Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Emerging Trends in Cyberspace: Dimensions and Dilemmas

Nazli Choucri

Professor, Political Science Department
Massachusetts Institute of Technology

August 1, 2016

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

Citation: Choucri, N. (2016). Emerging trends in cyberspace: Dimensions and dilemmas. In P. Williams, & D. Fiddner (Eds.), *Cyberspace: Malevolent actors, criminal opportunities, and strategic competition* (pp. 53–74). U.S. Army War College Press.

Unique Resource Identifier: ISBN: 1-58487-726-X.
https://publications.armywarcollege.edu/pubs/2388.pdf

Version: Final published version.

CHAPTER 3

EMERGING TRENDS IN CYBERSPACE: DIMENSIONS AND DILEMMAS

Nazli Choucri

This chapter was originally 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.

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 into the realm of high politics and are at the forefront of nearly all key issues in international relations. However, 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 various forms of power and potential. 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 refer-

ences to cyberconflict, cyberpower, cyberintrusion, cybercooperation, and cybersecurity, 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 point 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 chapter is to highlight the salience of cyberspace's characteristic features, which are so fundamentally different from those of the traditional realities we are already accustomed to. Emergent trends on the Internet reflect significant shifts of actors and actions in the cybersphere and reveal the reconfigurations of interests and influence in the virtual domain of world politics. We begin by signaling some of the distinctive features of cyberspace and cyberpolitics, which create disconnects between traditional and familiar conditions and the current realities.

CYBERSPACE AND CYBERPOLITICS

Of the many critical disconnects between the new cyberarena and the traditional domain of international relations, we focus on seven of the most problematic for all actors in world politics—state and nonstate, 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 between contemporary understandings of international relations.[1] These pertain to:

a. **Temporality**, in the sense that chronological time is replaced by near instantaneity in the realization of action and 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, however, the sovereign state is trying increasingly 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 the emergence of new actors and modalities of interaction.

e. **Participation,** in the sense that access to cybervenues 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 identity for actors as well as the difficulty of linking actors to specific actions.

g. **Accountability,** which refers to the absence of 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.[2]

OLD LEGACIES AND NEW REALITIES

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

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 a large number of new states, formed by the decolonization process coupled with the periodic reframing of sovereignties and territorial boundaries. Somewhat related, with a logic and dynamic of its own, is the growth in the number of international institutions and the expansion of scale and scope of their 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 expansions, the corporate structure of investment activities took on worldwide risks and responsibilities to investors of various kinds. The use of "private" may be somewhat misleading in this context, as state-based or state-owned firms should not be ignored. With the nationalization of resource extraction enterprises, for example, the state replaced the private (and usually foreign) investor in ownership as well as in operations and management.

Slow at first, and then more rapid—eventually occuring at an accelerated pace—is the growth of voluntary, not-for-profit entities in international relations. Initially, they appeared largely for the purpose 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 of these non-profits were encouraged by the state system; others by the profit-seeking sector. But all pursued 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 of control over 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 these developments were due to the construction of cyberspace.

Realities of the 21st century.

When we factor in the construction of cyberspace—especially the dramatic expansion of cyberaccess worldwide, the growth of "voicing," global civil society, and the new economic and political opportunities afforded by the Internet—cybervenues 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 well-being—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, rather than reducing, the impact 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 with, 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 important, if not more so, is the clear dominance of the private sector in the management of the cyberdomain. 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 cybermanagement coupled with growing politicization. The management system put in place by the United States early in the cyberera was being contested by states with alternative visions and interests, 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 states, firms, organizations, institutions, and individuals. The challenge now is to provide this new imperative with robust theoretical and empirical foundations, which would at the very least enable the formation of robust policy responses.

All of this is due to the construction of cyberspace.

The Net Results.

Almost by definition, new forms of conflicts have emerged—for state and nonstate 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 nonlegitimate venues. To be fair, international law for cyberspace is at the early stages of development; the rules for legal cyberconflict and competition and the acceptable venues for cybercontention are at their earliest stages.

Concurrent with the growth of conflict in cyberspace—or uses of cybervenues for the conduct of traditional conflict—are diverse international efforts to develop rules of cyberconduct; norms for cyberbehavior, laws, and regulations; and institutions for cybersecurity. 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 traditional- and cyberpolitics 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 to reasoned policies based on robust principles.

Table 3-1 summarizes the differences in strategic international context "then" and "now."

THEN: 20th-Century Power-Politics Only the Major Powers	NOW: 21st-Century Cyberpolitics Anyone & Everyone
Bipolarity	Multiplicity & Diversity
Structural Power Balance	Structural Instability and 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

Table 3-1. Strategic Context—Then and Now.

EMERGENT TRENDS IN CYBERSPACE

We now turn to cyberaccess and patterns of cyberparticipation. If we consider mobile signals as a notable indicator, then Figure 3-1 reminds us that by 2010, only 10 percent of the world's population did not have access to a mobile cellular signal. For all practical purposes, almost the entire globe was covered. However, this statistic in itself obscured many important features of cyberparticipation. See Figure 3-1.

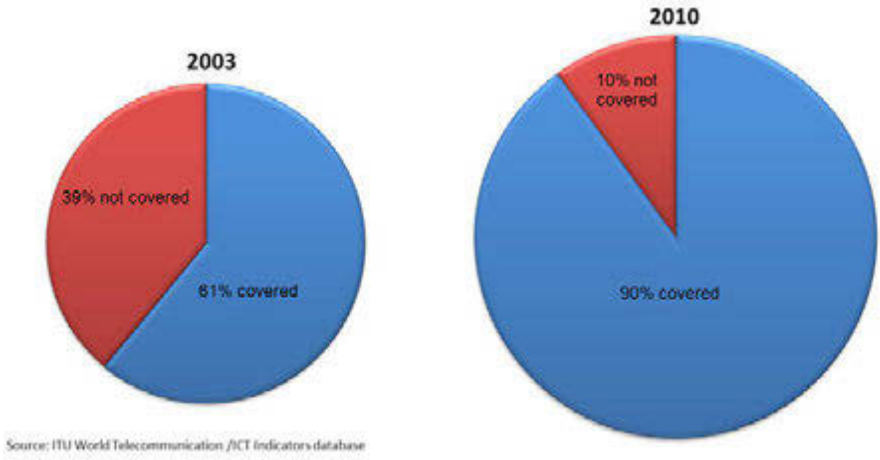

Figure 3-1. Percentage of the World's Population Covered by a Mobile Cellular Signal, 2003 Compared to 2010.[3]

Distribution of Users.

We show in Figure 3-2 that in 2012, Asia hosted the largest percentage of users worldwide. The regional distribution for that year illustrates an interesting disparity anchored, not only by differences in population size, but also in rapid growth in cyberaccess.

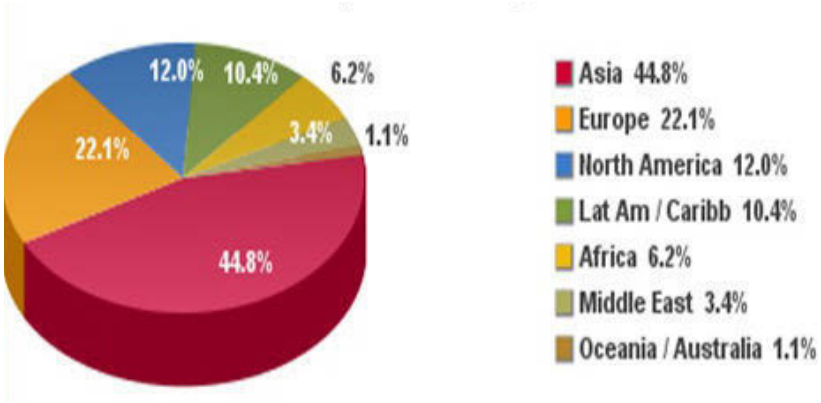

Figure 3-2. Internet Users in the World, Distribution by World Regions, 2011.[4]

Figure 3-3 presents a different view of cyberparticipation, 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 can guarantee results, but it must be recognized as a notable feature of cyberdemography.

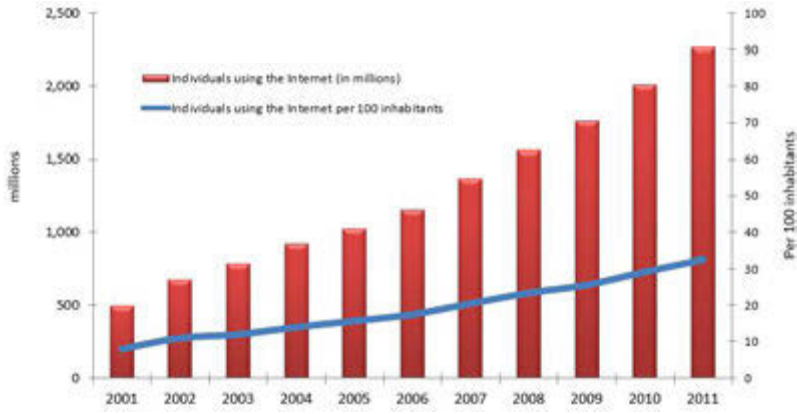

Figure 3-3. Global Numbers of Individuals Using the Internet, Total and Per 100 Inhabitants, 2001-2011.[5]

Yet another perspective on the political demography of cyberspace is based on the 2010 Internet User statistics worldwide. If we consider total Internet users, note, for example, the differences between the United States (227 million) and China (298 million): these figures represent 74 percent of the total U.S. population, but only 22.4 percent 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.

New Complexity.

Nowhere is the influence of cyberdemography 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 3-4 trail behind significantly. These are all

absolute figures, which 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 3-4. Internet Users by Country, 2009.[6]

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 3-5 shows Internet usage by language for 2010. This figure "speaks for itself." Especially significant is the size of the representation of non-Western language. Such differentials may well enhance, rather than dampen, the politicization of cyberspace and the salience of "high politics."

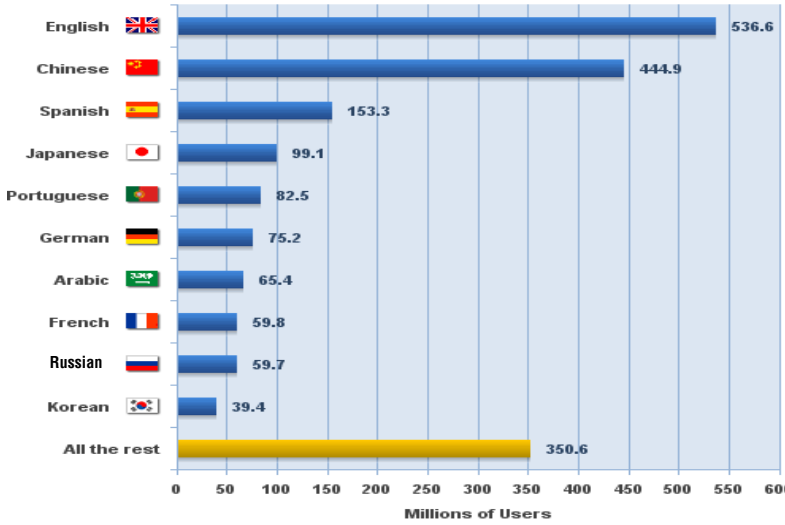

Figure 3-5. Top Ten Languages on the Internet, 2010, in Millions of Users.[7]

MALEVOLENCE AND THREATS TO CYBERSECURITY

We have focused so far on emerging trends in cyberspace. Characteristic features of cyberdemography 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: the denial of service, a variety of cyberattacks, and select facets of cyberespionage. These reflect different challenges to cybersecurity—by different actors, with different motivations, different instruments, and different stakes. However, these challenges are all driven by the basic primitives of international politics; that is, the pursuit of power and the pursuit of wealth.

Cyberattacks.

Cyberattacks have become an integral part of the entire cyberecology. 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 and individual as well as organizational users.

Figure 3-6 shows the growth of cyberattacks, 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 the physical location of the attacker, but does not imply that government action was the source. In the most general terms, this growth further reflects the "power of the individual" unrestrained by sovereign jurisdiction of conventional territorial boundaries.

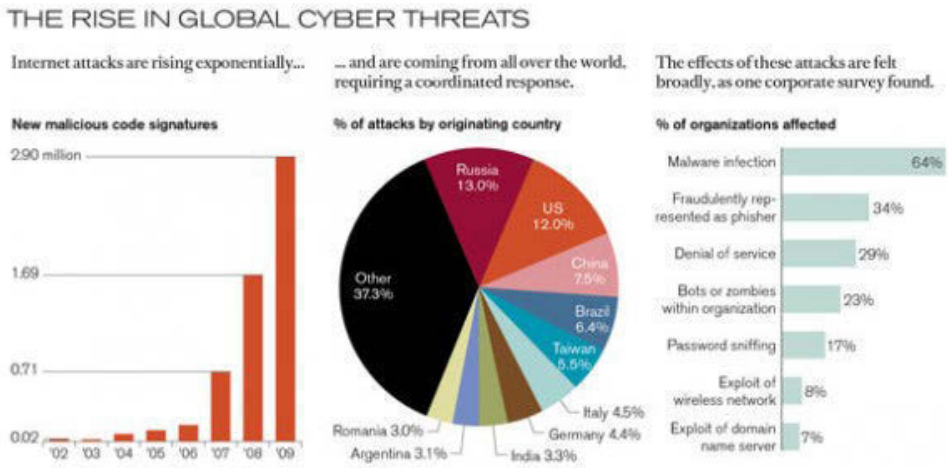

Figure 3-6. Cyberattacks: The Rise in Global Cyberattacks.[8]

Denial of Service.

The foregoing notwithstanding, at the same time, the state does not remain inert. We see the hand of government in the denial of service. Denial of service is a prerogative of the state, with formal authority, legitimacy, and regulatory capability. Figure 3-7 shows denial of service requests to Google, indicating how often governments request content removal, and how often Google agrees to the requests. The figure also indicates the reason stated for the request. To note the obvious, the diversity of requests is remarkable, as is the distribution of requests. Of course, there are considerable differences in government systems and national and social priorities, capabilities, and cyber-access. To note only the three most obvious cases—Brazil, Germany, and 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 the democratic state (India). Interestingly, India features prominently in another dimension of cybermalevolence, namely, as a target of espionage from China.

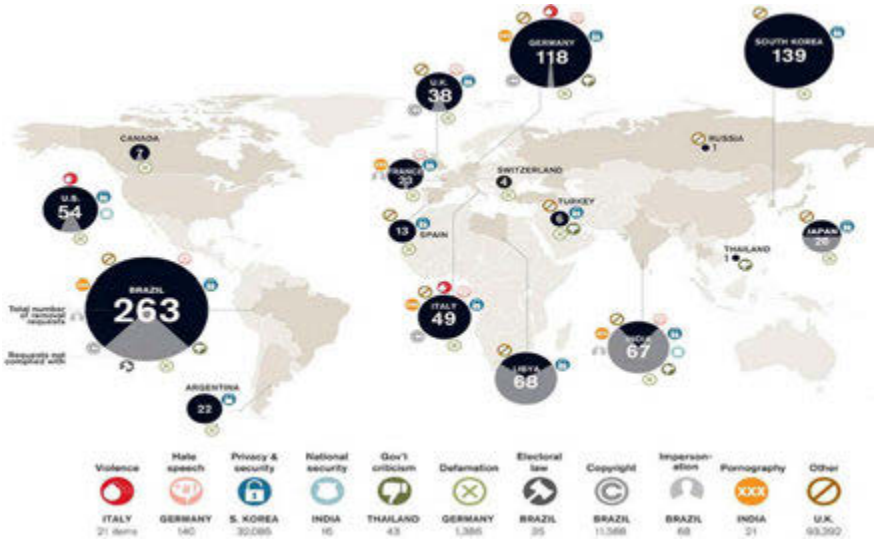

Figure 3-7. Denial of Service.[9]

Cyberespionage.

Given the fluidity of the emergent cyber-based vocabulary, it is often difficult to distinguish between "attack," "penetration," and "damage" as forms of behavior just like it is difficult to differentiate among 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 3-8 shows one representation of computers "compromised" with China as the source. This representaation, put forth in the *MIT Technology Review,* reflects the reach of computer penetration and compromise origination from China. Unexpected in Figure 3-8 is the salience of India as a target country—compared to other targets that are depicted. Either India's cyberdefenses are weaker than those of other state-locations, or India holds a greater attraction for penetration by users from China.

None of the data in Figure 3-8 have the precision or the empirical foundation of the 2012 Mandiant report, but they do provide a sense of the attributed Chinese penetration.[10] 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.

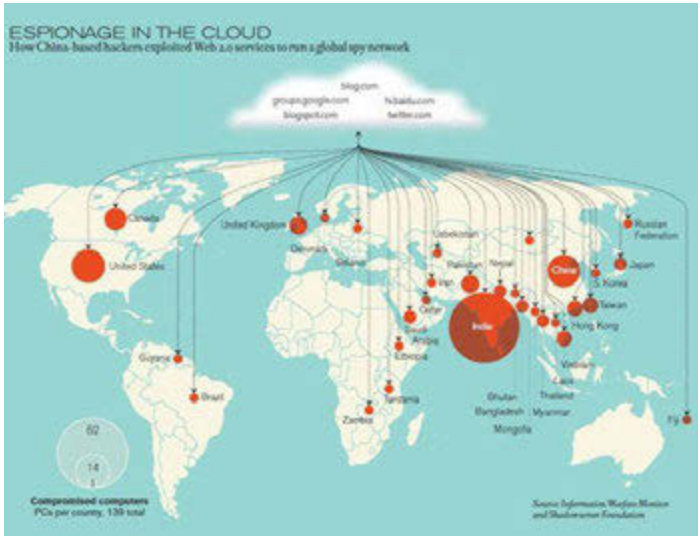

Figure 3-8. Espionage in the Cloud.[11]

EPILOGUE

The state-based international system, anchored in the traditional Westphalian concept of sovereignty, is increasingly influenced by the 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 (cyberthreats) and new dimensions of national security (cybersecurity), 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, nonstate commercial entities with new products and processes, entities operating as proxies for state actors, and novel criminal groups, often too anonymous to identify, too varied to list, and too difficult to locate—all shaping new and unregulated markets. Third is the wide range of novel types of asymmetries that shift power relations and create new opportunities to exploit the advantages afforded by cyberanonymity. For example, such opportunities allow for weaker actors to threaten stronger ones, or for criminals to expand their activities, or for individuals to challenge the power of the state system—to note some of the most obvious possibilities.

Developments such as these are all breeding grounds for **malevolence** in its various forms, which create unprecedented threats to the stability and security of the state system, business enterprises, and activities of not-for-profit nonstate actors. The militarization of cyberspace, potentials for cyberwarfare, 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 cyberespionage. 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 particular chapter, the issues addressed in this monograph all point to an increasingly critical global dilemma surrounding the governance of cyberspace. At its core, the dilemma is framed by two countervailing trends—on the one hand is the growth of an 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 cybergovernance. This dilemma, noted here in the idiom of the marketplace, is fundamentally one of power politics—a 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 cybersphere.

ENDNOTES - CHAPTER 3

1. Nazli Choucri, *Cyberpolitics in International Relations*, Cambridge, MA: MIT Press, 2012; David Easton, *The Political System: An Inquiry into the State of Political Science*, New York: Alfred A. Knopf, 1953.

2. For this concept of politics, see Harold D. Lasswell, *Politics: Who Gets What, When and How*, New York: McGraw-Hill, 1958; David Easton, *A Systems Analysis of Political Life*, New York: Wiley 1965; and Easton, *The Political System*.

3. Data from ITU World Telecommunications/ICT indicators database.

4. Internet World Stats, Copyright 2001-11, Miniwatts Marketing Group, available from *internetworldstats.com*.

5. Data from ITU World Telecommunication/ICT Indicators database.

6. A News.com.au graphic of Internet users by country as of 2009, July 29, 2009, Sydney, New South Wales, Picture by Simon Wright, Newspix, available from *internetpromotion-australia.com.au/internetpromotionblog/?p=250*.

7. Internet World Stats.

8. Tommy McCall (Infographics.com) in David Talbot, "Moore's Outlaws," *MIT Technology Review*, Vol. 113, No. 4, July/August, 2010, p. 43.

9. Mike Orcutt and Tommy McCall, in Brian Bergstein, "Going Offline: Google reveals how often governments ask it to banish things from its services and how often it complies." *MIT Technology Review*, Vol. 114, No. 6, November/December 2011, pp. 30-31.

10. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," available from *intelreport.mandiant.com/Mandiant_APT1_Report.pdf*.

11. Talbot, pp. 36-43.