Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

Cyberpolitics in International Relations

Nazli Choucri

Professor, Political Science Department
Massachusetts Institute of Technology

Spring 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.

CyberPolitics in International Relations

CYBERPOLITICS, a recently coined term, refers to the conjunction of two processes or realities—those pertaining to traditional human contentions for power and influence (*politics*) surrounding the determination of *who gets what*, *when*, and *how*, and those enabled by a constructed domain (*cyber*) as a new arena of human interaction with its own modalities, realities, and contentions.

Created with the Internet at its core, 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*. It has become a venue of unprecedented opportunity, a source of vulnerability, a disturbance in the familiar international order, and a venue of potential threat to national security.

Many features of cyberspace are reshaping contemporary international relations theory, policy, and practice. Among these are: *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 feature is at variance with our common understanding of social reality. 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, or unipolar structures—may not be congruent with these new cyber features with the increasing diversity of individual, groups, and non-state voices and influence in an international context characterized by decentralization, localization, and diverse asymmetries in modes of leverages, power, and influence.

In short, the dramatic expansion of cyber access worldwide, the growth in *voicing*, global civil society, and the new economic and political opportunities afforded by cyberspace are critical drivers of the ongoing realignments. And, most important of all, they have already assumed constitutive features of their own. At the same time, however, some of the emergent features of the 21st century state system are reflected in the cyber domain as well (See Figure 1).

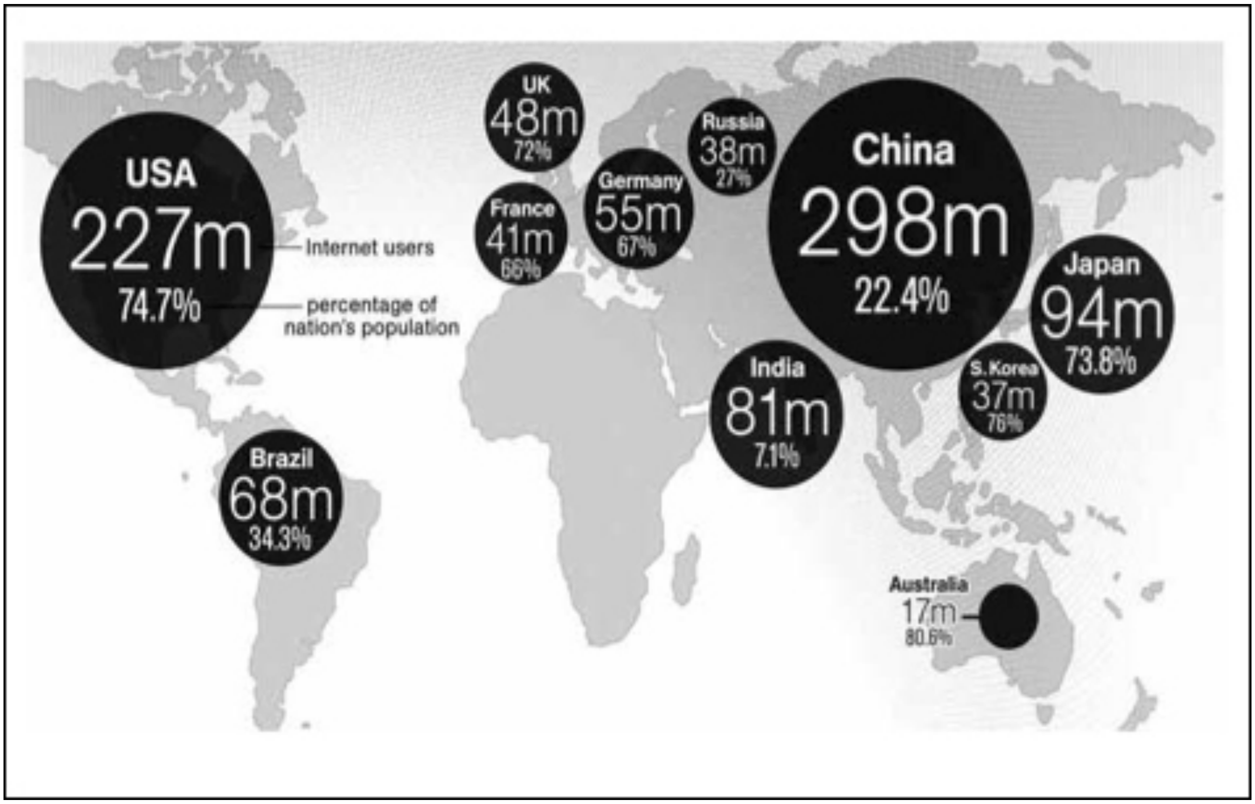

Figure 1: Worldwide Internet user statistics, 2009. Source: July 29, 2009: Sydney, NSW. A News.com.au graphic of Internet users by country as of 2009. Pic. Simon Wright. © Newspix.

International Relations

The expansion of cyber access has already influenced the Westphalian state-based international system in powerful ways. Among the notable impacts are the following:

1. 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).
2. 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.
3. 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.
4. 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.

5. Unprecedented and unexpected 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).
6. Significant push back by traditional international institutions (such as the International Telecommunications Union) that question the legitimacy of the new institutions for management of cyberspace.
7. New demand for cyber cooperation to contain the growth of cyber conflicts further reinforced by a growing push for framing global cyber norms.
8. 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.
9. 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).
10. 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.

Re-Visiting "Levels of Analysis"

The impacts of cyberspace are already apparent at all levels in international relations. To summarize the most obvious:

The Individual: New Power—New Possibilities

Cyberspace enables and empowers the individual in unforeseen and diverse ways. Cyber interaction allows self-definition as well as the individual-framing of political stances. By participating in cyber venues, individuals 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 of challenge to 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.

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 extend their reach and to 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).

All of this contributes to the push for a new and more comprehensive view of national security—one that extends beyond traditional concerns to include 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 sustainability, stability, and security. Recognizing that cyberspace is a war-fighting domain, the world's major power, the United States, has created the U.S. Cyber Command to centralize command of cyberspace operations and coordinate defense of U.S. military networks. Several other countries have followed suit.

The International System: Density of Decision Entities

The increased density of decision makers, noted earlier, is accompanied by a remarkable expansion of governance structures to manage information and communications technologies and to support development objectives. 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 are increasingly complex. 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. 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.

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.

Overall, 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 man-made cyber arena. And we hardly expect that to change on short order.

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. What is clearly 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. But 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 international agreements on operational goals and global cyber norms.

New Imperatives

Despite a growing literature on cyber-related issues in the study of international relations, a consolidated body of knowledge has yet to develop. There is no common consensus on the effects of cyberspace on international relations or what constitutes data, analysis, cases, comparisons, or any of the usual tools of inquiry in the social sciences. Nonetheless, we point to three knowledge-building imperatives or essential activities for consolidating and expanding our knowledge of cyberpolitics in international relations.

These are to (a) formulate the domain ontology (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); (b) leverage knowledge networking, (to help reduce barriers to knowledge access by drawing on the power of collaboration), and (c) expand multilingual capabilities (to allow people to express themselves in their own language and idioms and likewise for others to understand and to engage in their own language and idioms).

The Future of Cyberpolitics

The future of cyberpolitics can be framed by the intersection of two traditional dimensions of world politics: (a) state sovereignty versus private authority, and (b) international conflict and violence versus cooperation and collaboration. Shown in Figure 2, this frame yields different stylistic models with different normative underpinnings, different assumptions about international relations, and different expectations of interactions among decision entities. As model types, these futures can be used to signal possibilities and potentials, not to generate specific predictions.

One model, called the garrison state, is a future defined by high sovereign control over cyber venues in a world with a great deal of conflict and violence. It may well reflect the values of countries like Saudi Arabia, Myanmar, North Korea, and China.

Another is cyber anarchy, also a future of conflict and violence, but one dominated by private authority. In many ways, this future approximates the proverbial Hobbesian state of nature, the war of all against all.

A third model, is the global cyber commons, anchored in international cooperation and coordination in a world controlled by non-state actors, agents, and entities. This future is shaped by norms and requires only shared understandings to sustain effective Internet and other cyber operations.

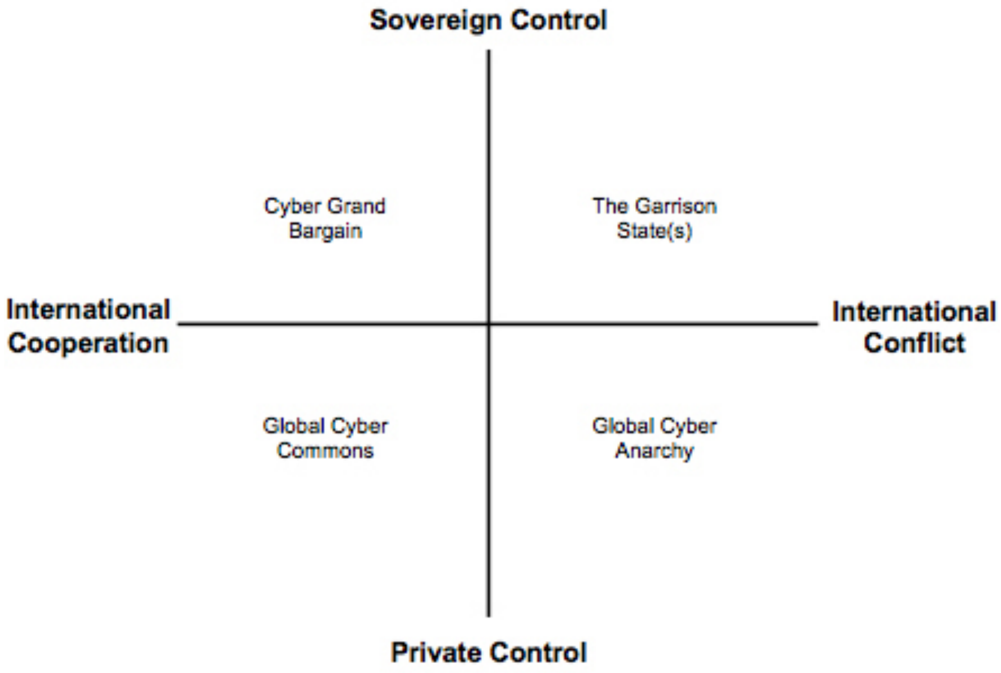

Figure 2: Potential futures of Cyberpolitics in international relations. Source: Choucri, Nazli. 2012. Cyberpolitics in International Relations. Cambridge, MA: MIT Press, p. 235.

Fourth is a cyber grand bargain, characterized by a high degree of international cooperation and managed by sovereign states. With some refinements and alterations, this future may well be consistent with the original United States vision of the Internet, shared by Europe, Japan, and other democracies.

We do not expect the future of cyberpolitics to conform to any model in its pure form, but we suggest that each model highlights different contingencies and thus helps inform our overall expectations.

End Note

If twenty-first century international relations theory is to address cyberpolitics as an important aspect of contemporary reality, it cannot ignore the fundamentals of cyberspace—and its distinctive properties of temporality, physicality, permeation, fluidity, participation, attribution, and accountability. We have come to the end of an era in which cyberspace is separate from the real international relations of the 20th century. Cyberspace is now integral to the world we live in.

The immediate challenge for theory, policy and practice is to consider, clarify, and converge on matters of concepts and metrics—or at least on some rules of thumb—that can best address the objective and subjective for cyberpolitics in international relations. All of this will become more and more central to the fabric of world politics as the twenty-first century unfolds.