Emerging Trends in Cyberspace: Dimensions & Dilemmas

Nazli Choucri

Professor of Political Science, MIT

Prepared for Conference on

Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition

Mathew B. Ridgeway Center, University of Pittsburgh

November 1-2, 2012

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

Contents

I. Introduction

Almost everyone everywhere recognizes that cyberspace is a fact of daily life. Created by human ingenuity with the Internet at its core, cyberspace has become a fundamental feature of the 21st century. Almost overnight, interactions in this virtual domain have catapulted to the realm of *high politics* and are at the forefront of almost all major issues in international relations. Today, this domain has become a source of vulnerability – posing potential threats to national security and a disturbance of the familiar international order – and a major arena of unlimited opportunity for power and potential across various forms of value. The rapidly shifting configurations of interactions in this virtual domain – with expanding actors and actions with diverse causes and consequences – continue to create major disturbances in the traditional system, a major legacy of the 20th century.

The vocabulary of world politics has already accommodated these new realities by signaling references to cyber conflict, cyber power, cyber intrusion, cyber cooperation, cyber security, to name only a few. The early concepts were put forth in hyphenated terms (such as cyber-security); now these are increasingly framed in one word (notably, cybersecurity). At first glance, such differences might seem trivial, but the shifts points to an explicit recognition of a new phenomenon, one that is no longer captured by the hyphenated concepts imported from the familiar politics of 20th century international relations.

The purpose of this paper is to highlight the salience of cyberspace with characteristic features so fundamentally different from those of the traditional realities to which we are so accustomed. Emergent trends in the Internet reflect significant shifts of actors and actions in the cyber sphere, and reveal the reconfigurations of interests and influence in the virtual domain of world politics. We begin by signaling some of distinctive features of cyberspace and cyberpolitics that create disconnects between tradition and familiar conditions and the current realities.

II. Cyberspace and Cyberpolitics

Of the many critical disconnects between the new cyber arena and the traditional domain of international relations, we focus on seven of the most problematic for all actors in world politics, state and non-state, formal and informal. Individually, each feature is at variance with our common understanding of social, political, and economic realities. Jointly, they signal a powerful disconnect contemporary understandings of international relations (Choucri, 2012: 4). These pertain to:

(a) *Temporality*, in the sense that chronological time is replaced by near instantaneity in the realization of action and in the potential reaction.

(b) Physicality, meaning that activities undertaken or decisions made are not constrained by geography, spatial consideration, or sovereign boundaries.

(c) *Permeation,* which refers to communication and activities that penetrate state boundaries and sovereign jurisdictions. As we shall indicate later on, however, increasingly, the sovereign state is trying to control access, with varying degrees of success.

(d) *Fluidity*, which refers to the ease with which shifts in patterns of interactions take place, with attendant configurations and reconfigurations, and emergence of new actors and modalities of interaction.

(e) *Participation*—in the sense that access to cyber venues has already shown how barriers to activism and political expression can be reduced, and the wide range of effects that could then occur.

(f) *Attribution*—where the basic property of cyberspace in this connection refers to the obscurity of identify for actors as well as linkages of actors to specific actions.

(g) *Accountability*—which refers to the absence mechanisms of responsibility due most largely to the lack to attribution possibility.

Any one of these factors alone creates serious dilemmas for the conduct of international relations. Jointly, they suggest that cyberpolitics in this domain cannot be reduced to a mirror image of interactions in world politics as conventionally understood – given the historical record and the tradition of empirical analysis, on the one hand, and our conceptual and theoretical tools on the other.

In this context, *cyberpolitics,* a recently coined term, refers to the conjunction of two processes or realities—those pertaining to traditional human interactions (*politics*) surrounding the determination of *who gets what*, *when*, and *how*, and those enabled by the uses of a virtual space (*cyber*) as a new arena of interaction with its own modalities, realities, and contentions. (For this concept of politics, see Lasswell, 1958 and Easton, 1953; 1965).

III. Old Legacies and New Realities

The traditional system of international relations, such as those with bipolar, multipolar, or unipolar structures, which are generally characterized by hierarchical power relations, are being replaced by new structural configurations characterized by diffusion of power, decentralization, diverse asymmetries and different types of power relations. Together these new features are co-existing, if not replacing, the well-known vertical structures of power and influence. Cyberspace may be relevant to all these but it did not create them.

3.1 Legacies of the 20th Century

By definition, the legacies of the 20th century shape the basic parameters of the 21st century. Some of these legacies will prove to be transient; others are definitional in setting the contours of 21st century international relations power and politics. Most notable among these is the large number of new states due to the decolonization process coupled with periodic reframing of sovereignties and territorial boundaries. Somewhat related with a logic and dynamics of its own, is the growth in the number of international institutions and the expansion of scale and scope of activities.

We also must recognize the explosion of profit seeking private sector activities and the consolidation of global reach permitted and propelled by technological innovations, market conditions, and emergent opportunities. With persistent expansion, the corporate structure of investment activities took on worldwide risks and responsibilities to investors of various kinds. The use of "private" may be me somewhat misleading in this context, as state-based or state-owned firms, should not ignored. With the nationalization of resource extraction enterprises, for example, the state replaced the private (and usually foreign) investor in ownership as well as operations and management.

Slowly at first, and then more rapidly – eventually at an accelerated pace – is the growth of voluntary, not-for-profit entities in international relations. Initially they appeared largely for purposes of expanding religious faith. Gradually and almost imperceptibly, they adopted a wide range of causes, pursuing an ever-expanding set of activities and interests. Some were encouraged by the state system; others by the profit-seeking sector; and all pursuing a target based agenda driven by specific interests even when these were defined in broad terms. With the increasing politicization of science and technology worldwide, the scientific community supports a wide range of research activities organized around particular knowledge interests. Over time, it became clear that the post-World War II major powers no longer held the monopoly over control to the global political, social, or economic policy agenda. By the 1980s,the international policy priorities, consumed by the conjunction of developmental and environmental challenges, framed what was arguably the first, most comprehensive global approach to policy imperatives – at all levels of development and all forms of political aggregation. The concept of "sustainability" was framed to become as salient as "security," as conventionally understood in world politics.

None of this was due to the construction of cyberspace.

3.2 Realities of the 21st century

When we factor in the construction of cyberspace – especially the dramatic expansion of cyber access worldwide, the growth in "voicing," global civil society, and the new economic and political opportunities afforded by the Internet – cyber venues appear to be more than enablers of power and influence. They are critical drivers of the ongoing realignments, the means by which all actors, at all levels of analysis, pursue their goals and objectives. Furthermore, they have assumed constitutive features of their own.

Constructed by human ingenuity, cyberspace is a domain of interaction enabled by new forms of communication venues. Almost overnight, human beings – who now recognized the salience of the natural environment and its life supporting properties to be fundamental to survival and wellbeing – were interacting in a new environment whose properties were yet to be fully understood.

This particular reality of the 21st century did not replace, reduce, or eliminate the effects of 20th century legacies. It created added complexities—augmenting not reducing the impacts of the features noted above. The "new" reality altered key traditional dynamics of world politics and shaped many new features that were largely unprecedented but profoundly pervasive in scale and scope. To begin, the 21st century witnessed the effects of changes in the traditional power calculus. The old "polarity" framework in international relations was replaced by a highly distributed structure. This shift, a legacy of the 20th century, must be viewed in conjunction with critical elements of the new realities.

Among these are the powerful asymmetries in power and capability in traditional (kinetic) and new (cyber) terms. Stated differently, almost overnight, many states – large and small – expanded their cyber-based capabilities in ways that were not contingent on their position in the traditional power-based system. Equally, if not more importantly, is the clear dominance of the private sector in the management of the cyber domain. The fact is that the state system is a latecomer with respect to governance and the operation of cyberspace. Thus, we have increasing complexity in cyber management coupled with growing politicization. The management system put in place by the United States early in the cyber era was being contested by states with alternative visions and interest, such as China, Russia and others.

For the state system as a whole – as well as for individual countries – many features of cyberspace, such as those noted above, created new vulnerabilities and new challenges for national security. Cybersecurity is now fundamental to the security of the state, firms, organizations, institutions and individuals. The challenge now is to provide this new imperative with robust theoretical and empirical foundations that would at the very least enable the formation of robust policy responses.

All of this is due to the construction of cyberspace.

3.3 The "Net" Results

Almost by definition, new forms of conflicts have emerged – for state and non-state entities – supported by new instruments, tools, and weapons. These new conflicts are political and economic in nature, driven by the pursuit of power and the pursuit of wealth – in both legitimate and non-legitimate venues. To be fair, the international law for cyberspace is at early stages of development, the rules for legal cyber conflict and competition and the acceptable venues for cyber contention are at their earliest stages.

Concurrent with the growth of conflict in cyberspace – or uses of cyber venues for the conduct of traditional conflict – are diverse international efforts to develop rules of cyber conduct, norms for cyber behavior, laws and regulations, and institutions for cyber security. Since the state is the only entity enfranchised to speak or act in the international system on behalf of its citizens – or people within its borders – it leads the formal cyber-related discussions and represents both private and public interests.

In the most general terms, we can identify two specific and overarching outcomes for the international system of 20th century legacies and 21st century realities. The first is an increasingly "close coupling" between the traditional and cyber politics in international relations, reflecting the growing interconnections between two initially distinct and separate arenas of interactions. By definition, "close coupling" does not necessarily imply mirror-image dynamics. That in itself in an empirical question. The second is the evolution of "hybrid" policies, generally in response to particular dilemmas rather than reasoned policies based on robust principles.

Table 1 summarizes the differences in strategic international context "then" and "now" This table provides a short hand reminder of the major shifts in world politics before and after the construction of cyberspace.

Table 1
Strategic Context – Then & Now

Then: 20th C. **PowerPolitics** ***Only the Major Powers***	**Now: 21st C.** **CyberPolitics** ***Anyone & Everyone***
Bipolarity	Multiplicity & Diversity
Structural Power Balance	Structural Instability & Volatility
Clear Deterrence Calculus	Complexity in Deterrence Calculus
Recognized Symmetry	Uncertain Asymmetry
Known Actor Identity	Obscured Actor Identity
Shared Aversions	Varied Avoidance
State Dominance	Loss of State Dominance
Known Paths & Outcomes	Unknown Paths & Outcomes

IV. Emergent Trends in Cyberspace

We now turn cyber access and patterns of cyber participation. If we consider mobile signals as a notable indicator, then Figure 1 reminds us that by 2010, only 10% of the world's population did not have access to mobile cellular signal. For all practical purposes, almost the entire globe was covered. But this statistic in itself obscured many important features of cyber participation.

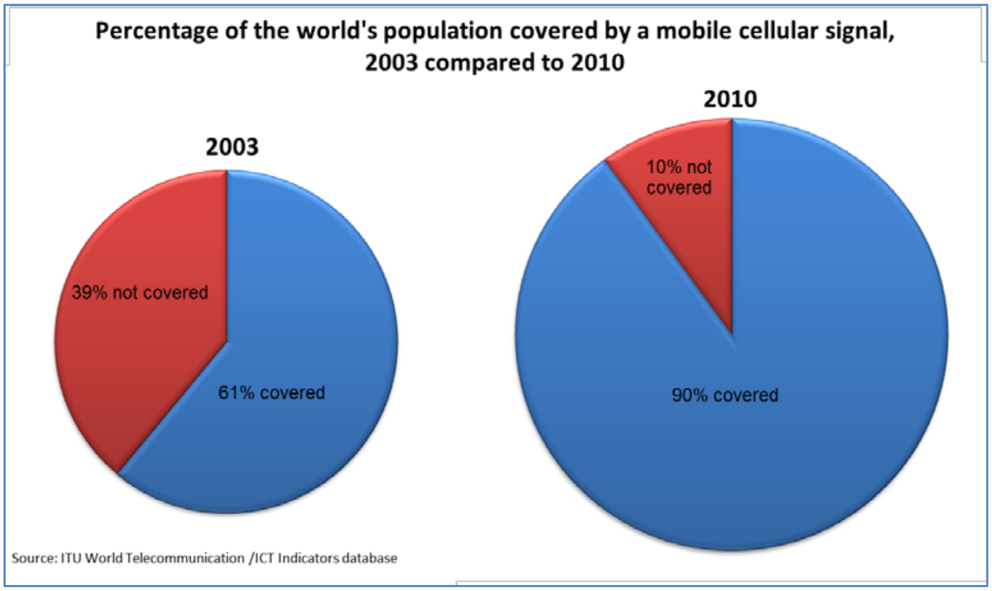

Figure 1: Percentage of the World's population covered by a mobile cellular signal, 2003 compared to 2010.

Source: ITU World Telecommunications/ICT indicators database.

4.1 Distribution of Users

We show in Figure 2 that, for 2012, Asia hosted the largest percentage of users worldwide. The regional distribution for that year is shown in Figure 2 and illustrates an interesting disparity anchored by differences in population size but also in rapid growth in cyber access.

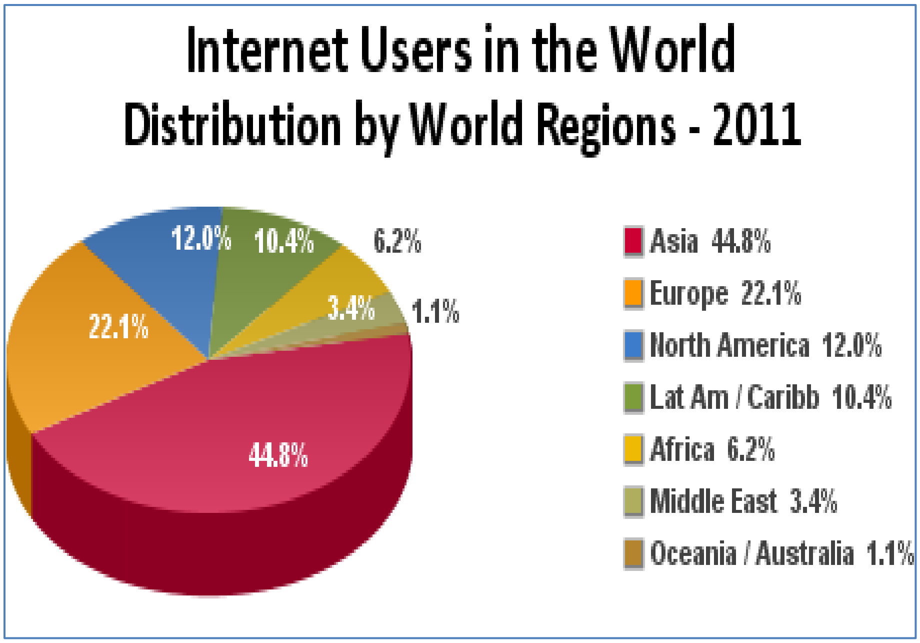

Figure 2: Internet Users in the World – Distribution by World Regions, 2011.

Source: Internet World Stats. Copyright © 2001-2011, Miniwatts Marketing Group. www.internetworldstats.com/.

Figure 3 presents a different view of cyber participation, one that focuses on the number of individual users, and thus draws attention to new features of international relations. We consider this indicative of "people power," in the sense that the individual is now able to articulate preferences and voice interests. None of this guarantees results but it must be recognized as a notable feature of the cyber-demography.

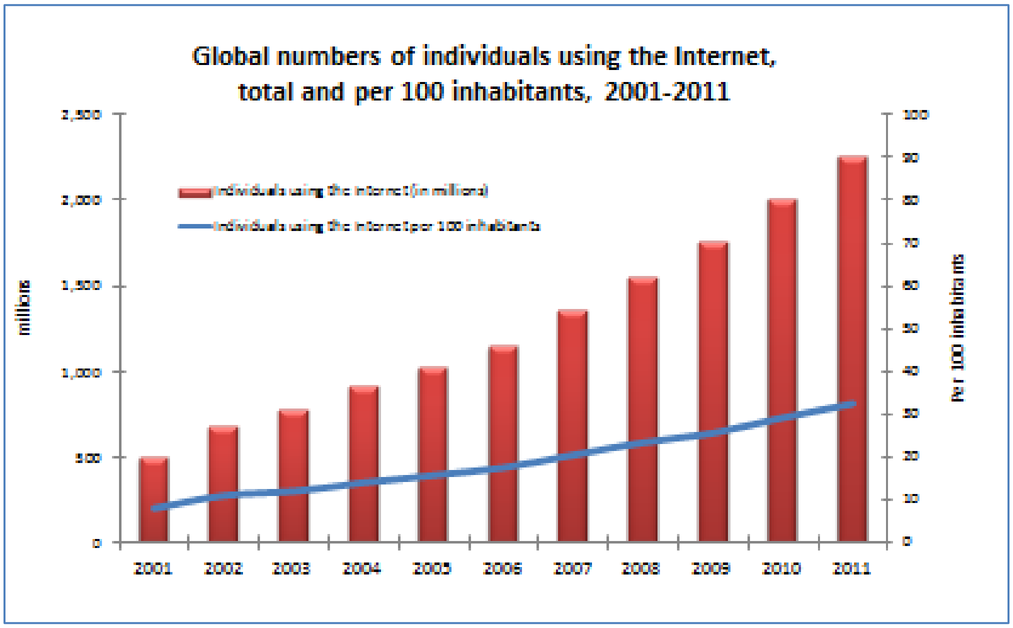

Figure 3: Global numbers of individuals using the Internet, total and per 100 inhabitants, 2001-2011.

Source: Data from ITU World Telecommunication/ICT Indicators database

Yet another perspective on the political demography of cyberspace, shown in Figure 4, is based on 2010 Internet user statistics worldwide. If we consider total Internet users, note for example, the differences between the US (227 million) and China (298 million), these figures represent 74% of the total US population but only 22.4% of China's population. Invariably, the character of cyberspace is influenced by shifts in the composition of users. With this demographic contour of cyberspace, new complexity follows.

4.2 New Complexity

Nowhere is the influence of the cyber-demography more evident than in the languages used on the Internet. While English continues to dominate, Chinese is a close second. The other notable languages shown in Figure 4 trails behind significantly. These are all absolute figures that reflect the accumulation of language use over time. They provide little insight into differences in rates of change across languages. These differences shape much of what is observed at aggregate levels.

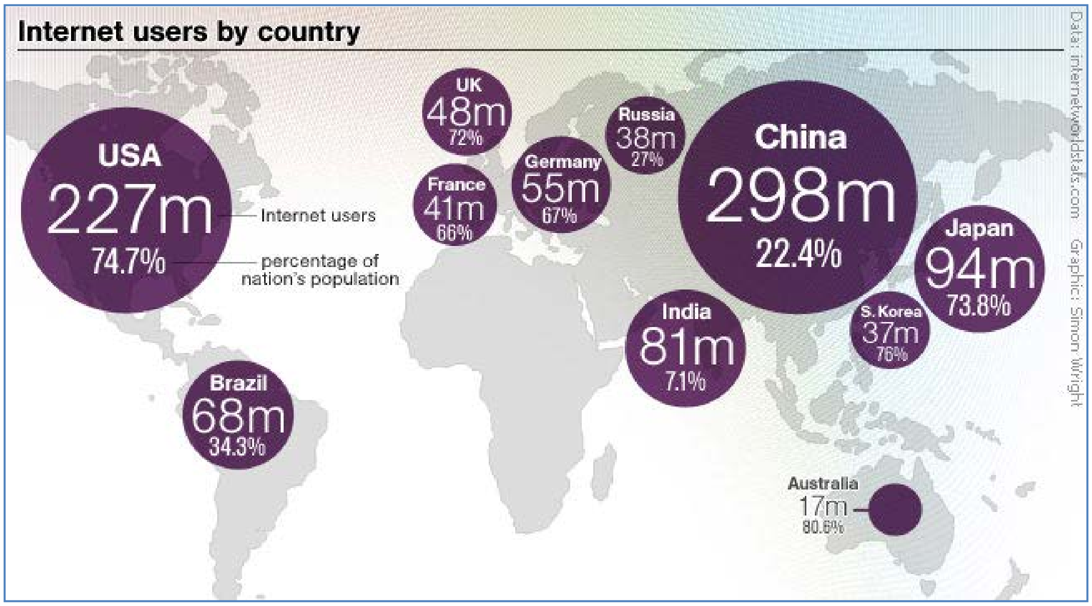

Figure 4: Internet Users by Country, 2009

Source: July 29, 2009: Sydney, NSW. A News.com.au graphic of Internet users by country as of 2009. Pic. Simon Wright. ©Newspix. http://www.internetpromotion-australia.com.au/internetpromotionblog/?p=250\

Among the most significant features of the new political demography of cyberspace – the user, the language used, and the implications for the pursuit of power and the pursuit of wealth – is the variety we observe in rates of change. Figure 5 shows Internet usage by language for 2007 and growth between 2000 and 2007. This figure "speaks for itself." For example, with only 3.7% of the cyber population using Arabic in 2007, the rate of growth was at 1575.9% from over these seven years. By contrast, English, the dominant language in the early years of the Internet was used by 30.1% of the cyber population in 2007 with a growth of 267.3% over this period. It goes without saying that cyber access was growing over time, the voice of non-western speakers clearly dominates. Such differentials are likely to enhance, rather than dampen the politicization of cyberspace and the salience of "high politics."

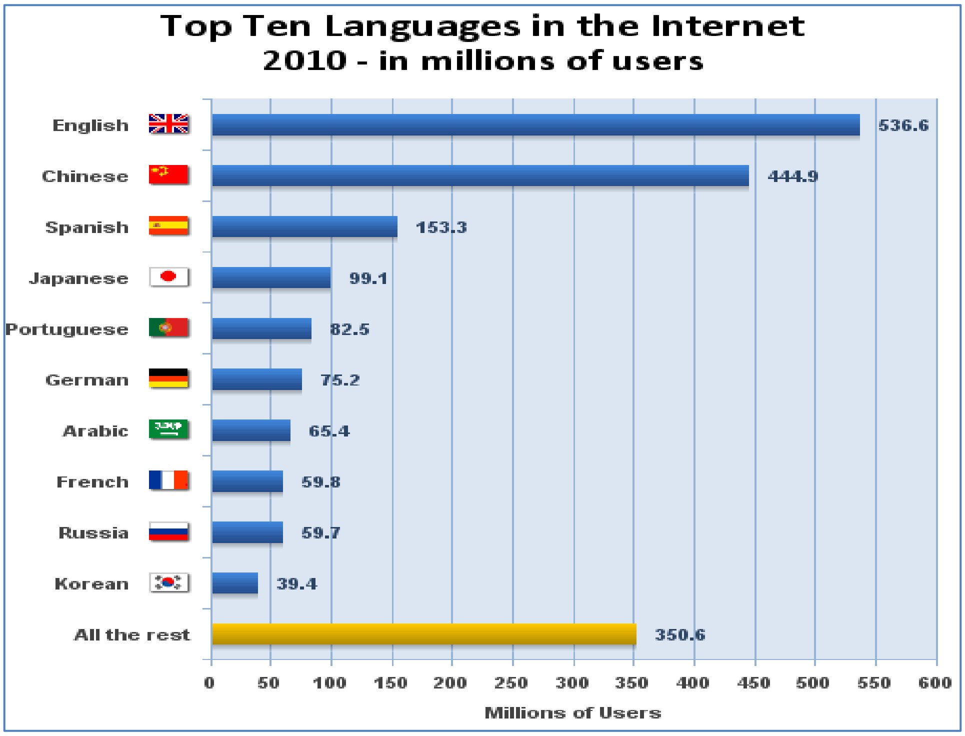

Figure 5: Top Ten Languages in the Internet, 2010 – in millions of users.

Source: Internet World Stats. Copyright © 2001-2011, Miniwatts Marketing Group. www.internetworldstats.com/.

V. Malevolence and Threats to Cyber Security

We have focused so far on emerging trends in cyberspace. Characteristic features of cyber demography and shifts in the configuration of users constitute "fundamentals" of this new arena of interactions. With the basics in place, we now turn to three forms of well-documented activities, namely denial of service, variety of cyber attacks, and select facets of cyber espionage. These reflect different challenges to cybersecurity – by different actors, different motivations, different instruments, and different stakes.

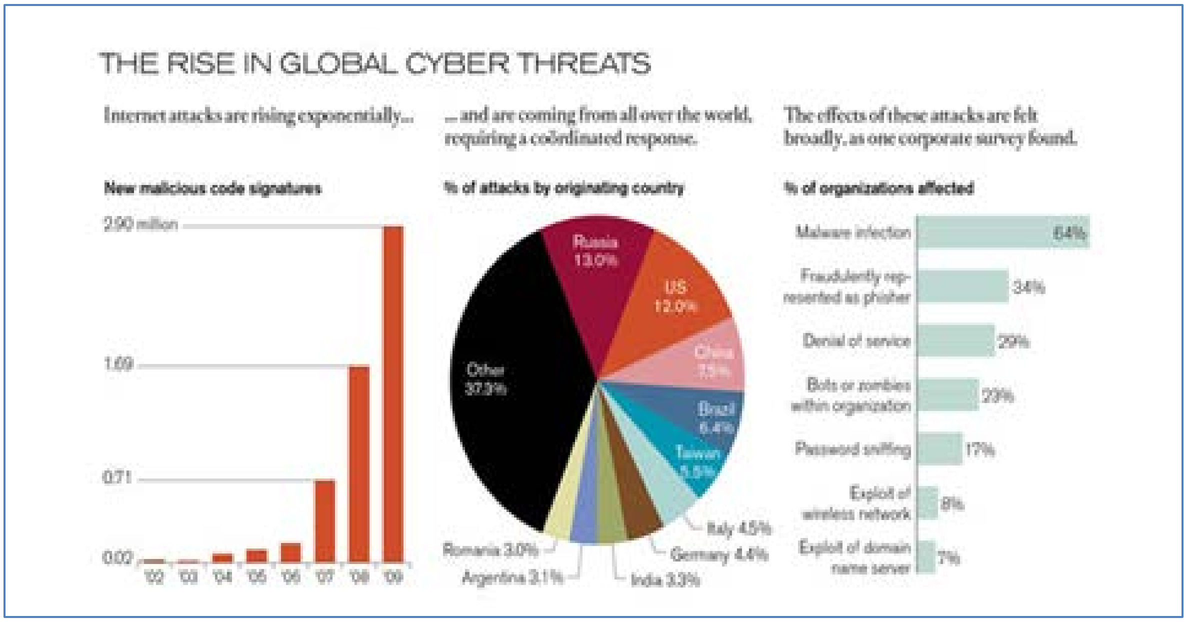

Figure 6: Cyber Attacks: The Rise in Global Cyber
Source: McCall, Tommy/Infographics.com in Talbot, David. 2010. "Moore's Outlaws." *Technology Review,* 113 (4) 43.

But, these are all driven by the basic primitives of international politics, that is, the pursuit of power and the pursuit of wealth.

5.1 Cyber Attacks

Cyber attacks have become an integral part of the entire cyber ecology. The diffusion of damage-creating tools and the deployment of malevolence technologies, coupled with the growth of markets for malware put cybersecurity at the forefront of national and international concerns in almost all parts of the world, threatening sovereign states as well as private entities, individual as well as organized users.

Figure 6 shows the growth of cyber attacks, the originating country location and the number of organizations affected by different tools of malevolence. Clearly, from the country of origin we cannot conclude that the government itself is responsible for the attacks. The originating country refers to location of address, not government action. In the most general terms, this further reflects the "power of individuals" unrestrained by sovereign jurisdiction of conventional territorial boundaries.

5.2 Denial of Service

The forgoing notwithstanding, at the same time, the state does not remain inert. We see the hand of government in denial of service. Denial of service is the prerogative of the state, with formal authority, legitimacy, and regulatory capability. Figure 7 shows denial of service requests to Google. The figure shows how often governments request content removal, and how often Google agrees to the request. The figure also signals the reason stated for the request. To note the obvious, the diversity is remarkable as is the distribution of requests. Of course, there are considerable differences in government systems, national and social priorities, capabilities, and cyber access. To note only the three most obvious cases – Brazil, Germany, South Korea – the size and reasons illustrate salient issues at the state levels. By contrast, if we consider India and Libya, the drivers of requests in the then authoritarian state (Libya) are far greater and more varied than in democratic state (India). Interestingly, India features prominently in another dimension of cyber malevolence, namely as a target of espionage from China.

5.3 Cyber Espionage

Given the fluidity of the emergent cyber-based vocabulary, it is often difficult to distinguish among "attack," "penetration," and "damage" as forms of behaviors, as it is difficult to differential among

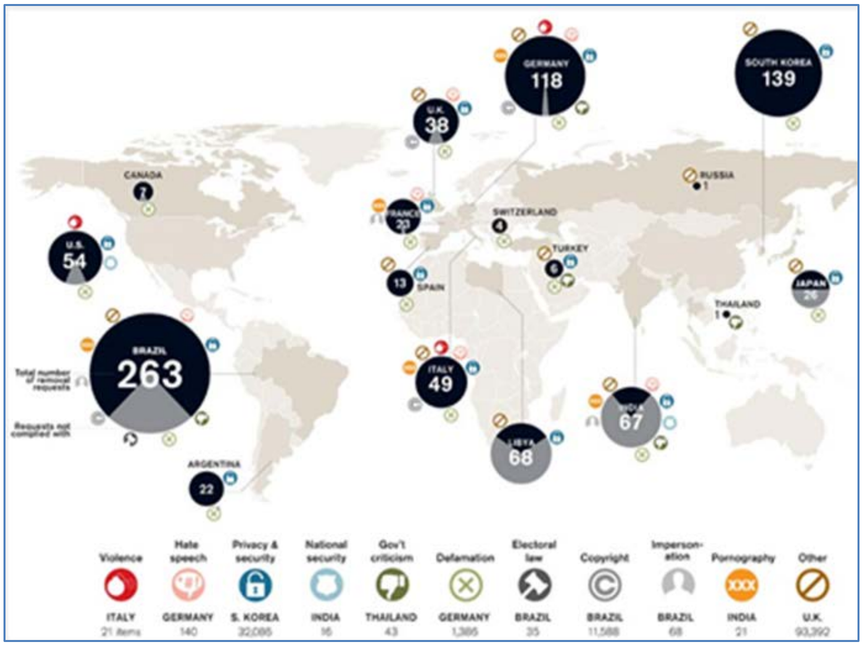

Figure 7: Denial of Service

Source: Bergstein, Brian. (2011). Going Offline: Google reveals how often governments ask it to banish things from its services and how often it complies. *Technology Review*, November/December, pp. 30-31.

instruments and tools or "malware" or other types. Of course, motivations are usually attributed to, rather than announced by the actor or country-source. With these considerations in mind, Figure 8 shows one representation of computers "compromised" with China as the source. This representation, put forth in the MIT *Technology Review*, reflects the reach of computer penetration and compromise origination from China. Unexpected in Figure 8 is the salience of India as a target country – compared to other targets in this figure. Either India's cyber defenses are weaker than those in other state-locations, or India holds greater attraction for penetration by users from China. None of this has the precision nor the empirical foundations of the recent Mandiant report, but it does provide a sense of the attributed Chinese penetration. The general view is that such penetration is largely in the form of industrial or corporate espionage. By international standards, such penetration is a form of illegitimate "technology-leapfrogging," one that is manifested through venues not exactly advocated for by development analysts.

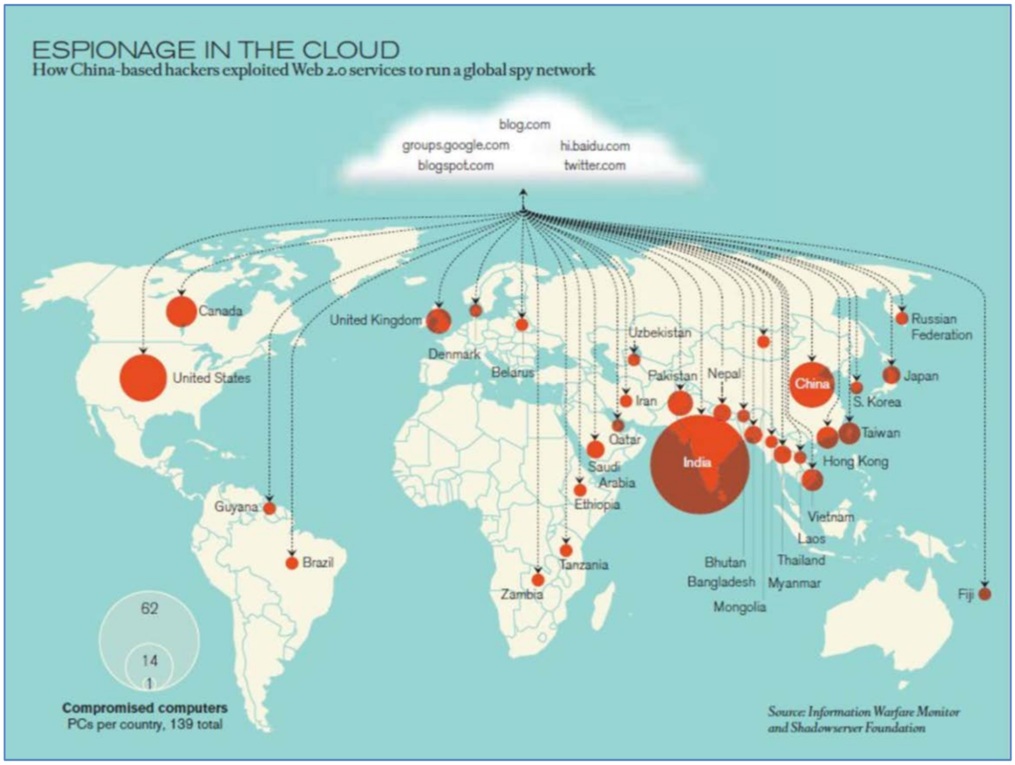

Figure 8: Espionage in the Cloud

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

VI. End Note

The state-based international system, anchored in the traditional Wesphalian concept of sovereignty, is increasingly influenced by the rapidly construction and expansion of cyberspace. Among the many effects, the following are among the most notable: First are the new challenges to *national security*, with new sources of vulnerability (cyber threats), new dimensions of national security (cyber security) coupled with uncertainty, fear, and threat from unknown sources (attribution problem). Second, is the empowerment of *new actors*, some with clear identities and others without – but all with opportunities for growth. Among these are national actors created to exercise access control or denial, non-state commercial entities with new products and processes, entities operating as proxies for state actors, and novel criminal groups, often too anonymous to identify and varied to list and too difficult to identify – all shaping new and unregulated markets. Third is a wide range of novel types of *asymmetries* that shift power relations and create new opportunities for almost all states. Such shifts provide opportunities for weaker actors to threaten stronger ones, for various uses of the advantages afford by cyber-anonymity, or for the new venues for political, industrial or military via cyber venues, or expansion of criminal activities and the like.

These developments are all breeding ground for *malevolence* in its various forms that create unprecedented threats to stability and security of the state system, business enterprises, and activities of not-for-profit non-state actors. These include the militarization of cyberspace, potentials for cyber warfare, threats to critical infrastructures, and so forth are among the explicit and evident threats. Equally, and perhaps more damaging, is the multiplication of computer penetration activities that appear to be in the realm of industrial and technological cyber espionage. Given the mounting evidence of such malevolence, the international community is beginning to recognize the salience and significance of this threat-trajectory.

While not the focus of this paper, the issues addressed therein all point to an increasingly critical global dilemma surrounding the governance for cyberspace. At its core, the dilemma is framed by two countervailing trends: On the one hand, is the growth of increasingly strident "demand" for governance mechanisms regulating conduct in cyberspace; on the other is the consolidation of international cleavages over the policy principles upon which to construct the "supply" of mechanisms for cyber governance. This dilemma, noted here in the idiom of the market place, is fundamentally one of power politics – worldwide struggle over new opportunities for the pursuit of power and wealth as well as gains in strategic and market contexts – made possible by the fluidity of the cyber sphere.

REFERENCES

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

Easton, David. (1953). *The Political System: An Inquiry into the State of Political Science*, New York: Alfred A. Knopf.

Easton, David. (1965). *A Systems Analysis of Political Life*, New York: Wiley.

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

Mandiant. (2012). *APT1: Exposing One of China's Cyber Espionage Units*. Retrieved from: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.