health, arrested trends in major diseases, greater environmental sustainability, and collaborative partnering strategies for development -- to highlight key elements. These rounds of global accords illustrates the important learning process, for example:

- Since the MDG goals are the outcome of negotiation among diverse states and non-state actors, the result demonstrates broadening participation in global discourse.
- Since states are required to report on their performance toward attainment of the MDG targets, the result is to create roots of accountability.
- Since non-state agencies, the business community, the IT industry, and other interests involved in the framing, formulation, and conduct of the WSIS all participated under the auspices of a UN task force, the result is to legitimize the process as well as the expected products.
- Since both the preparatory phase for the WSIS and the eventual follow-up were designed to buttress the MDGs, the result is an emerging institutional connection between the nature of the development challenges and the empowering potentials of cyber access for facilitating responses to recognized challenges.

At the same time, however, this learning process has direct implications for the security at all levels of analysis – the individual, the state and society, the international system and the global system. All of this illustrated one of the new challenges challenge for the social sciences, namely, how to best address the matter of security in the most comprehensive and overarching terms – in both the traditional and the virtual contexts. But there are other challenges as well. –

IV. New Challenges for the Social Sciences

The social sciences were developed to understand human behavior and social interactions. They were built by carefully separating humans from nature, and then segmenting modes and types of human activities. Social scientists have focused on and excelled in investigations of the properties – structures and processes – of social systems. The remarkable advances in the social sciences could not have taken place without such differentiations.

4.1 Systems of Interaction

At this point, we recognize that that humans are embedded in three distinct systems, each with its specific properties:

(i) the social system (that we are all accustomed to and has been the focus of the social sciences),

(ii) the natural system (the life supporting properties that affect and are affected by human activities) and

(iii) the cyber system (the constructed arena of human interaction we call cyberspace, and whose distinctive properties we noted early on).

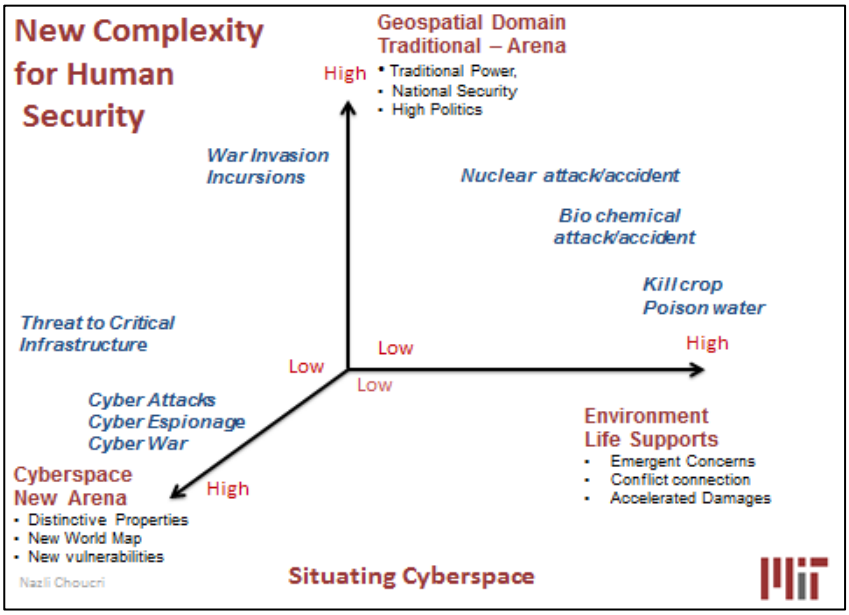
The critical point is that individual and societies require – and even depend upon -- the security and sustainability of all three systems. The social sciences must now address the interaction among these three systems.

4.2 Complexity of Security and Sustainability

The traditional conception of security --- individual, natural, and international – is security connected to matters of military defense and protection of the borders. More recently, this has been augmented by taking into account the sustainability of the entire social system. The imperatives of the environmental system and the integrity of its life supporting properties constitute a distinct trajectory with dominant properties that are not constructed by humans. Its sustainability is essential for the survival and security of the social system. The new, constructed system of social interaction, cyberspace, has characterized by properties that include those noted at the onset of this paper. Figure 6 shows the combined trajectories of the three systems – social,

environmental and cyber – and some illustrative activities or conditions associated with each.

Figure 6: Situating Cyberspace



Source: N. Choucri, "Dimensions of Security" ECIR Project, MIT: 2013.

Consistent with the synergy between cyberspace and sustainability—and their convergence on the global agenda, we note that we have as yet little consensus on these issues or on what constitutes data, analysis, cases, comparisons, or any of the usual tools of inquiry in the social sciences applied effectively to for cyberspace. While environmental metrics have been developed, they are usually dealt with in, or in the context of the social system – but seldom with reference to, or compared with, cyber-metrics. At the same time, cyber metrics remain to be examined in conjunction with social or environmental metrics or contexts. Such an undertaking would amount to a major challenge for the social sciences.

4.3 Demand for New Knowledge

Concurrently, the growing demand for new knowledge to help manage transitions toward a sustainable future further reinforces the relevance of cyberspace in the process and its connections to the other trajectories of security and sustainability. To increase the likelihood of the anticipated shift toward knowledge-intensive sustainability solutions, and in a situation of relatively underdeveloped scientific and technological foundations for sustainable development, it is imperative that existing knowledge of all types be readily accessible to interested communities everywhere. Over time, we expect access to cyber venues to reinforce the synergy and to improve performance along the cyber and the sustainability trajectories

We propose to draw on lessons developed through analysis of the sustainability *problematique* that are highly relevant to cyberspace in an international frame of reference. The lessons are derived from experience with the Global System for Sustainable Development (GSSD), a multilingual knowledge system focusing on the uses of cyber venues for knowledge provision, access, and retrieval, with particular emphasis on all aspects of sustainable development.

The GSSD ontology system was designed at a time when sustainable development was a new issue in both the scholarly and the policy communities, with little foundational knowledge or empirical grounding. The GSSD ontology of sustainability is anchored in the master variables—population, resources, and technology—and their constituent elements, rooted in an integrated theoretical framework, and rests on empirically based core organizing principles. The ontology was anchored in four features associated with diverse facets of the master variables and their disaggregation:

- types of human activities,
- known problems associated with human activities,
- types of problems associated with each activity,
- scientific and technological solutions to known problems,
- socioeconomic and national policy responses to known problems.
- coordinated international action

Each feature is unbundled into a set of nested subcategories. The overall ontology is then completed and bounded by types of coordinated international actions.

Whether these factors constitute essential elements of a viable solution strategy for understanding and tracking cyberpolitics in the longer run, and whether the strategy is scalable and portable, remain to be seen. Based on the GSSD initiative, we believe that this approach can be generalized and applied to many other issues and aspects of cyberpolitics in international relations. Karl W. Deutsch observed that relevant knowledge depends on four things: the interests of the knower, the characteristics of situation to be known, the methods by which situation features can be determined, and the "system of symbols and physical facilities by which the data selected are recorded and used for later application" (Deutsch et al. 1957, 5–6).

So, too, any understanding an issue or problem involves more than just producing a good representation of it; it also requires taking into account relevant situational features. The GSSD lessons are especially relevant in light of the coevolution of cyberspace and sustainability on the global agenda. In these areas as in others, broadening the discourse about any issue area—the problems, the issues at stake, the questions to be addressed, and the designing of solution strategies—will enhance its understanding and the wisdom that comes with it.

At the same time, the tendency to focus on the uses of knowledge underestimates the power inherent in its reuses. Exploiting two characteristics of knowledge, complementarity and leakage, contributes to our understanding of "the potential for virtuous and vicious circles" (Easterly 2002, 153).

More important, there is as yet no comprehensive view of the ways in which major forms of human activities within the cyber domain generate problems that bear on both the cyber and the traditional arenas, nor is there a coherent understanding of various solutions, social or technical. Providing a systematic and internally consistent conceptual map is a step in the direction of intellectual order and coherence, one that serves as an important means of unbundling the knowledge content of sustainable development. Google provides excellent search functions but does not provide content organization services, nor does it seek to do so.

For these reasons, the role of a domain *ontology* in the cyber context is very important. This means to establish knowledge coherence and organization by identifying an internally consistent method for determining, identifying, and connecting different facets of the issue in question in an empirically verifiable way). An ontology itself carries several specific benefits.

The first is *conceptual:* in light of the increasing importance of cyberspace, a holistic and integrative view buttressed by constituent elements and their linkages would be a major step in constructing knowledge about the constituent elements of cyberspace and cyberpolitics, and about the interlinkages.

The second is *strategic:* an ontology of the cyber-international relations domain facilitates navigating through the growing volume of potentially relevant materials and enables access to cutting-edge analysis, innovative technologies, and multidisciplinary knowledge.

The third benefit is *cohesion*: defining the dimensions of cyber-based actions and reactions provides varieties of perspectives and signals situations in which the solution to one problem becomes the source of another.

The fourth is *functional*: it helps guide the use and reuse of knowledge, and update understandings as needed.

The fifth benefit is *operational*: ontology is central to the design of web-based systems for the management, e-distribution, and sharing of knowledge devoted to the issues in question. All of these features are important in the development of new knowledge.

It is increasingly important that knowledge users as well as knowledge providers from various parts of the world express themselves in appropriate languages and idioms, using appropriate concepts and terms. As noted earlier, while English remains major language, it is rapidly declining. Thus, an added relevance of GSSD is that it operates in two non-Western languages, Arabic and Chinese, as well as in Spanish.

V. End-Note

The construction of cyberspace surely ranks as one of the most important products of human ingenuity during the last part of the 20th Century. The expansion of cyber access and cyber participation will also rank among the most remarkable examples of technological diffusion and adaptation throughout human history. Early in this paper we noted some specific

features of cyberspace that are at variance with current conception of social interactions and social order known to the social sciences, in theory and in practice. The features – which we have referred to earlier as temporality, physicality, permeation, fluidity, participation, attribution and accountability – are particularly vexing in the context of international relations. They undermine the very principles of international order, such as sovereignty, jurisdiction, boundaries, to note only a few. And, as noted earlier, the remarkable growth in cyber access affects all levels of analysis in traditional international relations – the individual, the state and non-state actors, the international system, and the global system – often in profound and potentially irreversible ways.

It is tempting to interpret recent trends in cyber access as evidence of "leveling the playing field" in international interactions. We have yet to formalize concepts of cyber power, cyber conflict or cyber warfare, in relation to their functional counterpart in the traditional order. So, too, the powerful role of deterrence in conventional strategic interactions is not readily portable to the cyber domain.

The ecology of the cyber sphere is not fully understood, nor is the entirety of its shifting parameters. By contrast it appears that interaction in the virtual domain is creating a cyber-demography that may well be approximating that of the traditional world. We have not yet engaged in a systematic comparison of the "real" and the cyber domains, but we can infer that there are likely to be some powerful differences – beyond the features noted at the onset

This possibility framed an important question for the social sciences: To what extent is the knowledge we have built, the theories we have developed, and the methods of inquiry we have utilized portable from the traditional arena to the cyber domain?

In this paper we do not address this question head on, but we do note some specific challenges to the social sciences. Some are due to the differences between the cyber arena and the traditional social order. Others are due to advances in the social sciences that must now take into account the cyber domain as well. Still others are due to our improved understanding of the social order and its contextual features.

If there is one effect of cyberspace that turns traditional understanding of power and influence in world politics "on its head", it is the empowerment of the individual. Not only does the individual "voice" matter, action can follow "voicing" – and, most remarkably, bypassing the constraints of boundaries, territoriality, jurisdiction or other defining features of the traditional world order.

Not discussed in this paper are aspects of social interaction in the cyber domain that appear to be entirely consistent with the traditional order. Market mechanisms have long been established in the domain, a development that would be considered valuable on all counts. Concurrently we have seen the growth of markets in malware, clearly less desirable but especially difficult to control given the anonymity factor that impedes any effective accountability.

In retrospect, it is clear that the state and the state system itself is a newcomer in the cyber domain. The Internet has been managed by the private sector. State instruments and

regulations played little role early on and still lag in the larger scheme of things. But the state is rapidly extending is influence – with different states manifesting this extension in different ways – despite the attendant constraints. Scholars of international relations schooled in assumptions of the dominance of the state and state power may find these assumptions at variance with the salience of private sector in management of the cyber sphere.

The state system of the 21st century is embedded nearly as much in the cyber domain as it is in the natural environment. Put differently, and perhaps more accurately, the state cannot extract itself from its natural environment and it is not likely that is could insulate itself from the cyber arena. For the social sciences, the question is: does this matter? If so how? If not, why not?

References

Brown, John Seely, and Paul Duguid. 2000. *The Social Life of Information*, Cambridge, MA: Harvard Business Press.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*, Cambridge, MA: MIT Press.

Choucri, Nazli. 2012. "Cyberpolitics in International Relations," in Joel Krieger (ed.), *The Oxford Companion to Theoretical Economics (TE),* (pp. 267-271), New York: Oxford University Press.

Choucri, Nazli. 2013, Spring. "Cyberpolitics in International Relations." *précis,* MIT Center for International Studies. http://web.mit.edu/cis/precis/2013spring/cyberpolitics.html#.Ue_4ddLijh4

Choucri, Nazli. 2013 "Dimensions of Security", ECIR Project, MIT.

Deutsch, Karl W., S.A. Burrell, R.A. Kann, M. Lee, Jr., M. Lichterman, R. E. Lindgren, F.L. Loewenheim, and R.W. van Wagenen. 1957. *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience,* Princeton, NJ: Princeton University Press.

Easterly, William. 2002. *The Elusive Quest for Growth: Economists' Adventures and Misadventures in the Tropics*, Cambridge, MA: MIT Press.

Friedman, Allan, Tyler Moore, and Ariel D. Procaccia. 2010. "Would a 'Cyber Warrior' Protect Us? Exploring Trade-offs Between Attack and Defense of Information Systems." *Proceedings of the 2010 New Security Paradigms Workshop*. Concord, MA (pp. 85-94).

Gilpin, Robert. 1987. *The Political Economy of International Relations*, Princeton, NJ: Princeton University Press.

Kello, Lucas. 2013. "Cyber Disorders: A Field in Technological Sleep," *International Security*, 38 (2).

Nye, Joseph S. Jr. and Jack Landman Goldsmith. 2011. "The Future of Power,"

Rady, Mina. 2013. "Anonymity Networks: New Platforms for Conflict and Contention." MIT Political Science Department Research Paper No. 2013-5. March 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2241536

Sechrist, Michael, Chintan Vaishnav, Daniel Goldsmith, and Nazli Choucri. 2012. "The Dynamics of Undersea Cables: Can the Old Modes of Governance Cope with New Demands of the Cyberspace?" *Proceedings of the 30th International Conference of the System Dynamics Society*, Elke Husemann and David Lane (eds.). St. Gallen, Switzerland. July 22-26, 2012.

Vaishnav, Chintan, Nazli Choucri, and David D. Clark. 2012. “Cyber International Relations as an Integrated System,” Presented at the *Third International Engineering Symposium*. CESUN 2012, Delft University of Toronto, June 18-20, 2012.