ECIR EXPLORATIONS IN CYBER INTERNATIONAL RELATIONS

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

The Role of Cyberspace in International Relations: A View of the Literature

Robert Reardon
Political Science Department
Massachusetts Institute of Technology

Nazli Choucri
Political Science Department
Massachusetts Institute of Technology

April 1, 2012

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.

MINERVA INITIATIVE
DEPARTMENT OF DEFENSE

The Role of Cyberspace in International Relations:
A View of the Literature

Robert Reardon and Nazli Choucri[1]

Department of Political Science, MIT

Paper Prepared for the 2012 ISA Annual Convention

San Diego, CA

April 1, 2012

Abstract

This paper reviews the literature on cyber international relations of the previous decade. The review covers all journal articles on the role of cyberspace and information technology that appeared in 26 major policy, scholarly IR, and political science journals between the years 2001-2010. The search yielded 49 articles, mostly from policy journals. The articles are sorted into five distinct issue areas: global civil society, governance, economic development, the effects on authoritarian regimes, and security. The review identifies, and discusses the significance of three unifying themes throughout all of the articles: efforts to define the relevant subject of analysis; cyberspace's qualitatively transformative effects on international politics, particularly the empowerment of previously marginalized actors; and, at the highest analytic level, efforts to theoretically capture the mutually embedded relationship between technology and politics. These themes can help guide future research on cyber international relations, and focus attention on ways that debates within each of the five distinct issue areas are interconnected, and can be usefully approached using a unified conceptual framework.

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 authors and do not necessarily reflect the views of the Office of Naval Research.

[1] Comments should be directed to Robert Reardon, Department of Political Science, Massachusetts Institute of Technology, Cambridge, MA, reardon@mit.edu.

1. Introduction

Recent decades have witnessed such rapid changes in computer technologies that the period is frequently referred to as the "Digital Age." The most extraordinary development of the Digital Age has been the development of an interconnected and standardized set of globe-spanning networks of computers and communication devices. By 2012, this "network of networks" has developed into a global arena of interaction for countless shared activities and the exchange of information and ideas by people around the world, involving a sizable fraction of humanity on a daily basis.[2] It is now common to speak of the sum of these connections among computing and communications devices as a single, shared virtual domain: cyberspace.[3] In an astoundingly short time, activities in cyberspace have developed from a very marginal role in the overall scope of human affairs to a central one.

It is reasonable to expect that the development of cyberspace, because of its growing relevance to an increasing number of social and political activities, has begun to exert influence on the course of global politics. If one defines politics as, at its core, the determination through social relationship of "who gets what, when, how," then the rapid growth of social activity in cyberspace, and the increasing importance of relationships in that domain to international security, the global economy, political and social organization, and the development and spread of ideas, should be seen as potentially transformative.[4] Indeed, this is now often the received wisdom among journalists and policy makers, who have devoted increasing attention to the effects – good and ill – of cyberspace on human society.

It would also be reasonable to expect that the rise of cyberspace as a significant locus for human political, social, and economic activity would have attracted the attention of scholars of international relations. Even skeptics who doubt cyberspace can play a transformative role in international politics should be eager to subject common claims to critical and rigorous tests. Moreover, given that significant and growing public resources are now being expended to address various aspects of "cyberpolitics," including cyber security and military strategy, and the promotion of international access to cyberspace as a way to encourage global economic

[2] US policy documents characterize the Internet as a "network of networks." See *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington, DC: Executive Office of the President of the United States, 2009, p.C-8.

[3] This paper adopts the definition of cyberspace presented in the *Cyberspace Policy Review*: "The interdependent network of information technology infrastructures," which includes the Internet and other affiliated networks such as telecommunications networks. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington, DC: Executive Office of the President of the United States, 2009, p.1

[4] This widely used definition of politics comes from Harold D. Lasswell, *Politics: Who Gets What, When, How*, New York: Whittlesey House, 1936.

development and democratization, one could argue that social scientists have an obligation to address these issues, particularly if they are skeptical of these endeavors.[5]

This paper reviews the international relations community's efforts over the past decade to measure and understand the influence of cyberspace's on international politics. It highlights dominant themes, and identifies common theoretical and conceptual threads that cut both within and across different issue areas. It provides a useful baseline of current perspectives on cyberspace and its implications for international relations. With this analysis, we hope to signal the significance of cyberspace in international politics, point to the important work done so far, and identify critical next steps.

2. Approach and Methods

This study considers the body of cyber-related research that has appeared in the top English-language (largely, but not exclusively, American) academic international relations journals, as well as a number of the most highly respected political science journals that regularly publish articles in international relations. The search focused on the first decade of the 21st century (2001-2010), and involved a thorough search of a total of 26 journals: 18 academic journals, and for comparative purposes, 8 major policy-oriented journals. Of the 18 academic journals, 12 were IR-focused journals, while the remaining 6 were general political science journals. The following selection criteria were used: (a) articles that were of typical journal-article length (generally 4 pages or longer – *i.e.*, very short articles from the policy-oriented journals were excluded); (b) articles that were focused largely on issues related to cyberspace, information and communication technologies (ICTs), the Internet and Internet-based social media, or the "information revolution"; and (c) articles that concentrated largely on international issues. The study did include several articles that only secondarily or indirectly involved international considerations, but addressed issues high relevant to international politics (*e.g.*, single-country case studies that illuminated issues of international concern).[6]

[5] For a discussion of the meaning and relevance of "cyberpolitics" and related background materials, see Nazli Choucri, "Introduction: CyberPolitics in International Relations," *International Political Science Review* 21.3 (2000), 243-263.

[6] See Appendix for the list of journals included in the survey, and the articles found. Journals were chosen primarily, but not exclusively, according to its impact score and the breadth of topics covered and methodologies and paradigms represented.

3. Results

The search revealed remarkably few articles on cyber international relations. This was the case with both the policy and academic journals, but was most profound with the academic journals

3.1 Literature Search

Overall, between 2001-2010, in all 26 journals, there appeared 49 articles that met the selection criteria. Of the 49 articles, 16 appeared in academic journals, and 33 appeared in policy journals.[7] The 49 articles were sorted according to year, issue area, and international relations paradigm that most informed the analysis. There was notable variation in the number of articles published per year,[8] Interestingly, the decade began and ended with the strongest years for cyber-related publications in the policy journals: the two years 2001 and 2010 alone accounted for half of the policy articles over the entire 10-year period.

3.2 Central Themes

Nearly all of the articles (47 of the 49) fall into five major issue areas: global civil society, the governance of cyberspace, economic development, the effects of cyberspace on authoritarian regimes, and security. Two of the 49 (Herrera, 2003; and Manjikian, 2010) deal with broader theoretical issues of cyber international relations. Both the academic and policy literatures gave the most attention to cyber security. The academic literature focuses heavily on governance and on the prospects of a global civil society. By contrast, the policy articles pay more attention to development and the effects of cyberspace on authoritarian regimes. Overall, each of the five major issue areas was covered by at least one article from both the academic and policy literatures.[9]

[7] The average figures can be misleading, as the majority of academic journals that were considered in the study did not publish any cyber-related articles over the course of the decade. In fact, of the 18 included in the study, only 6 published one or more articles that met the criteria. Of these, only two journals published three or more articles: *International Studies Quarterly* (5), and *Millennium* (5). *Millennium* had such a high number of articles related to cyberspace because the journal released a special issue on the topic in 2003. Interestingly, of the 6 broad political science journals that were included, only one – *Political Science Quarterly* – published an article (and only one) that met the study's criteria. This stands in contrast to the policy journals, all of which published at least one cyber-related article during the decade. These journals covered a range from a low of one article (*Journal of International Affairs*) to 13 articles (*Foreign Affairs*).

[8] It is important to note that this overall variation was driven largely by the variation in the number of policy articles. The number of academic journal articles, in additional to being much less, exhibited less variation over the decade.

[9] Surprisingly, there was little correlation between topic and journal.

3.3 Conceptual Perspectives

The 49 articles were sorted according to the particular conceptual or theoretic paradigm or analytic lens that best describes the paper's analytic approach: realism, liberalism, or constructivism. The realist paradigm focuses on the distribution of power among states as the driving force in international relations.[10] Realists categorize world politics as a struggle among states under conditions of anarchy to maximize their security and guarantee their survival. Because states cannot rely upon a higher authority to protect them, they are, in the final analysis, dependent upon their own efforts to secure themselves from the predations of other states. Although realism allows for domestic politics, non-state actors, and other forces beyond the state itself to play an important role in determining international behavior, these forces do not challenge the primacy of states and state interests in international politics.

Liberal international relations theory focuses on the role that "[s]ocietal ideas, interests, and institutions" play in shaping state preferences, and in turn influencing state behavior.[11] Liberalism considers both domestic society, such as domestic political institutions and culture, as well as the operation of international non-state actors and social processes. Liberals view state preferences and behavior as being constrained and influenced by both domestic and international civil society.

Constructivism breaks with realism, liberalism, and institutionalism by focusing on the socially constructed nature of international relations rather than materially rooted interests and power relationships.[12] Constructivists argue that many of the structures practices of international politics are based on socially constructed identities, worldviews, and ideas, rather than material forces. Because of this, these structures and patterns of interaction can change according to changes in the actors' ideas and assumptions about the nature of the world. As a result, the exchange of ideas through "communicative action" can have an important effect on international relations that is independent of any change in underlying material conditions.

[10] Steven M. Walt, "The Progressive Power of Realism," *American Political Science Review*. 91.4 (1997), pp.931-936.

[11] Andrew Moravcsik, "Taking Preferences Seriously: A Liberal Theory of International Politics," *International Organization* 51.4 (1997), p.513.

[12] Alexander Wendt, "Anarchy is What States Make of It," *International Organization* 46.2 (1992), pp.391-425.

3.4 Comparative Features

Table 1 shows the distribution of the articles from the academic journals sorted by IR paradigm and major issue area.

TABLE 1: Articles from Academic Journals

	Realism	Liberalism	Constructivism	No Dominant Paradigm
Global Civil Society			• Comor (2001) • Deibert (2003) • Murphy (2009)	
Security	• Goldman (2004) • Newmyer (2010)		• Dartnell (2003) • Der Derian (2003) • Hansen and Nissenbaum (2009)	• Eriksson and Giacomello (2006)
Authoritarian Regimes		• Corrales and Westhoff (2006)		
Development		• Alden (2003)		
Governance	• Drezner (2004)	• Newman (2008)	• Farrell (2003)	
General Theory			• Herrera (2003)	• Manjikian (2010)

As Table 1 shows, constructivists dominated the academic literature on cyber politics over the decade. This was true even in the area of security, where realism is usually predominant. Half of the articles in the survey found in academic journals are constructivist. This is rather paradoxical. In the context of international cyber politics, realist theories of international relations are most applicable to issues related to cyber security and cyber warfare. Realist theories can help to explain how states use cyber technologies to advance their interests in security, and how they may respond to other states' cyber capabilities. Although many constructivists do not contest the idea that there is a material basis to security threats, they argue that the labeling of diverse activities as threats to national security is a product of intersubjective interpretation rather than materially determined. It may also be that constructivists' greater eagerness to engage with the cyber security issue reflects a reluctance on the part of realists to study cyberspace.

Table 2 shows the distribution of articles from the policy journals sorted by issue area and IR paradigm.

.

	Realism	Liberalism	Constructivism	No Dominant Paradigm
Global Civil Society			• Comor (2001) • Deibert (2003) • Murphy (2009)	
Security	• Goldman (2004) • Newmyer (2010)		• Dartnell (2003) • Der Derian (2003) • Hansen and Nissenbaum (2009)	• Eriksson and Giacomello (2006)
Authoritarian Regimes		• Corrales and Westhoff (2006)		
Development		• Alden (2003)		
Governance	• Drezner (2004)	• Newman (2008)	• Farrell (2003)	
General Theory			• Herrera (2003)	• Manjikian (2010)

TABLE 2: Articles from Policy Journals

Table 2 illustrates the dominance of the realist and liberal paradigms in the policy literature. Realism is the dominant paradigm on matters of security, while the liberal approach dominates on most other issues. This is unsurprising. Realist theories of deterrence, crisis management, and conflict may be used to understand whether cyberspace is stabilizing or destabilizing, whether cyber technologies will be a new source of conflict or of peace, and whether states will engage in cyber arms racing. Realism can also present a challenge to theorists who argue that the development and growth of cyberspace is undermining the authority of states and empowering new international actors. By contrast, liberal IR theories can help explain how access to cyberspace can promote the development and spread of political ideas, the organization of civil society, and the development of transnational social networks. Liberalism suggests that access to and control of cyberspace can shape state behavior and influence international politics. Liberal institutionalist theories are applicable to our understanding of international efforts to promote cooperation among states on issues related to cyber security, the governance of cyberspace, and cyber arms control. Similarly, liberalism can help explain the behavior of international non-state actors such as non-governmental organizations, ethnic and national groups, cybercriminals, and cyber terrorism.

4. A Closer Look at Central Themes

We now focus on each of the five central themes in the literature: global civil society, security, effects on authoritarian regimes, development, and governance. Each of the five issue areas is marked by its own set of debates and policy concerns. In a subsequent section, we highlight several underlying themes that cut across all five issue areas that could help to guide future research.

.

4.1 Cyberspace and Global Civil Society

For two decades, scholars have suggested that ICTs can foster the establishment of a "global civil society," *i.e*., civil transnational groups that exist and function across international borders and independent of the authority of states.[13] These groups, networked through – and empowered by – cyberspace, could together form the basis of a new and transformative global polity or "public sphere" that will reshape world politics and promote international peace and democratic norms.[14] Five of the articles from the survey address the role that cyber technology can play in fostering the development of such a "global civil society" (GCS).

The GCS literature most directly addresses the question of whether cyber technology has a transformative effect on the international system by examining its ability to promote the development of new transnational actors that transcend and challenge the authority of states. It is not surprising that constructivists have taken the lead in this area, as constructivism is in many ways best suited to address changes to identity through communicative action, a central mechanism for the development of a global civil society. Overall, the literature is critical of earlier work on IT and GCS, which most of the articles characterize as naïve and inappropriately optimistic.[15] Nonetheless – with the exception of Morozov, who is the most critical of utopian claims about cyber technology's ability to spread peace, freedom, and prosperity through the creation of global social networks – no author in this set dismisses the power of cyber technology

[13] The seminal work on this topic is Ronnie D. Lipschutz, "Reconstructing World Politics – the Emergence of Global Civil Society," *Millennium* 21.3 (1992), 389-420. Also see Manuel Castells, *The Rise of the Network Society*, Malden, MA: Blackwell,1996.

[14] The term "public sphere" is from Jürgen Habermas, *The Stuctural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, Cambridge, MA: MIT Press, 1989 (originally published in German in 1962). In this context, it refers to the development of a public virtual space that is global and independent of government authority, in which citizens can voluntarily associate in political discourse.

[15] Deibert qualifies Castells's "network society" argument by highlighting the politically contested nature of the architecture of cyberspace, and the uncertainty over its future course. Comor makes a similar argument in his critique of "GCS progressives." Ronald J. Deibert "Black Code: Censorship, Surveillance, and the Militarization of Cyberspace," *Millennium* 32.3 (2003), 501-530; Comor, Edward, "The Role of Communication in Global Civil Society: Forces, Processes, Prospects," *International Studies Quarterly* 45.3 (2001), 389-408; and Castells, 1996.

to promote new transnational actors, groups, and shared identities.[16] Each author offers important qualifications and conditions for the understanding of cyber technology's transformative effects on international politics and political actors.

All of the authors (again, with Morozov as an exception) see cyberspace as a potential tool of empowerment. Mernissi, for example, describes how cyber technology has empowered women in the Arab world by providing them with an accessible forum for political expression.[17] The openness and anonymity of cyberspace has given these women a voice they would otherwise have not had, and this is beginning to have a positive effect on the position of women in Arab society. Other authors, such as Schmidt and Cohen, describe cyberspace as empowering non-state groups relative to the state.[18] Similarly, Murphy argues that cyberspace is facilitating the creation of a Habermasian "public sphere" in the Arab world – an online civil political forum for rational debate and expression that can serve as an important critique of state authority, something that has never previously existed in the region.[19]

Several authors argue that prospects for a GCS will always be limited by the fact that social relationships established online are much weaker and more transient than the interpersonal ties and identities forged in the "real" world. Murphy describes online interactions as shallow, and citizens as typically more interested in light entertainment than political debate and expression. Comor offers the strongest argument about the transience of online relationships and their inferiority to real community ties. Identities, according to Comor, can be very resistant to the sort of "relatively mediated" relationships that are forged over the Internet. He is skeptical about cyberspace's ability to overcome local culture and regional identities and to replace them with global ones. Mernissi goes even further by describing cyberspace as a threat to local identity. She points to cyberspace's annihilating effect on the "*hadud*," the frontier between the private and public life.[20] Yet, while these authors raise logical points and important challenges to earlier assumptions in the literature, they fail to back up these claims with empirical analysis. They also fail to fully consider cases in which important transnational social ties already exist, and how these ties can be affected by cyberspace.[21]

[16] Evgeny Morozov, "The Internet," *Foreign Policy* 179 (2010), 40-44.

[17] Fatema Mernissi, "Digital Scheherazades in the Arab World," *Current History* 105.689 (2006), 121-126.

[18] Eric Schmidt and Jared Cohen, "The Digital Disruption: Connectivity and the Power of Diffusion," *Foreign Affairs* 89.6 (2010), 75-86.

[19] Emma C. Murphy, "Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere," *International Studies Quarterly* 53.4 (2009), 1131-1153

[20] Mernissi, 2006, pp.123-124.

[21] Murphy (2009) comes closest to this in her analysis of the Arab world. However, Murphy's central focus is whether an Arab public sphere is forming. The paper acknowledges that a number of pan-Arab groups

Murphy, Comor, Deibert, and Mernissi all see cyberspace as a potential vehicle for global capitalism and commercialism, which to varying degrees they describe as a threat to civil society. Murphy describes the Arab public sphere as being embedded in a broader global sphere dominated by international capitalism. This can have a fragmenting effect on the Arab public, and can overwhelm local culture. It also, according to Murphy, promises to spread to global norms of rationality and cosmopolitanism, which can serve as a check on anti-intellectual and anti-rational forces from within the region.[22] Deibert considers powerful commercial actors as an international force that threatens to undo the open architecture of the Internet. In particular, he cites the success that these actors have had in promoting strong protections for intellectual property, which threatens to reduce innovation and creativity.[23]

Several of the authors describe political contestation not only within cyberspace, but over the architecture of cyberspace itself. Schmidt and Cohen, for example, argue there is a contest over cyberspace between potential winners and losers. In this case, it is the large and democratic states of the West that will benefit most from the diffusion of cyber technology in its current configuration, while small and autocratic regimes will seek to mitigate the threat it poses to regime stability. Deibert argues that states may alter the very architecture of cyberspace to suit their purposes, fragmenting it into a "patchwork quilt."[24] Murphy considers the effect that "non-virtuous" identity-based transnational groups might have on the public sphere, as these groups can be empowered by cyber technology just as more "virtuous" civil-society groups can.[25]

A particularly valuable contribution to theory is Deibert's focus on the technical and material elements of cyberspace, and its relationship to these political contests. He observes that the technical characteristics of the Internet – the core of cyberspace – limit or shape what is possible in the political realm and, as a result, shape outcomes. Deibert highlights the fact that the open character of the Internet was consciously designed into the system by the creators and built into its architecture. While the Internet was designed this way, it can be changed. Simultaneously, political actors contest the design of this architecture. This duality touches the core of the relationship between technology and politics, and illuminates the mutually embedded relationship between them. As the technology spreads and impacts a wider range of actors and the things they value, these actors will contest the architecture of cyberspace and seek to redesign it at a technical level in order to advance their particular interests. Citizen and non-governmental

are empowered and strengthened by cyberspace, but does not address the conditions under which this might be the case, or the potential magnitude.

[22] Murphy, 2009, pp.138-139.

[23] Deibert, 2003, pp.506-511.

[24] Deibert, 2003, p,514.

[25] Murphy, 2009, p.1131.

advocates of an open architecture may prevail, but they will have to triumph over political, commercial, and military interests working toward the "colonization" cyberspace.[26]

Morozov correctly points out that there continues to be a lack of empirical evidence to support the claim that cyberspace is facilitating the rise of a GCS. The constructivist approaches used in this literature are not incompatible with empiricism, and would benefit from greater evidence. Deibert's argument that the architecture of cyberspace is being contested in ways that threaten its openness, for example, is well suited to case-study analysis. Close examinations of cases in which security and economic interests contested the very fabric of cyberspace with citizen groups,NGOs, and other stakeholders could lend greater weight to these arguments.

4.2 *Governing Cyberspace*

The contestation among a variety of international stakeholders – including states, international and non-governmental institutions (IOs and NGOs), private firms, and other non-state actors – over the technical standards, regulations, and institutions that determine the structure of cyberspace is the central issue in the governance of cyberspace.[27] Six of the articles from the survey – three from the academic literature – focus on governance. All of these articles examine how novel models of international governance may be constructed to adjudicate disputes among states and other international stakeholders over how the Internet ought to be structured and regulated. All are concerned to varying degrees with the role that states may play in this process. Although these authors disagree over the power that different states can have over Internet governance – and over how much influence they ought to have – they uniformly reject the early literature on the subject that imagined an open and decentralized Internet that was self-governing and self-regulating, and that could function completely independent of any state authority.

All three of the academic journal articles argue for the continued role of state authority in cyberspace governance. Drezner adopts the strongest position in this regard, arguing that state authority has not declined, and that outcomes in international cyber governance are determined by the interests of the most powerful states in the system.[28] Novel hybrid forms of governance that incorporate non-governmental and private actors, he argues, represent the purposeful delegation of authority by states. The structures of these institutions are determined by the collective gains

[26] Deibert, 2003, p.503, fn.6.

[27] A seminal work on this issue is Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999.

[28] Daniel W Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 199.3 (2004), 477-498.

they offer to the most powerful states, while weaker states are relegated to a marginal role. Non-governmental and private actors serve primarily as agenda-setters. Drezner draws on the governance structures for the Internet's technical standards such as ICANN (Internet Corporation for Assigned Names and Numbers), the EU's data privacy regulations, and international enforcement of intellectual property rights (IPR) to illustrate his point. Drezner convincingly argues that state power remains highly relevant to the governance of cyberspace. He admits, though, that non-state actors can still leverage their technical expertise to influence outcomes, and leaves open the question of how great a role other actors can play.

Newman challenges the assertion that governance outcomes are determined by the distribution of state power. Looking at the development of data privacy regulations in the EU, he argues that "transgovernmental policy entrepreneurs" were responsible for creating international privacy rules, and that if the interests or preferences of the most powerful EU states determined the outcome that no such regulations would have been created.[29] Newman identifies national-level private data authorities among the EU member states as the principal drivers of international rulemaking. The data authorities successfully used their domestic authority and expertise as levers to push for EU-level regulations, and were motivated by their particular bureaucratic interests. Newman's argument presents a strong challenge to the claims of Drezner and others who are skeptical of the erosion of state authority. More empirical work is needed, however, to determine whether such findings are can be generalized, and applied beyond the EU, whose supranational governance structures and relatively homogenously national preferences could make it unrepresentative of broader issues of global governance. It is unclear the degree to which Newman's thesis reflects characteristics unique to cyberspace, globalization in general, or the EU in particular.

Farrell, too, argues that state authority over cyberspace has not declined. In a largely constructivist analysis, he looks at the Safe Harbor agreement between the United States and the EU on data privacy, and finds that while the agreement is in fact a novel hybrid approach to international governance based on private rule implementation, the basic rules themselves were instituted by state authority, and that the Safe Harbor agreement provides an important role for states both in its design and enforcement.[30] In this case, states resorted to new governance forms in order to reconcile divergent normative values about privacy and about the state's authority to regulate in this area. These new forms are not the direct result of the distribution of power among

[29] Abraham L. Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive," *International Organization* 62.1 (2008), 103-130.

[30] Henry Farrell, "Constructing the International Foundations of E-Commerce – The EU-US Safe Harbor Agreement," *International Organization* 57.2 (2003), 277-306.

the states involved, nor are they a compromise between the initial US and EU bargaining positions. Instead, the two sides arrived at a novel solution to the governance problem they faced through persuasion and "communicative action," leading each party to support a governance structure it had not previously considered.

Writing for the policy community, Cukier and Baird both propose similar public-private partnerships for governance that rely on the authority of states for legitimacy and effectiveness. Cukier argues that governments offer greater opportunities for democratic participation than international organizations and NGOs, and can provide greater legitimacy.[31] He argues that hybrid institutions for governance can successfully combine the democratic legitimacy of governments and their superior powers of enforcement with the inclusiveness and superior expertise of pluralistic systems. Baird also describes international organizations as insufficiently democratic, and as unable to fully represent all of the relevant stakeholders needed for effective Internet governance.[32] Looking specifically at ICANN, however, Baird suggests that the United States's unique relationship with this organization, however exclusive and inequitable, is preferable to any international model of governance that would jeopardize the openness of the Internet. The United States, she argues, has a greater commitment to liberal values than most states, and is more likely to guarantee that those values are reflected in the governance of the Internet than would be the case with any arrangement that provides greater decision-making authority to other international stakeholders, which often have interests that are at odds with these values. Both Cukier and Baird favor, in general, a more inclusive set of governing institutions that mix states with private and non-governmental actors. Aside from the problem of other powerful actors espousing values that are at odds with those of the liberal West, both also acknowledge the difficulty of creating such institutions in a way that allows the less powerful stakeholders in the international system to have a voice. In particular smaller and poorer states have had little influence over the regulations, laws, and technical standards that define cyberspace. The issue is not simply providing these states a seat at the table, but that they often lack the expertise and organizational capacity to deal with many of these issues.

Cukier, Baird, and Lessig all devote attention to the Internet's underlying architecture, and how the political contestation of technical standards and regulations – particularly the regulation of intellectual property – determine the degree to which cyberspace can function as an open "commons" and a progressive political force. Baird and Lessig both see the open design of

[31] Kenneth Neil Cukier, "Who Will Control the Internet," *Foreign Affairs* 84.6 (2005), 7-13.
[32] Zoë Baird, "Governing the Internet: Engaging Governments, Business, and Nonprofits," *Foreign Affairs* 81.6 (2002), 15-20.

cyberspace as the fundamental underpinning of both political freedom, and of technological innovation and global economic development. Lessig makes the most specific argument in this regard, pointing to the way in which the Internet's architecture, as originally configured, can serve as a platform upon which innovative new applications can be developed, such as the World Wide Web. These authors argue that such innovation is possible only so long as cyberspace is maintained as a global commons. Lessig argues, however, that the "enclosure" of the cyber commons has already begun, and points especially to stronger intellectual property rights for software. Such regulations advance the interest of the most powerful actors in the system at the expense of the weakest. They dampen innovation and raise the barriers to international development and economic growth.[33]

One of the most interesting aspects of the literature on governance is its identification of the tradeoff in the governance of cyberspace between inclusivity and openness. Nearly all authors favor a more inclusive and democratic arrangement for cyberspace governance that better represents the diversity of stakeholders. Outside of the liberal West, few stakeholders are willing to support continuing the Internet's existing architecture. In fact, as Lessig points out, and as many of the authors in other sections of this survey have argued, the openness of cyberspace has already begun to change, and the cyber commons has long begun to fragment along political boundaries. No one in this set offers a clear way forward, or a solution to these fundamental problems with governance. Farrell provides the important insight that persuasion can be an effective mechanism for shared governance, and a tool for reconciling fundamental differences in values. If cyberspace indeed promises to have a progressive transformative effect on international politics, or can do so under certain conditions – a claim that very much remains open to question – then the governing institutions that shape cyberspace's architecture, and in turn its social political effects, will be critical.

4.3 Economic Development

Eight of the 49 articles address the promise cyber technology holds for international economic development. This is an area that has traditionally been marked by optimism, as illustrated in the early literature on the "knowledge economy," which emphasized the potential gains in economic growth that could be achieved from a greater ability to quickly send, access, and store information on a global scale.[34] Persaud, for example, considers cyberspace as a

[33] Lawrence Lessig, "The Internet Under Siege," *Foreign Policy* 127 (2001), 56-65.

[34] While economists and social scientists have long studied the role of information and knowledge in economic activity, discussion of a "knowledge economy," in which ICTs have brought about

mechanism for the improved flow of knowledge which itself is treated as an economic good. He imagines the diffusion of IT – along with international economic liberalization – as a way to allow capital to flow across borders to be invested in "good ideas." "[K]nowledge development" is likely to take place at network nodes where the educated and trained are most heavily concentrated, giving the centers of the developed world an added advantage.[35]

While the authors of these eight articles are, to different extents, optimistic about information technology's impact on economic growth, they also acknowledge that these effects are not equitably and evenly distributed across different societies. Instead, the diffusion of cyber technology is likely to create – and to deepen – a "digital divide" between the developed societies capable of better harnessing the technology for productivity gains, and the less developed that are not. Hammond, for example, claims that this increasing gap could ultimately create a security threat, as the poor who are excluded from the global information society and its wealth turn to violent means as a way to capture some of these gains.[36]

Yet the authors do not agree on the specific causes of the digital divide or the appropriate policies to address it. Funabashi, for example, argues that underdeveloped countries can take advantage of information technology and "leapfrog" past developed states: *i.e.*, less developed states can move directly to the latest technologies such as satellite and mobile telecommunications systems, or advanced wireless Internet systems.[37] Others, such as Litan, argue that such leapfrogging is not possible so long as states lack the human capital, regulatory practices, and stable legal, political, and economic institutions necessary to leverage technology for economic development.[38] Poor states also often lack even the most basic physical

transformative change in the social and economic order, can be traced to the seminal works of Fritz Machlup, *The Production and Distribution of Knowledge in the United States*, Princeton, NJ: Princeton University Press, 1962; Peter F. Drucker, *The Age of Discontinuity: Guidelines to Our Changing Society*, New York: HarperCollins, 1969; and Peter F. Drucker, *Post-Capitalist Society*, New York: HarperCollins, 1993. Most of the authors considered here make a less expansive argument than Drucker's, whose thesis is more akin to that of Castells in arguing that the new information technologies would bring about a fundamental categorical shift in the economic and social order that would challenge the primacy of states in the international system (Castells, 1996). Most of the authors considered in this section argue only that the evolution and diffusion of cyber technologies will have a significant effect on economic production and the distribution of wealth. For an economic analysis of the effect of ICTs on economic growth and productivity, see For a dissenting view, see Erik Brynjolffson and Adam Saunders, *Wired for Innovation: How Information Technology Is Reshaping the Economy*, Cambridge, MA: MIT Press, 2009. For an earlier, dissenting view, see Robert J. Gordon, "Does the New Economy Measure up to the Inventions of the Past?" *Journal of Economic Perspectives* 14.4 (2000), 49-74.

[35] Avinash Persaud, "The Knowledge Gap," *Foreign Affairs* 80.2 (2001), 109.

[36] Allen L. Hammond, "Digitally Empowered Development," *Foreign Affairs* 80.2 (2001), 96-106.

[37] Yoichi Funabashi, "Asia's Digital Challenge," *Survival* 44.1 (2002), 135.

[38] Robert E. Litan, "The Internet Economy," *Foreign Policy* 123 (2001), 16-24.

infrastructure on which an information-based economy would depend, such as a reliable supply of electricity.

Alden, who focuses on IT in Africa, offers a different view. While Alden agrees that cyberspace offers benefits for Africa's urban elite, and leaves the rural poor behind, he argues that initiatives by the developed countries to expand the reach of IT in Africa only further the interests of the wealthy interests with an economic stake in the development of cyberspace.[39] He points to the coupling of IT diffusion with economic liberalization policies as evidence that the driving factor behind these initiatives is not development but the expansion of global capitalism. To Alden, the diffusion of IT is simply a new form of imperialism.

Hammond, on the other hand, argues that it is powerful corporate interests themselves that are most capable of laying the foundation for IT diffusion among the underdeveloped. He supports "enlightened capitalism" in which corporations partner with NGOs and public charities to deliver services on a global level.[40] Others, such as Kudaisya and Bletha, believe that it is the government itself that must play this role. Looking at the development of cyber technologies in the United States and East Asia,[41] Bleha argues that East Asian states such as Japan and South Korea have been more effective at building IT infrastructure because of improved policy choices. Barshefsky and Persaud see an important role for the government in establishing strong protections for intellectual property, all within a liberal international trade regime.[42]

Ultimately, much of the debate in this literature is over broader development strategies and the appropriateness of neoliberal policies. Few of these arguments are unique to cyberspace, and reflect the authors' orientations toward different development strategies and toward globalization as a whole. The other authors accept IT as a legitimate development tool, but disagree over how much influence must be granted to disempowered actors in the international

[39] Christopher Alden, "Let Them Eat Cyberspace: Africa, the G8 and the Digital Divide," *Millennium* 32.3 (2003), 457-476. A similar argument is made by Kudaisya in his examination of the role that IT has played in India's economic development. He argues that the vast majority of the country's population is too poor, rural, and uneducated to take part in the information revolution. Gyanesh Kudaisya, "India's New Mantra: The Internet," *Current History* 100.645 (2001), 162-169. At the time of Kudaisya's writing, Internet penetration in India was extremely low, and limited to the educated and urban elite. Internet and mobile telecommunications penetration in India has increased enormously since 2001. As of the end of 2011, 10% of India's population of 1.2 billion was using the Internet. An additional 346 million Indians had mobile telephones with data-package subscriptions. Rajini Vaidyanathan, "Is 2012 the Year for India's Internet?" *BBC News*, January 3, 2012, http://www.bbc.co.uk/news/business-16354076.

[40] Hammond, 2001, p.106.

[41] Kudaisya, 2001; Thomas Bleha, "Down to the Wire," *Foreign Affairs* 84.3 (2005), 111-117; and Philip J. Weiser and Thomas Bleha, "Which Broadband Nation*?" Foreign Affairs* 84.5 (2005), 161-166.

[42] Charlene Barshefsky, "Trade Policy for a Networked World," *Foreign Affairs* 80.2 (2001), 134-146; Persaud, 2001.

governance of cyberspace, and over the level of economic development and state capacity that is required for poorer societies to reap the benefits of access to cyberspace.

Missing from this literature is a fuller explanation of how IT can itself help to provide many of the necessary conditions for societies to successfully exploit cyberspace for economic gain. Hammond comes closest to recognizing this, suggesting that outside actors are well suited to provide a range of basic services related to IT that can then be used by underdeveloped societies to achieve economic growth. He is not explicit, however, about which services – such as education, strong national IP protections, or advanced infrastructure – are most necessary, or why.

The literature on cyberspace and development also suffers from a lack of empirical studies. As is the case in other areas, this likely results at least in part from a lack of data. Nearly all of the authors are writing in the early 2000s, when cyber penetration in the developing world remained at near-trivial levels, and the effects of cyber on development may have been too small for empirical analysis. New studies that reexamined these issues with more recent data would be valuable.

4.4. Cyberspace and Authoritarian Regimes

A third distinct issue area in the literature is the effect of the diffusion of cyberspace on authoritarian regimes. These regimes may be faced with a “dictator’s dilemma”: in order to reap the potential economic rewards offered by adopting information technologies, they must accept the political risks these same technologies present.[43] In the earliest days of the Internet, many scholars and policy analysts were optimistic about the democratizing and liberalizing effects that cyberspace would have on societies ruled by authoritarian regimes.[44] The articles in this survey are, for the most part, less sanguine. There are two notable outliers. Mavhunga (2005) views cyberspace as a liberating tool, empowering “cyber-guerillas” in Zimbabwe (as well as Zimbabweans in the diasporas abroad) and enabling them to challenge the Mugabe regime’s

[43] Landmark works on this issue include Christopher R. Kedzie, *Communication and Democracy: Coincident Revolutions and the Emergent Dictator's Dilemma*, Santa Monica, CA: RAND,1997; Taylor C. Boas, "The Dictator's Dilemma: the Internet and U.s. Policy Toward Cuba." *Washington Quarterly* 23.3 (2000), 57-67; and Shanthi Kalathil and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*, Washington, DC: Carnegie Endowment for International Peace, 2003. A related literature addresses the effects of cyberspace on governance in mature democracies. See Walter B. Wriston, "Bits, Bytes, and Diplomacy," *Foreign Affairs* 76.5 (1997), 172-182; and Bruce Bimber, "The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism," *Polity* 31.1 (1998), 133-160.

[44] See Kalathil and Boas, 2003, pp.1-2.

narrative with its own “counternarrative.”[45] Reynolds (2004), looking at the online political discourse in the United States after the 9/11 attacks, argues that the Internet acted as a force for the promotion of human rights, paradoxically by providing a forum where citizens could challenge the traditional media, which he characterizes as “friendlier to war opponents.”[46] The other authors, however, see cyber technology as “value neutral.”[47] They argue that authoritarian regimes can effectively manage this tradeoff, at least over the near- and medium-term, and exploit the economic potential of information technology while mitigating its negative political effects.

Boas, Hachigian, and Kalathil all describe the subtle and complex systems of control that authoritarian regimes can use to overcome the politically destabilizing effects of cyberspace. Hachigian’s description of the Chinese Internet is the most detailed. China employs a spectrum of tools to control access, censor online activity and expression, and encourage regime-supporting online political activity. The resulting system semi-permeable: the state is unable to monitor and censor the vast number web sites that can be accessed, but can raise enough of a barrier to dissuade all but the determined from visiting politically sensitive sites, and reduces the number that do so to a manageable amount. The regime leverages its control over the domestic network to create a set of market incentives for service providers to engage in self-monitoring and self-censorship without the need for any direct state role. Similarly, through high-profile and well-published arrests, the Chinese government encourages self-censorship on the individual level. Finally, the regime uses cyberspace to its own advantage by using it as a platform for its own propaganda and by encouraging online displays of nationalism by citizens.[48]

Hachigian argues, however, that not all authoritarian regimes are adopting the Chinese model of control. Authoritarian regimes, she argues, will choose different regulatory approaches and control mechanisms depending on the relative importance of ideology and the provision of economic growth and improving living standards as the basis of their legitimacy. Because Beijing’s legitimacy rests on its ability to deliver economic benefits to its citizens, it chose a strategy that maximizes access to cyberspace while adopting intricate control systems to limit its political effects. Other states such as North Korea, where the regime’s legitimacy rests on ideological claims, have chosen not to promote cyber access. Other regimes, like that in Burma,

[45] Mavhunga, Clapperton, “The Glass Fortress: Zimbabwe’s Cyber-Guerilla Warfare,” *Journal of International Affairs* 62.2 (2009), p.160.

[46] Glenn Harlan Reynolds, “The Blogs of War,” *National Interest* 75 (2004), p.62. Reynolds, a prominent conservative blogger, has a personal interest in the argument that blogs are serving as a check on liberal media bias.

[47] Ian Bremmer, “Democracy in Cyberspace,” *Foreign Affairs* 89.6 (2010), 86-92.

[48] Nina Hachigian, “The Internet and Power in One-Party East Asian States,” *Washington Quarterly* 25.3 (2002), 41-58; and Nina Hachigian, “China’s Cyber-Strategy,” *Foreign Affairs* 80.2 (2001), 118-133.

occupy a middle ground. Corrales and Westhoff offer a similar theoretical claim, arguing that it is the degree to which a regime is economically inward- or outward-looking that determines the strategy it uses toward adopting cyber technology. Corrales and Westhoff offer the only scholarly article in the sample, and provide the most empirically rigorous test of their theory by using a large-*n* analysis.[49]

Despite this pessimism about the politically liberalizing potential for cyberspace, Kalathil and Hachigian argue that over the longer term, cyberspace will promote democratic political change. For Hachigian, this is likely to happen suddenly as the result of a crisis. She maintains that a state like China could lose its ability to effectively censor online communication and exchange in the heat of a political crisis, and this could snowball into a serious political challenge to the regime. It is unlikely that this will happen, though, until cyber technology has penetrated much more deeply into Chinese society (Hachigian is writing in 2001 and 2002). Kalathil believes change will occur more gradually. Kalathil's argument rests on adoption by China and other authoritarian regimes of ICTs as a way to streamline the provision of government services. In the near term, this benefits the regime by increasing its legitimacy and strengthening its capacity and its ability to exercise political control in the provinces. However, this process will ultimately promote greater transparency, which could lead to more democratic governance.[50]

Boas, Hachigian, and Corrales and Westhoff demonstrate that this is an area ripe for theory development. All offer convincing hypotheses to explain both how authoritarian regimes will approach cyberspace and how cyberspace might effect political change in those regimes. This is another area where more empirical work is badly needed. This is particularly the case in the wake of the Arab Spring, Iran's Green Movement protests, and other political movements in which information technology played a visible role. Such recent cases offer a potentially rich testing ground for theory.[51]

4.5 Cyberspace and Security

Nineteen of the 49 articles examine the relationship between cyberspace and international security. Within this issue area, the authors discuss a wide variety of phenomena – so wide, in fact, that it begs the question of exactly what is meant when the authors use terms such as "cyber conflict," cyber security," or "cyber warfare." The issues these articles discuss include

[49] Javier Corrales, and Frank Westhoff, "Information Technology Adoption and Political Regimes," *International Studies Quarterly* 50.4 (2006), 911-933.
[50] Shanthi Kalathil, "Dot.com for Dictators," *Foreign Policy* 135 (2003), 42-49.
[51] This is not to say that there has not already been important case-study work on this issue. See, for example, Kalathil and Boas, 2003.

propaganda, tactical "information operations," strategic attacks on critical infrastructure, espionage. They include routine phenomena such as attempts to penetrate sensitive networks, and speculative scenarios such as massively destructive "cyber attacks" against civilian targets.[52] The discussion in this literature also takes place on two different levels. On one level, there is a discussion about the nature of the threat and potential means to address it. On another, there is a meta-discussion about the ontology and epistemology of cyber security, and the evolution of the concept. The latter often portrays the former as an exercise in alarmism, where loosely defined and speculative threats are presented in order to advance particular political agendas. While the policy articles from this literature, which are largely informed by realist assumptions, typically fall within the first discussion – the material nature of the threat – the articles from the academic literature are typically constructivist, and engage with the meta-discussion on the security discourse itself.[53]

Several of the authors treat IT as a military technology that can enhance traditional forms of state military power. However, even within this group, there is some disagreement over the nature of the technology and how it can best enhance military capabilities. Newmyer and Goldman, for example, both discuss the contribution of IT to the revolution in military affairs (RMA).[54] Goldman describes how IT can serve as a foundational element of RMA on which

[52] The term "cyber attack" is perhaps the least specific, as it is often used to refer to any malicious activity via cyberspace. This includes propaganda, denial of service, data corruption, espionage, or sabotage. The effects may or me not be violent, and in fact may or may not spill over into the physical realm. Many – if not most – of these activities would not be considered an "attack" under normal uses of the term. "Cyber security" is an equally broad term. In general, it refers to the integrity of electronic networks, their intended use, and all associated data and systems. This could include anything from ordinary hygiene on personal systems to the defense of military networks from electronic warfare. It can also refer to both the defense of one's own networks or the development or use of offensive capabilities against an adversary. For a thorough review of the different terms and the evolution of related concepts, particularly in the context of US government use, see Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*, New York: Routledge, 2008.

[53] Liberalism is poorly represented in the sample overall. As Eriksson and Giacomello note, liberal scholars of IR have in general paid less attention to security. Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27.3 (2006), 221-244.

[54] Emily O. Goldman, "Introduction: Information Resources and Military Performance," *Journal of Strategic Studies* 27.2 (2004), 195-219; Jacqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *Journal of Strategic Studies* 33.4 (2010), 483-504. Although the term "revolution in military affairs" or "RMA" dates back more than three decades, it became popular to speak of such a revolution after the first Gulf War. The term refers to qualitative changes in military capabilities brought on my technological innovation and/or novel forms of military organization. There is no consensus, however, over which technologies or organizational innovations are most important, or even whether such a revolution is taking place. For a useful summary, see Theodor W. Galdi, *Revolution in Military Affairs?: Competing Concepts, Organizational Responses, Outstanding Issues*, Washington, DC: Congressional Research Service, 1995. Also see John Arquilla and David Ronfeldt, "A New Epoch – and Spectrum – of Conflict" in *In Athena's Camp: Preparing for Conflict in the Information Age*, John Arquilla and David Ronfeldt, eds, Santa Monica, CA: RAND, 1995, pp.1-20.

other capability-enhancing technologies depend. She describes IT as an efficiency-booster or multiplier that allows modern militaries to quickly distribute large volumes of information and – importantly – parse them in order to identify what is strategically useful. Newmyer, though, sees IT primarily as a tool or information operations (IO) that can disrupt an adversary's information systems. This can include psychological operations, military deception, electronic warfare, and computer network operations (CNO).[55] For Goldman, IT is most useful to states that already possess sophisticated military capabilities, while for Newmyer, it is a tool of asymmetric warfare that provides advantages to weaker challengers (in this case China) through its low barriers of adoption and use.

Others, including Bousquet and Littwak, focus less on the technology itself, and more on the importance of networked forms of military organization, for which IT is merely an important facilitator. Bousquet, for example, describes warfare in the digital age as "chaoplexic," *i.e.*, based on decentralized and highly mobile units capable of swarming and adapting their strategy and tactics in real time according to an adversary's reactions.[56] Luttwak adopts a similar view in arguing that IT has not actually produced significant military gains for the United States because it has failed to adapt organizationally.[57] He argues that the thinking of US military planners is flawed in considering IT to be a capability-enhancing technology, when in fact it requires a qualitative transformation in force structure in order for its full gains to be realized. Luttwak, however, sees the ability of reaping the benefits of network-centric organization as dependent upon the underlying technology, and therefore achievable only by the most advanced and sophisticated militaries.

Clarke and Lynn describe cyberspace as a new "domain" of conflict, a battle space in which both states and non-state actors can launch strategic "cyber attacks" against adversaries.[58]

[55] The U.S. Department of Defense defines information operations (IO) as: "[t]he integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." The terms used in the text are not those used by Newmyer, but are official terms form the Defense Department lexicon. Psychological operations, military deception, CNO, and electronic warfare are 4 of the military's 5 core IO capabilities. Chairman of the Joint Chiefs of Staff, "Department of Defense Dictionary of Military and Associated Terms," Joint Publication 1-02, November 8, 2010 (as amended through January 15, 2012), p.160; Chairman of the Joint Chiefs of Staff, "Information Operations," Joint Publication 3-13, February 13, 2006, Chapter II.

[56] Antoine Bousquet, "Chaoplexic Warfare or the Future of Military Organization," *International Affairs* 84.5 (2008), 915-929.

[57] Luttwak, Edward N., "Power Relations in the New Economy," *Survival* 44.2 (2002), 7-17.

[58] Richard Clarke, "War from Cyberspace," *National Interest* 104 (2009), 31-36; William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89.5 (2010), 97-108. The 2011 Pentagon strategic plan for cyberspace identified cyberspace as an "operational domain," akin to other domains such as air, sea, and space. The Defense Department stated its plan to "organize, train, and equip for cyberspace as we do in air,

Such conflict can be wholly contained within cyberspace, lead to escalation among the combatants in the physical world, or inflict economic or physical damage. There is disagreement here as well, though, over the nature and scale of the threat. Clarke refers to constant and increasing attacks in cyberspace, but does not specify what is being attacked, or what sort of attacks are taking place. In fact, we discover that for the most part these "attacks" consist of espionage, an activity not traditionally considered to be an attack at all at least not in the context of internationally accepted laws of war.

Clarke, Clark and Levin, Lynn, and Christopher Hughes all argue that large-scale strategic attacks through cyberspace against "critical infrastructure" pose a grave threat to national security.[59] Such attacks might be attractive to an adversary, they argue, because they can be cheap and difficult to trace. Cyberspace was designed to be an open environment, and has an architecture that allows for substantial anonymity, often making it difficult or impossible to attribute an attack to a particular attacker with confidence. These authors tend to draw on neorealist concepts of international security that were developed during the Cold War, especially deterrence theory and the offense-defense balance. They place emphasis on the low cost of cyber attacks, particularly in contrast to higher cost of defenses. They all argue that mere defenses are insufficient protection against cyber attacks, as they impose little or no cost on an unsuccessful attacker, who is free to try again. As a result, the United States and its allies must develop offensive cyber capabilities (as well as more "active" defenses that can scrutinize the contents of packets) as a deterrent.[60]

The academic literature on cyber conflict, in contrast to the policy literature's realist tendencies, is mostly constructivist. This literature has mostly focused on how cyberspace facilitates the spread of transformative ideas that can lead to changes in identity and perceptions that threaten to disrupt the existing social order. A number of the articles deal explicitly with the way this process has come to be interpreted as a threat to national security. Der Derian, for example, argues that both the emergence of the "Digital Age" and the attacks of September 11, 2001 have in different ways "transformed the meaning and discourse of national security."[61] Der Derian envisions two manners of transformative discursive change, both drawing on the

land, maritime, and space to support national security interests." U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, p.5.

[59] Clarke, 2009; Lynn, 2010; Wesley K. Clark and Peter L. Levin, "Securing the Information Highway," *Foreign Affairs*, 88.6 (2009), 2-9; Christopher R. Hughes, "Google and the Great Firewall," *Survival* 52.2 (2010), 19-26.

[60] It is Lynn (2010) who raises the need for "active" defenses. However, the term is not precisely defined, and its meaning is not entirely clear from the context of the article.

[61] James Der Derian, "The Question of Information Technology in International Relations," *Millennium* 32.3 (2003), p.452

communicative power of cyberspace and other forms of communications technology. On the one hand, there is "poeisis," in which a positive transformation of thought can be brought about by demonstrating new possible forms for the international security discourse. Der Derian uses the fall of the Berlin Wall in 1989 as an illustrative example. On the other hand, there is "mimesis," in which repetitive and violent visual images – which Der Derian labels as "infowar" – can lead to a starker security discourse. Der Derian cites the 9/11 attacks as an example of mimesis. He argues that these two transformative processes contest one another in an "epistemic battle for reality" to define the security discourse.[62] To Der Derian, the current vogue of "cyber security" is a result of this process. He desires to return to the pre-9/11 "Digital Age" zeitgeist.

Dartnell discusses how cyberspace can be used as a medium through which powerful messages can promote change in individuals' identities and therefore reshape political boundaries and actors. He describes this process as "transform[ing] the notions of self and safety that are at the heart of security."[63] For Dartnell, the chief actors are not states behaving tactically but non-state actors hoping to spread "transnational ideological radicalism" strategically.[64] Rather than logic bombs and malware, Dartnell and Der Derian focus on the role of ideas in international security. Ideas do not threaten critical infrastructure or military capabilities, but can destabilize the social and political order by altering actors' notions about safety, threat, and violence.

The most relevant articles in the policy literature to these arguments concern the use of cyberspace by terrorists to organize, recruit, gather intelligence, and coordinate attacks. Authors such as Kohlmann and Brachman describe a virtual war (or "netwar") waged in cyberspace by decentralized, networked organizations of terrorists and fellow travelers.[65] Kohlmann goes so far as to argue that the threat from cyber terrorists is greater than that the risk of an attack against critical infrastructure. These terrorists are waging a war that the United States is "gradually losing" because of its failure to mount an offensive against them.[66] Echoing Dartnell and Der

[62] Der Derian, 2003, p.453.

[63] Michael Dartnell, "Weapons of Mass Instruction: Web Activism and the Transformation of Global Security," *Millennium* 32.3 (2003), p.478.

[64] Dartnell, 2003, p.486.

[65] Evan F. Kohlmann, "The Real Online Terrorist Threat," *Foreign Affairs* 85.5 (2006), 115-124; Jarret Brachman, "Watching the Watchers," *Foreign Policy* 182 (2010), 60-67. Arquilla and Ronsfeldt coined the term "netwar" to refer to "societal-level ideational conflicts waged in part through internetted modes of communication." This can include "public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks." They distinguish this from "cyberwar," which they use in manner similar to military information operations. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" in Arquilla and Ronfeldt, 1995, pp.27-28.

[66] Kohlmann, 2006, p.115.

Derian, Kohlmann argues that these groups have been particularly effective at spreading propaganda by using video and other high-impact media. Brachman argues that a new class of cyber terrorists – or "jihobbyists" – operate mostly or even exclusively online as propagandists and recruiters. Conway, on the other hand, argues that the concept of "cyberterrorism" is itself flawed, arguing that most of the activities discussed by authors such as Kohlmann and Brachman are not in fact acts of terrorism properly construed.[67] They do not entail acts of violence against noncombatants, and are often even legal activities.

Conway's critique raises larger ontological problems with the literature on cyber security. In particular, the terms "attack," "war," "threat," and "security" are used ambiguously, and often refer to activities that are not generally viewed as acts of war or threats to national security. This issue is most directly addressed by Hansen and Nissenbaum, who analyze the discourse of "cyber security" by drawing on the Copenhagen School's concept of "securitization," which considers "security" to be a "discursive modality with a particular rhetorical structure and political effect" that places threats to particular "referent objects" beyond (or above) the scope of normal politics.[68] These authors consider how "cyber security," a term originally reserved for the technical integrity of networks, became a matter of national security and high politics. Following Deibert, they identify four referent objects to which cyberspace presents an existential threat, either materially or "ideationally" the state, the nation, private actors, and networks.[69] However, they reject Deibert's notion of four separate discourses of cyber security, and instead argue that the four referent objects offer "competing articulations" for a single discourse of cyber security. This complex process of securitization takes place through three mechanisms, or "grammars" of discourse: the use of technical expertise as a means of speaking authoritatively, the connection of cyber security to everyday activities and practices, and "hyper-securitization" in which cyberspace is linked to cascading and cataclysmic disaster (which has never occurred in reality).

Hansen and Nissenbaum's approach usefully draws attention to the way cyber phenomena have come to be defined within the national security context, and illuminate the several important mechanisms through which this has occurred. However, by treating all security threats simply as products of the social discourse, it cannot distinguish cyber security from other security issues, and therefore cannot be used to determine the degree to which cyber security is

[67] Maura Conway, "What Is Cyberterrorism?" *Current History* 101.659 (2002), 436-442.

[68] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53.4 (2009), p.1156.

[69] Hansen and Nissenbaum, 2009, p.1163; Ronald J. Deibert, "Circuits of Power: Security in the Internet Environment," in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, James N. Rosenau and J. P. Singh., eds, Albany: State University of New York Press, 2002, pp.114-142.

politically motivated alarmism or a measured response to legitimate external threats. This is a critical distinction for policy makers: if the cyber threat has been inflated relative to other security concerns, this information should be available to inform the policy process and the allocation of defense resources. From a theoretical perspective, while the literature has identified important mechanisms for securitization, it has failed to explore the bureaucratic or organizational interests that could be driving this process. Who or what drives the various competing articulations of cyber security, and what are the motives?

The literature also fails to fully address the roles of non-state and private actors in cyber defense. Several of the authors note that cyber security's heavy involvement of civilian actors in the private sector distinguishes it from traditional deterrence contexts. Clarke and Adams, for example, both describe the private sector as the principal target for cyber attacks.[70] Both also suggest that the military play a larger role in defending civilian networks. Yet there has been little effort to explore the ramifications of this interdependence between the state and private sector beyond Rex Hughes's observation that cyber blurs the boundary between the two. More is said about non-state actors in the academic literature. Der Derian describes how non-state actors are becoming "super-empowered players" in a "global heteropolar matrix" of networked relationships.[71] Dartnell similarly describes the empowerment of non-state actors and the formerly marginalized in cyberspace.[72] Yet these authors focus on non-state actors as potential threat agents in cyberspace. They address neither the interdependence between the state and private sector in securing cyberspace, nor do they fully explore the ways in which different non-state actors might be empowered by cyber technology.

5. Unifying Themes

The convergence among the 49 articles on five distinct issue areas suggests that there is broad agreement among the international relations community, both academic and policy-oriented, about what the most important debates are over cyberspace. However, the fact that 47 of the 49 articles can be categorized into these five issue areas illustrates how little work has been done, at least in the major journals, on conceptual themes and theoretical puzzles related to cyberspace that connect these five issue areas. By looking across the entire set of 49 articles, particularly the two – Herrera (2003) and Manjikian (2010) – that do address broader cross-cutting issues, we identify three unifying themes: defining cyber-related phenomena and

[70] Clark, 2009; James Adams, "Virtual Defense," *Foreign Affairs* 80.3 (2001), 98-112.
[71] Der Derian, 2003, p.451.
[72] Dartnell, 2003.

developing the appropriate conceptual frame for analyzing cyberspace; the qualitatively transformative effect of cyberspace on international politics, particularly with respect to the empowerment of formerly marginalized groups; and the mutually embedded relationship between international politics and technological change.[73] Of these three, the last – the mutual embeddedness of technology and international politics – is at the highest analytic level, and ultimately provides the structure for the other two unifying themes.

The first unifying theme is the problem of defining the cyber domain and its related politically relevant phenomena. This theme can be further divided into two parts, one technical, and one political. On a technical level, there is the question of what technology or technological innovations ought to be the subject of the analysis. Is it the Internet, information technology, communication technology, or networks? Cyberspace, in fact, is strongly tied to each of these concepts, but it is not easy to say which offers the most appropriate analytic frame. Cyberspace is a network, a platform for new technological innovations such as social media, a conduit for communication, and a repository of information. It is unclear how it should be conceptually connected to other technologies such as telecommunications or computers. It is also unclear where the appropriate boundaries are between the technology of cyberspace, its related practices and technical standards, and the individual users that constitute networks. These are conceptual puzzles of the first order, and require greater attention from scholars and policy practitioners.

The second unifying theme is the transformative power of cyberspace, a view shared to some extent by nearly all of the 49 articles. Importantly, both the policy and academic articles we reviewed were significantly more conditional in their claims about cyberspace's ability to transform politics than earlier writings. The debates in the literature largely focus on which actors cyberspace will empower (or in some cases disempower), and what the ultimate effects those changes will be for human freedom and material well-being. In fact, the best of these articles move beyond the simple – and poorly specified – question of whether cyberspace is eroding the authority of states, and instead look at the ways in which different actors, both state and non-state, may be empowered in different ways and to different degrees under various conditions.

However, by situating these questions within narrowly defined issue areas, the authors mostly overlook important ways in which these issues are connected. For example, there is likely much to be gained from a shared dialogue among scholars studying global civil society or the affects of cyberspace on authoritarian regimes on the one hand, and scholars focused on cyber

[73] Manjikian, 2010; Geoffrey L. Herrera, "Technology and International Systems," *Millennium* 32.3 (2003), 559-593.

security on the other. All three areas involve the empowerment of relatively marginalized actors in ways that might challenge state authority. To cyber security specialists, this is typically treated as a security threat: potentially dangerous networks of non-state actors can threaten a state's security and the well-being of its citizens in novel ways. To those focused on GCS and authoritarian regimes, however, this same empowerment is typically treated as a positive outcome. Yet on a material level all of these phenomena are very much related. They are also, importantly, interconnected on a policy level. For example, efforts to improve attribution as a way to increase security in cyberspace could also help authoritarian regimes better control the Internet at the expense of their citizens. Much could be gained from an examination of the connections.

At the highest analytic level, all five issue areas are unified by the question of how international politics and technological change are interrelated. Herrera identifies this problem most directly, and – building on the earlier work of Buzan and Little – offers several important insights into how IR theory might begin address it.[74] Most importantly, Herrera notes that technology ought not be considered a purely material, apolitical, and exogenous influence on international relations, as is often implicit in the IR literature. The physical and technical aspects of technology necessarily lie within a broader "socio-technical system" that additionally incorporates procedures, standards, regulations, institutions, processes, operations, and operators.[75] A socio-technical system is at once both technical and material on the one hand, and political on the other. One cannot be separated from the other: the social world shapes and defines how technical systems arise, evolve, and spread. As many of the authors note, for example, today's Internet was designed according to a set of technical standards that were chosen for a particular political purpose. It could have been designed differently.[76] This design is continuously contested by a wide set of international actors. The outcome of this contestation, and in turn, the technical evolution of the Internet, will be determined according to the limits imposed on this system by the physical world, the interests of the various actors, and the political institutions that shape the contest. Similarly, cyberspace itself can impose limits on this political contest, and affect its outcome.

Framed in this way, the linkages across the different issue areas become more apparent. Specifically, both within each issue area and across them, political contestation and the architecture of cyberspace are interlinked. In the literature within each issue area, the authors

[74] Herrera, 2003; Barry Buzan and Richard Little, *International Systems in World History: Remaking the Study of International Relations*, New York: Oxford University Press, 2000.
[75] Herrera, 2003, p.561.
[76] See Lessig, 1999. Also, Deibert, 2003.

focus on the ways in which international politics at all levels of analysis – the structure of the international system, international institutions and regimes, the preferences and interests of state and non-state actors – influences the physical infrastructure, laws, regulations, and standards that define the technical system that constitutes cyberspace. Equally, these same constitutive layers that define the architecture of cyberspace – from material structures to syntactic code – by limiting and shaping the potential semantic content of cyberspace, determine its potential influence on international politics. Whether the debate is over cyberspace's potential to challenge autocratic regimes, present novel security threats, or empower various non-state actors or transnational groups, the outcome can only be understood by accounting for this duality between the technical and the political.

6. Conclusion

This paper reviewed the literature on cyber international relations of the previous decade. It began with a survey of all journal articles published on this topic from 26 major policy, scholarly IR, and political science journals between the years 2001-2010. This yielded 49 articles, mostly from policy journals. We then looked for common elements across these 49 articles in order to identify the basic contours of the state-of-the-art of the IR and policy communities' engagement with issues related to cyberspace. While two of the articles addressed theoretical issues related to cyberspace's impact on international relations as a whole, the remaining articles could usefully be sorted into five distinct issue areas: global civil society, the governance of cyberspace, economic development, the effects of cyberspace on authoritarian regimes, and cyberspace and security. The articles were additionally sorted according to the IR theoretical paradigm (realism, liberalism, or constructivism) that best informed the analysis.

We reviewed this literature in the context of each of the five issue areas. We then went on to identify three unifying themes that served as common elements throughout all of the articles: efforts to define the relevant subject of analysis; cyberspace's qualitatively transformative effects on international politics, particularly the empowerment of previously marginalized actors; and, at the highest analytic level, efforts to theoretically capture the mutually embedded relationship between technology and politics. We suggest that these themes could help usefully guide future research on cyberspace, and focus attention on ways that the debates within each of the five issue areas are interconnected, and could potentially be approached under a unified conceptual framework.

It is also useful to identify two encouraging developments in this literature that represent important progress in the scholarship on cyberspace. We suggest these developments be furthered by future studies. First, many of the 49 articles we reviewed exhibit a tendency toward greater empiricism than previous scholarship on cyberspace, which was often more speculative and argumentative. This is particularly the case with articles focused on authoritarian regimes and the governance of cyberspace. These efforts have led to greater theoretical nuance, and an improved understanding of cyber international relations, and further empirical work can shed more light on important questions.

Second, these articles typically demonstrate a greater awareness of the underlying technology of cyberspace than earlier work. This, too, should serve as a model for future scholarship. The contest for control of cyberspace, as well as contests for political influence and military power within cyberspace, cannot be fully understood without an accounting of what is possible on a technical level, and how the technical level constrains political behavior. Yet important questions remain in this regard. What, for example, are the technical limitations faced by states such as China in their efforts to manage and control the use of cyberspace within their territories? What types of cyber attacks are technically feasible, and what are the barriers and potential challenges to mounting an effective defense? How can policies best promote the diffusion of ICTs in ways that are most likely to promote global economic development, and do so more equitably? These are fundamental questions in the literature that cannot be addressed without a careful balance between technical understanding and rigorous social science.

7. Appendix

We searched 26 journals – both academic and policy-oriented – for articles that focused primarily or in large part on the effects of cyberspace and information technology on international relations, broadly construed. The search was limited to the decade from 2001-2010. The search was conducted in two steps. First, we searched the 26 journals for articles containing the key terms "ICTs," "information revolution," "information technology," or "cyber." This yielded an initial set of articles. Second, we looked for additional articles by reading through the abstracts of every article in the 26 journals from the 10-year period to identify articles the initial search may have overlooked. In the end, we discovered a total of 49 articles.

The following 26 journals were used for the search:

Academic Journals (18):

- *American Journal of Political Science*
- *American Political Science Review*
- *Annals of the American Academy of Political and Social Science*
- *British Journal of Political Science*
- *European Journal of International Relations*
- *International Interactions*
- *International Organization*
- *International Political Science Review*
- *International Security*
- *International Studies Quarterly*
- *Journal of Conflict Resolution*
- *Journal of Peace Research*
- *Journal of Strategic Studies*
- *Millennium*
- *Perspectives on Politics*
- *Political Science Quarterly*
- *Security Studies*
- *World Politics*

Policy Journals (8):

- *Current History*

- *Foreign Affairs*
- *Foreign Policy*
- *International Affairs*
- *Journal of International Affairs*
- *National Interest*
- *Survival*
- *Washington Quarterly*

We sought to include the most widely read, cited, and respected journals in the field. We purposely excluded journals with a regional emphasis (e.g., *Middle East Studies, European Union Politics*, or *Journal of Common Market Studies*), as well as journals that were primarily focused on law, legislation, or American politics (*e.g., American Politics Quarterly, Legislative Studies Quarterly,* or *American Journal of International Law*). Similarly, we excluded articles that discussed cyber-related issues strictly in the context of American politics (i.e., the effect of campaign websites on US electoral outcomes).

It is important to note that many of the academic journals searched published no articles on cyber politics between 2001-2010 (all of the policy journals published at least one article on the topic). If additional journals were included in the search, it would unlikely add to the number of articles we found (and in fact we confirmed this by searching a number of additional journals – e.g., *Journal of Politics*).

The 49 articles found in the search are as follows:

Adams, James, "Virtual Defense," *Foreign Affairs* 80.3 (2001), 98-112.

Alden, Christopher, "Let Them Eat Cyberspace: Africa, the G8 and the Digital Divide," *Millennium* 32.3 (2003), 457-476.

Baird, Zoë, "Governing the Internet: Engaging Governments, Business, and Nonprofits," *Foreign Affairs* 81.6 (2002), 15-20.

Barshefsky, Charlene, "Trade Policy for a Networked World," *Foreign Affairs* 80.2 (2001), 134-146.

Bleha, Thomas, "Down to the Wire," *Foreign Affairs* 84.3 (2005), 111-117.

Boas, Taylor C., "Weaving the Authoritarian Web," *Current History* 103.677 (2004), 438-443.

Bousquet, Antoine, "Chaoplexic Warfare or the Future of Military Organization," *International Affairs* 84.5 (2008), 915-929.

Brachman, Jarret, “Watching the Watchers,” *Foreign Policy* 182 (2010), 60-67.

Bremmer, Ian, “Democracy in Cyberspace,” *Foreign Affairs* 89.6 (2010), 86-92.

Clark, Wesley K., and Peter L. Levin, “Securing the Information Highway,” *Foreign Affairs*, 88.6 (2009), 2-9.

Clarke, Richard, “War from Cyberspace,” *National Interest* 104 (2009), 31-36.

Comor, Edward, “The Role of Communication in Global Civil Society: Forces, Processes, Prospects,” *International Studies Quarterly* 45.3 (2001), 389-408.

Conway, Maura, “What Is Cyberterrorism?” *Current History* 101.659 (2002), 436-442.

Corrales, Javier, and Frank Westhoff, “Information Technology Adoption and Political Regimes,” *International Studies Quarterly* 50.4 (2006), 911-933.

Cukier, Kenneth Neil, “Who Will Control the Internet,” *Foreign Affairs* 84.6 (2005), 7-13.

Dartnell, Michael, “Weapons of Mass Instruction: Web Activism and the Transformation of Global Security,” *Millennium* 32.3 (2003), 477-499.

Deibert, Ronald J., “Black Code: Censorship, Surveillance, and the Militarization of Cyberspace,” *Millennium* 32.3 (2003), 501-530.

Der Derian, James, “The Question of Information Technology in International Relations,” *Millennium* 32.3 (2003), 441-456.

Drezner, Daniel W., “The Global Governance of the Internet: Bringing the State Back In,” *Political Science Quarterly* 199.3 (2004), 477-498.

Eriksson, Johan, and Giampiero Giacomello, “The Information Revolution, Security, and International Relations: (IR)relevant Theory?” *International Political Science Review* 27.3 (2006), 221-244.

Farrell, Henry, “Constructing the International Foundations of E-Commerce – The EU-US Safe Harbor Agreement,” *International Organization* 57.2 (2003), 277-306.

Funabashi, Yoichi, “Asia’s Digital Challenge,” *Survival* 44.1 (2002), 135-144.

Goldman, Emily O., “Introduction: Information Resources and Military Performance,” *Journal of Strategic Studies* 27.2 (2004), 195-219.

Hachigian, Nina, “The Internet and Power in One-Party East Asian States,” *Washington Quarterly* 25.3 (2002), 41-58.

Hachigian, Nina, “China’s Cyber-Strategy,” *Foreign Affairs* 80.2 (2001), 118-133.

Hammond, Allen L., “Digitally Empowered Development,” *Foreign Affairs* 80.2 (2001), 96-106.

Hansen, Lene, and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53.4 (2009), 1155-1575.

Herrera, Geoffrey L., "Technology and International Systems," *Millennium* 32.3 (2003), 559-593.

Hughes, Christopher R., "Google and the Great Firewall," *Survival* 52.2 (2010), 19-26.

Hughes, Rex, "A Treaty for Cyberspace," *International Affairs* 86.2 (2010), 523-541.

Inkster, Nigel, "China in Cyberspace," *Survival* 52.4 (2010), 55-66.

Kalathil, Shanthi, "Dot.com for Dictators," *Foreign Policy* 135 (2003), 42-49.

Kohlmann, Evan F., "The Real Online Terrorist Threat," *Foreign Affairs* 85.5 (2006), 115-124.

Kudaisya, Gyanesh, "India's New Mantra: The Internet," *Current History* 100.645 (2001), 162-169.

Lessig, Lawrence, "The Internet Under Siege," *Foreign Policy* 127 (2001), 56-65.

Litan, Robert E., "The Internet Economy," *Foreign Policy* 123 (2001), 16-24.

Luttwak, Edward N., "Power Relations in the New Economy," *Survival* 44.2 (2002), 7-17.

Lynn, William J. III, "Defending a New Domain," *Foreign Affairs* 89.5 (2010), 97-108.

Manjikian, Mary MacEvoy, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly* 54.2 (2010), 381-401.

Mavhunga, Clapperton, "The Glass Fortress: Zimbabwe's Cyber-Guerilla Warfare," *Journal of International Affairs* 62.2 (2009), 159-172.

Mernissi, Fatema, "Digital Scheherazades in the Arab World," *Current History* 105.689 (2006), 121-126.

Morozov, Evgeny, "The Internet," *Foreign Policy* 179 (2010), 40-44.

Murphy, Emma C., "Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere," *International Studies Quarterly* 53.4 (2009), 1131-1153.

Newman, Abraham L., "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive," *International Organization* 62.1 (2008), 103-130.

Newmyer, Jacqueline, "The Revolution in Military Affairs with Chinese Characteristics," *Journal of Strategic Studies* 33.4 (2010), 483-504.

Persaud, Avinash, "The Knowledge Gap," *Foreign Affairs* 80.2 (2001), 107-117.

Rawnsley, Gary D., "Old Wine in New Bottles: China-Taiwan Computer-Based 'Information Warfare' and Propaganda," *International Affairs*, 81.5 (2005), 1061-1078.

Reynolds, Glenn Harlan, “The Blogs of War,” *National Interest* 75 (2004), 59-64.

Schmidt. Eric, and Jared Cohen, “The Digital Disruption: Connectivity and the Power of Diffusion,” *Foreign Affairs* 89.6 (2010), 75-86.