

Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet

Ronald J. Deibert
Rafal Rohozinski

Introduction

The spectacular rise and spread of NGOs and other civil society actors over the last two decades is attributable in part to the emergence and rapid spread of the Internet, which has made networking among like-minded individuals and groups possible on a global scale. Powerful, search technologies like Google, "me-media" tools such as blogs and myspaces, and communicative systems like Skype, make it easy to form virtual communities, mobilize support, and effect political change. Widespread access to inexpensive digital cameras, editing systems, and distributional channels allows anyone with desire and a few hundred dollars to become a potential Spielberg or Riefenstahl. Causes of all shapes and sizes seek and find moral and financial support on a global basis and consequently, local politics now plays itself out on a planetary scale.

But the technological explosion of global civil society has not emerged without unintended and even negative consequences, particularly for non-democratic and authoritarian states. The Internet has enabled new, nimble and distributed challenges to these regimes, manifest in vigorous opposition movements, mass protests, and in some cases even revolutionary changes to long-established political authority. Even among democratic states, the explosion of global civil society has presented serious challenges, though of a slightly different nature. Just as progressive and social justice groups have made use of the Internet to advance global norms, so too have a wide variety of resistance networks, militant groups, extremists, criminal organizations, and terrorists. Whereas once the promotion of new information and communication technologies (ICTs) was widely considered benign public policy, today states of all stripes have been pressed to find ways to limit and control them as a way to check their unintended and perceived negative public policy and national security consequences.

In this chapter we examine the ways in which states have targeted the Internet and have begun to assert their power in cyberspace as a means to control and limit global civil society. While “global civil society” is used often and widely today, there is no consensus as to its meaning or significance, particularly among social scientists.¹ Typically, the phrase is used to describe those collective associations that citizens have formed to influence public policy, whether domestic or international, such as Amnesty International, the World Wildlife Fund, or the Campaign to Ban Landmines. Most, though not all, ascribe to global civil society a positive association, and see networks of global civil society reigning in sovereign states while simultaneously pushing for rights, justice, and environmental rescue. Critics, on the other hand, often question the significance, ideological bias, and/or inherently democratic nature of global civil society.²

Although important, it is not the intent of our chapter to engage these conceptual debates around global civil society fully, other than to agree with John Keane when he says that “[l]ike all other vocabularies with a political edge, its meaning is neither self-evident nor automatically free of prejudice.”³ We take, therefore, as a definitional starting point that which the London School of Economics’ Civil Society Project has developed:

Civil society refers to the arena of uncoerced collective action around shared interests, purposes and values. In theory, its institutional forms are distinct from those of the state, family and market, though in practice, the boundaries between state, civil society, family and market are often complex, blurred and negotiated. Civil society commonly embraces a diversity of spaces, actors and institutional forms, varying in their degree of formality, autonomy and power. Civil societies are often populated by organisations such as registered charities, development non-governmental organisations, community groups, women's organisations, faith-based organisations, professional associations, trades unions, self-help groups, social movements, business associations, coalitions and advocacy groups.⁴

¹ See Marlies Glasius, Mary Kaldor and Helmut Anheier (eds.). *Global Civil Society 2006/7*. London: Sage, 2005.

² See, for example, David Rieff, "Civil society and the future of the nation-state: Two views." *The nation* 268.7 (1999):11-16

³ John Keane, *Global Civil Society?* Cambridge University Press, 2003, p. xv.

⁴ http://www.lse.ac.uk/collections/CCS/what_is_civil_society.htm

The LSE definition captures some of the most important elements of civil society, particularly the theoretical (though not always practical) distinction from the state and market, the recognition of collective associations around shared political purposes, and the diversity of its many different manifestations. Adding the term “global” to “civil society,” simply acknowledges those associations whose political activities take them beyond the confines of their own sovereign state.

Following Keane, it is important to note that, in spite of the “progressive” bias that influences the organizational examples given in the LSE definition, global civil society itself can comprise a wide range of contrary ideological positions. What is less than clear is whether the notion has normative content that excludes groups, like Al Qaeda for example, that employ violence to further their ends. Historically, civil society has been strongly associated with minimizing violence, furthering dialogue, and expanding spheres of peace. Whether and where “uncivil” society groups fit into this equation is a debate that falls outside of the purview of this chapter. And yet the issue is important for our consideration here, since it has been precisely those militant and extremist actors that have been both significant beneficiaries and employers of the Internet, and have in turn been identified by authorities as a putative justification for policies aimed at reigning in and securing cyberspace.

To address these issues, we breakdown “global civil society” into three spheres of agency: *civic networks*, *resistance networks*, and *dark nets*. Civic networks refer to progressive environmental, peace, and social justice movements that are most typically associated with the term “civil society.” “Resistance networks” include those more radical groups who are opposed to the status quo and whose activities can be considered illegal in some jurisdictions, making them the target of law enforcement and intelligence agencies. Groups advocating electronic civil disobedience, for example, are examples of resistance networks. A third form of agency is the least well known, and has tended to fall outside of the scope of most scholarship on global civil society. This category, which we call “dark nets,” includes armed social movements, criminal networks, and the underground economy linking diaspora communities worldwide. Although it is the latter

two forms of agency that are most often used as justifications for assertions of state power in cyberspace and are the primary targets of filtering, one of the main contentions of our chapter is that such targeting can have collateral impacts on civic networks as well. In other words, state filtering policies and practices are altering the dynamic ICT environment not just for resistance networks and dark nets, but for civic networks as well.

Global Civic Networks in the Internet Environment

The last several decades have witnessed a rapid expansion of global civic networks. The source of this expansion is undoubtedly complex, and reflects a variety of independent factors having to do with the end of the Cold War, the rise of a set of global values and political causes, the decline of civic participation in traditional structures of political participation, development initiatives, and no doubt others as well. However, there should be no doubt that this expansion has also been the result of the enabling role played by the new media environment, and in particular the growing use of the Internet by civic networks, beginning in the 1990s and carrying through the early part of the 21st century.

Global civic networks were among the earliest adopters of Internet technologies for their collective activities, and have been at the forefront of innovative uses of new media, like SMS, VOIP, and blogs. The medium's constitutive architecture -- distributed, decentralized, and relatively cheap and easy to employ -- "fits" with the organizational and political "logics" of global civic networks. As John Naughton observes, by facilitating access to published data, information, and knowledge, lowering the barrier to information dissemination and overcoming traditional gatekeepers in media, facilitating rapid communication and information sharing on a global scale, and helping to form "virtual communities" of people with shared interests, the Internet's material properties (how they were constituted in the 1990s) fueled a remarkable and unprecedented expansion of global civic networks.⁵ In short, global civic networks both contributed to and were empowered by the evolving environment of Internet communications

⁵ John Naughton, "Contested Space: The Internet and Global Civil Society," in Helmut Anheier Marlies Glasius and Mary Kaldor (eds.) *Global Civil Society*, (2001) London: Sage, 2001.

The origins of civic networks' use of the Internet can be traced back to the early 1980s when social change and activist groups began to employ computer networks as a mode of information-dissemination and organization.⁶ These early networks were largely "basement operations" with individuals donating their time and computing equipment to assist in the NGO activities of which they were a part. By the late 1980s, more formal links had been established among some of these networks in England (GreenNet) and the US (PeaceNet and EcoNet), and then later Sweden (NordNet), Canada (Web), Brazil (IBASE), Nicaragua (Nicarao) and Australia (Pegasus). In 1990, the networks jointly founded the Association for Progressive Communications (APC), a global umbrella network that still exists as a coordinating and advocacy NGO with a significant presence in Internet governance forums throughout the world today.

Perhaps the earliest demonstration of the Internet's facilitation of civic networks' organizational and networking capacities can be found at the 1992 UN Earth Summit in Rio de Janeiro. The Earth Summit was a unique event involving the extensive and official participation of numerous NGOs from around the world. Leading up to the summit, the UN and the APC established a network to facilitate communications among NGOs and disseminate official summit information. As O'Brien and Clement note: "[b]ackgrounders to the issues, draft policies, country briefings, and logistical bulletins were posted by the UN to a set of computer conferences shared internationally on all APC networks. This allowed several thousand civil society groups around the world to be kept informed at very little cost to the UN."⁷ The global, distributed nature of the NGO participation – in other words, the fact that groups not physically present at Rio nonetheless had a hand in participating – was instrumental in the formulation of the several 'alternative treaties' that were put forth from the parallel NGO summit, called 'the Global Forum', held simultaneously with the Earth Summit.

⁶ This section draws upon Ronald Deibert, "Deep probe: the evolution of network intelligence." *Intelligence and national security* 18.4 (2004):175-200.

⁷ Rory O'Brien and Andrew Clement, 'The Association for Progressive Communications and the Networking of Global Civil Society: APC at the 1992 Earth Summit', <www.apc.org/english/about/history/rio_92.htm>.

The type of civic networking demonstrated at the Earth Summit played itself out repeatedly throughout the 1990s, having a tangible impact on local, regional, and international rule-making forums. For example, according to scholarly observations and those of the participants themselves, the Internet played a critical role in the International Campaign to Ban Landmines (ICBL).⁸ Although the campaign did not employ computer networks in any substantial sense until about 1995, from that point onwards the Internet was vital to collecting and disseminating information and forming strategy in the ICBL across its membership in more than 70 countries. The networks were, according to participants, crucial in lowering organizational costs and integrating into decision-making structures members from poorer, developing countries. More importantly, it dramatically augmented the intellectual capacity of the ICBL member NGOs, who were able to bring analytically and empirically informed analyses to the table when meeting with states on the landmines issue. It also knit the diverse participants together into a relatively coherent unit, particularly with regard to the ICBL strategy.⁹ As some prominent leaders of the ICBL noted, the ‘the ease and speed of communication within the ICBL provided by e-mail clearly had a great impact on the ability of civil society organizations from diverse cultures to exchange information and develop integrated political strategies.’”

Although perhaps the most prominent, the ICBL was not the only instance of global civic networks being empowered by the Internet, nor was the model it supplied – working within legitimate processes of political participation, albeit in very novel, challenging ways – generalized elsewhere. Indeed, the 1990s also saw the Internet employed by a growing number of “resistance networks” – anarchists, anti-globalization activists, environmental justice, and political opposition movements.¹⁰ In the landmark case of the opposition to the Multilateral Agreement on Investment (MAI) negotiations, for example, civic networks organized a multi-pronged campaign of resistance and protest across numerous countries and involving hundreds of loosely linked autonomous groups and

⁸ See Richard Price, "Reversing the gun sights: transnational civil society targets land mines." *International organization* 52.3 (1998):613-644.

⁹ Kenneth Rutherford, "Internet Activism: NGOs and the Mine Ban Treaty," *The International Journal on Grey Literature*, vol. 1, no. 3, pp. 99 - 106, 2000

¹⁰ Porta, Donatelladella. "Global-net for global movements? A network of networks for a movement of movements." *Journal of public policy* 25.1 (2005):165-190.

individuals.¹¹ Their activities broadsided state policymakers involved in the negotiation process and by some accounts led to the eventual cessation of the MAI negotiations. The MAI campaign, in turn, morphed into a broader virtual platform of civic networking around anti-globalization, most notably characterized by the street demonstrations of Seattle, Quebec City, Genoa, and elsewhere.¹² Today, this broadly distributed network of individuals concerned with economic and social justice continues to bristle with Internet-based political activity, although street demonstrations have been mitigated in the post 9/11 security environment.

Another celebrated networking campaign of resistance occurred in support of the Zapatista liberation movement.¹³ The Zapatistas are a revolutionary national liberation group based in the Mexican province in Chiapas. Beginning in the early 1980s, the Zapatistas formed an armed independence movement that attracted an international web of support among anti-globalization and other activists. "Hacktivists" in support of the Zapatista cause developed distributed denial of service tools that were employed as mechanisms of protest against the Mexican government, and brought forth one of the first instances of online civil disobedience.¹⁴ The methods of the Zapatista electronic civil disobedience campaign were, in turn, duplicated in other similar acts directed against perceived injustice and corporate power throughout the 1990s, with ambiguous but

¹¹ See Ronald J. Deibert, "International Plug 'n Play? Citizen Activism, the Internet, and Global Public Policy." *International studies perspectives* 1.3 (2000):255-272.

¹² A recent comprehensive survey of participants at five globalization protests found that 80% of those surveyed found out about the protests via the Internet. See Dana Fisher, "How Do Organizations Matter? Mobilization and Support for Participants at Five Globalization Protests." *Social problems* 52.1 (2005):102-121.

¹³ For a nuanced analysis that compares that MAI and Zapatista cases with a discussion of the role of the Internet, see Josee Johnston, "Solidarity in the Age of Globalization: Lessons from the Anti-MAI and Zapatista Struggles." *Theory and society* 32.1 (2003):39-91; Harry Cleaver, Jr., "The Zapatista effect: the Internet and the rise of an alternative political fabric." *Journal of international affairs* 51.2 (1998):621-640.

¹⁴ Hacktivism combines the notion of "hacking" in its original positive sense, as someone interested in exploring technology, with social and political activism. There is

always controversial results¹⁵. The rise of resistance networks, in turn, drew the attention of state intelligence and law enforcement worldwide.¹⁶

Over the several decades, the Internet has provided a technological foundation and material support for the massive flourishing of advocacy, rights, and justice movements worldwide. These movements have pressed upon traditional structures of political participation in ways that many believe are contributing to a fundamental change in world order. At the very least, these network-enabled transnational social movements have altered the operational environment for states, international organizations, and corporations who have been forced to address civil society stakeholders in all policy arenas. In some cases, such as the so-called coloured revolutions of the former Soviet Union, civic and resistance networks have actually been responsible for the overthrow of long-established authority structures. Without a doubt, the Internet has been indispensable to these activities.

Internet Protection and Hacktivism

The importance of the Internet as a material foundation and explosive engine for civic and resistance networks has not gone unnoticed. Within a dynamic, technologically savvy sector of civil society, a transnational social movement has emerged around what might be called "Internet protection" – that is, collective securitization whose aim is to uphold the Internet as a forum of free expression and access to information through advocacy, training, policy development, and technological research and development.¹⁷ Though coming at the problem from different backgrounds, Internet protection advocates are beginning to network around a shared agenda of communications security and privacy, freedom of expression, equal access, the protection of an open public domain of

¹⁵ Jenny Pickerill, "Radical Politics on the Net." *Parliamentary affairs* 59.2 (2006):266-282; and Brian Huschle "Cyber Disobedience: When Is Hacktivism Civil Disobedience?." *The International journal of applied philosophy* 16.1 (2002):69-83.

¹⁶ See for example Canadian Security and Intelligence Services, Report No. 2000/08: Anti-Globalization - A Spreading Phenomenon (August 2006); <http://www.csis-scrs.gc.ca/en/publications/perspectives/200008.asp>

¹⁷ For an overview, see Ronald Deibert, "Black code: Censorship, surveillance, and the militarisation of cyberspace." *Millennium* 32.3 (2003):501-530.

knowledge, and the preservation of cultural diversity. The participants in this social movement include local, regional, and global non-governmental organizations, activists, and policy networks, including major international rights organizations, such as Human Rights Watch and Amnesty International, as well as the OpenNet Initiative (and its partner institutions) itself.

Critical to the constitution of this social movement has been the support provided by major non-profit research and advocacy foundations, such as the Ford Foundation, Markle Foundation, Open Society Institute, the MacArthur Foundation, and others. The support of these non-profit foundations has included not only financial resources but also networking opportunities, venues for collaboration, and research and development coordination. To be sure, this type of support has had an important impact. However, the resources provided by these donor agencies do not rival the collective financial capacities that can be marshaled by states. Nor do they always come without unintended consequences. Scholars have noticed funding of this sort can promote the emergence of patron-client ties between donors and recipients, rather than horizontal links among civic networks.¹⁸ They may also create a hostile environment for civic networks due to the impression of outside ‘interference’ and ‘meddling’ – particularly if the NGOs are perceived as a thin vehicle for one state’s foreign policy within the jurisdiction of another state. One recent study found that nineteen countries, concentrated mostly in Africa, the Middle East, and the former CIS, have enacted or proposed laws over the past five years that restrict the activities of civil society.¹⁹

One area where the asymmetric capacities of civic networks may be most tangibly felt is in building code, software, and other tools explicitly designed with an Internet protection paradigm in mind. From the outset, the Internet’s character has been shaped not only by

¹⁸ See Sarah Henderson "Selling civil society: Western aid and the nongovernmental organization sector in Russia." *Comparative political studies* 35.2 (2002):139-168.

¹⁹ See “Recent Laws and Legislative Proposals to Restrict Civil Society and Civil Society Organizations,” *International Journal for Not-for-Profit Law*, 8.4 (August 2006), http://www.icnl.org/knowledge/ijnl/vol8iss4/art_1.htm; and Peter Ackerman, "The Right to Rise Up: People Power and the Virtues of Civic Disruption." *The Fletcher forum of world affairs* 30.2 (2006)

states and corporations but also by the distributed base of users themselves. Skilled computer geeks, hacktivists, and other individuals have been responsible for some of the most innovative Internet technologies, from open source/free software platforms to P2P networks and encryption systems. Although “Internet protection” technologies go back decades, in recent years there has been a more concerted and organized research and development effort, working in tandem with the policy/governance/awareness efforts described above. These efforts include tools to support anonymous communications online, such as the Tor system; tools that circumvent Internet censorship, such as psiphon or peacefire; and tools that support privacy online, such as PGP, scatterchat, and others. These tools are, in turn, increasingly localized to different country contexts, distributed via non-governmental organizations and human rights networks, and built into training and advocacy workshops organized by the Internet protection civic networks described above.²⁰ As we show below, however, state filtering efforts have deliberately targeted these Internet protection tools as a way to control and limit networking activities of civic and resistance networks.

Towards Uncivil Society Networks and the Rise of “Darknets”

The bulk of scholarship reflecting on the rise and spread of civic networks has tended to focus on those elements of civil society that are explicitly non-violent in nature, and liberal in outlook and spirit. These characteristics reflect, in large part, the “peace dividend” of the immediate post-Cold War era that provided a hiatus from decades of inter-state conflict, and where the bulk of visible or public sphere transnational networks tended to centre on issues of social justice, environment, and universal rights and values. Of these elements, even the most extreme forms, such as the anti-corporate resistance networks described above, were still largely characterized by non-violent methods, and centered in and around Western industrialized activist circles.

However, outside the focus of mainstream scholarship, other social movements and resistance groups began to discover and appropriate the Internet, recognizing the

²⁰ See, for example, the NGO-in-a-Box Security Edition, found here: <http://ngoinabox.org/boxes/security/>

unprecedented capabilities it offered for organization, communication, mobilization and action. These actors, ranging from militants, insurgents, criminal elements and diaspora and migrant communities, expanded exponentially, aided by the largely unfettered and unregulated growth of the Internet throughout the developed and developing world. Much less was said or known about these networks - whose activities and aims were facilitated by the Internet in much the same way as were global civic and resistance networks, but whose aims were often criminal, covert, and sometimes violent. These “dark nets” can be roughly divided into three categories.

The first and most well known of the dark nets are the armed social movements. Armed social movements can represent a multiplicity of local causes, but their ability to share tactics, contacts, and at times, drink from the same ideological well make them appear as a unified global network. In the post 9-11 era, Al Qaeda and the Jihad movements represent perhaps the most visible manifestation of this kind of armed social movement dark net. However, they are by no means the first and only networks of this kind. In the 1990’s, the old paradigm of wars between nation states was displaced by a new form of warfare – what Mary Kaldor calls “new wars.” What sets “new wars” apart from the previous generation of Cold War era armed struggles is the participants’ ability to leverage the emerging global networked economy – in particular the illicit global economy -- to become self reliant in the arms, money and political support required to pursue armed struggle against state and non-state actors. Many of the “new wars” that occurred during the 1990’s, particularly those in the developing world where first world militaries were neither involved as supporters or peacekeepers, were fought essentially as transnational civil wars where armed formations pursued both guerilla and conventional warfare against government and rival groups. In conflicts that included Sri Lanka, Somalia, former Yugoslavia, West Africa and Chechnya, “new wars” demonstrated that globalization had made armed social movements capable of challenging and at times defeating state actors without the need of state-based patrons or backers.

More importantly, this new generation of armed social actors also increasingly embraced the Internet, recognizing the capacity afforded to “effect” both their supporters and

opponents. Significantly, it was these groups, rather than First World militaries, that were the first to leverage the Internet as means to wage information operations that redefined the main field of battle away from the military and towards the political sphere.²¹ Beginning with the first Chechen war, the video taping of attacks on the Russian military became more important than the military significance of the attacks themselves. When shown to supporters, as well as the Russian public (via the rebroadcast in Russian television, and later on the Internet) their shock value was enough to convey the impression that the Russian military was being defeated. Similar tactics were adopted and further refined by Hezbollah in its resistance against Israeli occupation of Southern Lebanon prior to their withdrawal in 2001. Hezbollah produced reports in the form of music videos that were both broadcast across Hezbollah's terrestrial TV station, (al Manar) as well as made available for download from websites the movement had established as part of its strategic communications and information warfare strategy.

These video shorts proved highly effective, and have since undergone several significant evolutions, paralleling the spread and popularity of such on-line resources as YouTube and Indymedia that are used regularly by global civic networks and resistance groups. They are now one of the key instruments used by these movements to attract interest in their causes and are a significant feature of the more than 4,500 active Jihad websites, chat rooms, and forums. As the resources necessary for producing multimedia technologies continue to fall, and access to inexpensive digital cameras and editing software increases, the threshold and number of video and other multimedia products in circulation has grown exponentially. Meanwhile, the age of the producers has sharply declined. During the early months of the second Intifada, for example, several of the more compelling Power Point slides circulating on the Internet depicting the brutality of the Israeli reoccupation of the West bank were produced by a 14 year old living in a refugee camp in Lebanon.²²

²¹ See Rafal Rohozinski, (2003). *Bullets to Bytes: Reflections on ICT and "Local Conflict". Bombs and Bandwidth : The Emerging Relationship Between IT and Security*. R. Latham. New York, New Press: 288 p. ; 24cm.

²² *ibid.*

In addition to changing the nature of the conflicts, the video clips have also served to change the nature of the movements themselves. They have eliminated the need for strict command and control, especially for smaller and more marginal movements who can now claim legitimacy for their actions by “virtually” piggy backing on the perceived effectiveness and success of others. They also give the impression of a unity and scale among groups that in reality, simply does not exist. As a result, much as the discourse of human rights and other universal values provides a moral centre that binds many of the civic networks together, the depictions of resistance, wrapped in religious undertones, provide a means for smaller, more local struggles to identify with and benefit from a broader ideological pool. When networked together in this way, this ideological pool serves to demonstrate that resistance is not only possible, but also positively effective.

The Internet is only one of the tools used by armed social movements in the pursuit of their cause, but it is certainly the one that, because of its largely unregulated character and relative freedom of access, causes the greatest concern for states under threat from such actors. It is seen, at least in part, as the sea in which global militants find sanctuary of the kind that Mao postulated in his classical treatise on People’s War. The difficulty, then as it is now, is how to effectively separate the insurgents from the people, or armed social movements from the Internet, in a manner that does not destroy the latter.

Transnational criminal networks are a second form of dark nets. These actors, who can be large or small, local or transnational, exploit the relative anonymity offered by the Internet as well as the absence of harmonized national laws defining cybercrime, to circumvent or avoid prosecution. Much of the activities of these actors involve old crimes, such as fraud and theft, which have been adapted to the new possibilities offered by the emergence of the E-economy. In other cases jurisdictions with poorly functioning or non-existent laws are used to hide otherwise criminal activities, such as distribution of child pornography, out of the reach of authorities in jurisdictions where such activities are clearly criminalized.

Globally, the incidences of reported cybercrime is increasing in both developed and developing economies. In Russia, for example, acknowledged as a source of some of the most imaginative forms of cybercrime, incidences reportedly grew by almost 300% between 2003 and 2006.²³ Yet accurate comparative statistics makes measuring global cybercrime difficult. For example, in the US -- an economy in which losses caused by cybercrime were cited by one Treasury Board official as exceeding **\$105 billion** -- only in 2006 did the Department of Justice belatedly begin the process of establishing a baseline for measuring cybercrime. In part, the absence of reliable statistics reflects the difficulty faced by local police and justice institutions who have to police activities that may not be defined or considered criminal in their jurisdiction (or against which they have few tools). Quite simply the globalization of criminality has far exceeded the capacity of states to define or harmonize an effective global mechanism to contain or police it. Consequently, despite notable efforts, such as the Council of Europe's Convention on Cybercrime, criminal activity and networks continue to multiply and expand into new regions and activities. Russian hackers are implicated with identity theft and credit card fraud in the US and Europe. Nigerian gangs have become omnipresent in a variety of scams and wire fraud, while Chinese and Israeli gangs preside over a global distribution network of pirated DVDs and software. The result of this criminal use of the Internet is that in local jurisdictions the first real awareness of Internet use in their local community comes accompanied with a request for prosecution. In one particularly egregious case that occurred in the late 1990s, the entire .tj domain was registered by a US based entity that used it to host child pornography. Local Tajik authorities were forced to pursue legal action to claim the domain, a fact that did little to portray the social benefits of an unregulated Internet to the morally conservative Tajik society.

A third dark net, and perhaps the hardest to define, consists of the multitude of private social networks that exist among migrant and diaspora communities, and which play an important function in supporting the economic and social ties that bind these communities to their kin and communities of origin. These "private interest" networks

²³ Russian federal law captures cyber crime under 111 separate statutes ranging from "unlawful access to computer information," and, "creation, use and distribution of malware," through to fraud and Illegal distribution of porn materials and items containing child porn.

are the least well known and analyzed, as penetrating them requires gaining the trust of the communities. Often these networks serve specific social functions, circumventing cultural or social taboos, or serving highly specific economic interests. As a consequence, they are often deliberately “closed,” and thus may even be denied or downplayed by the communities they serve.²⁴

These networks are, nonetheless, among the most active of the dark nets, and hence tend to get labeled with the same negative image as the armed social movement or criminal networks because they appear to support or even appropriate the same means used by the latter. For example, diaspora communities are often used to facilitate the movement of funds outside of the formal banking system, especially among migrant communities in the Gulf, South Asia and the Horn of Africa. So called Hawala networks, which in some countries carry a volume of funds equal to or larger than the official banking system, have fallen under suspicion as having been the source of funds ending up in the hands of local militant groups.²⁵ While this may be the case, both the number of Hawala transfers used by terrorist groups as well as the amounts needed for carrying out terrorist attacks are relatively small given the overall volume of Hawala transfers, and could have just as easily been hidden in regular banking or other more on-line transactions (e.g., PayPal).

Although not often analyzed together by scholars with the civic networks described above, the “uncivil” dark nets described here are as much a part of global civil society as are the former. Following the LSE definition employed earlier in our chapter, they constitute an arena of uncoerced collective action around shared interests, purposes and values. Their institutional forms are distinct from those of the state, family and market, though in practice, the boundaries between them are often complex, blurred and negotiated. What differentiates them from the civic networks is, of course, their perceived illegitimacy, making them the target of state security and law enforcement. In

²⁴ See Rafal Rohozinski, “How the Internet did not transform Russia.” *Current History Intelligence and national security* 18.4 (2004):175-200.

²⁵ See Rafal Rohozinski, “Secret Agents” and “Undercover Brothers”: The Hidden Information Revolution in the Arab World. (unpublished paper) http://www.ssrc.org/programs/itic/publications/ITST_materials/rohozinskibrief3_4.pdf

the following section we turn to the ways in which states have attempted to control and contain the challenges presented by civic networks, resistance networks and dark nets through Internet filtering, surveillance and control.

Assertions of State Power over Civic, Resistance, and Dark Nets in Cyberspace

As the other chapters and the country summaries of this volume make clear, the problem of Internet filtering and censorship is growing in scope, scale, and sophistication worldwide. What began as a practice confined to a small handful of non-democratic regimes has expanded to countries throughout every region of the globe, and includes non-democratic, transition, and democratic countries. How much of this filtering be attributed to attempts by states to control the challenges presented by both civic, resistance and dark networks? Here there is no plain answer, as the motivations for Internet filtering and censorship vary among states, and are often shrouded in secrecy and deceit. We can, however, identify several areas from our research where states are asserting control over the Internet as a means to limit the threats posed by the varied elements of global civil society. As we will show, even in those cases where the targets are clearly “dark nets,” there can be collateral impacts on the communications environment for civic networks.

Filtering Data Analysis

The results of the ONI’s testing as presented in this volume, present a wide array of categories targeted for filtering, in both English and local languages, across numerous countries and several regions. In this section, we highlight several categories of filtering where it can be imputed that states are deliberately targeting content or communication channels of civic, resistance and/or dark nets. We also note those instances of collateral filtering, where filtering of content or communications channels of dark and resistance networks impact upon civic networks as well.

Human Rights

One area of obvious importance to civic networks, both as a normative underpinning and a source of content produced by those networks, is human rights. As many civic networks are critical of states' records in the areas of human rights, many of the affected states have been targeting the sources of that content for filtering. Pakistan, Myanmar, India, Iran, Uzbekistan, Algeria, Ethiopia, Tunisia, Vietnam, China, Syria, Saudi Arabia and Thailand all block access to at least one website categorized by the ONI as "Human Rights." Among those countries, China, Vietnam, Tunisia, Uzbekistan, Pakistan, Myanmar and Iran are all pervasive filterers of human rights categorized content. Among the 48 sites that the Chinese government blocks in this category are the websites of Chinese Rights Defenders, Human Rights in China, the Asian Human Rights Commission, Amnesty International, Human Rights Watch, and Olympic Watch – essentially the full panoply of international and country-specific organizations with an interest in China's human rights record. Iran's coverage is similar to China's, although it also singles out prominent individuals for filtering, such as the infamous blogger, Hoder. Vietnam tends to focus on country-specific human rights NGOs operating in the Vietnamese language, Tunisia strikes a balance between "international" and "country-specific," as does Myanmar, while Uzbekistan targets mostly independent media, TV, and radio websites related to Uzbek human rights. For its part, Pakistan targets almost exclusively those human rights sites related to the Balochistan liberation movement. Furthermore, 8 states (Algeria, Ethiopia, Iran, Myanmar, Saudi Arabia, Sudan, Tunisia, Yemen) block at least one women's rights site on the ONI's testing lists, with one state, Iran, blocking the highest amount (17 of 70 tested). Additionally, 7 states (China, Ethiopia, Iran, Myanmar, Pakistan, Syria and Tunisia) all have at least one blocked in the category "minority rights," with China blocking all sites tested related to Tibet. Overall, the ONI's testing results show a concerted effort among many states to target human rights related content.

Independent Media and Free Expression

In many states, control over major media, like television and radio, is seen as important lever of power that can be tightly regulated and controlled leaving independent media as

one of the only sources of news and free expression for civic and resistance networks. A total of 17 states (Algeria, Bahrain, China, Ethiopia, Iran, Kyrgyzstan, Myanmar, Oman, Pakistan, Saudi Arabia, Sudan, Syria, Thailand, Tunisia, Uzbekistan, Vietnam, and Yemen) blocked at least one website categorized by the ONI as a content provider in the “Independent” Media category. Not surprisingly, there is a strong degree of overlap among those countries that block a high amount of human rights content and independent media content. Other notable instances of filtering of independent media occurred in countries during election periods, a point that will be discussed in more depth later on. 19 states (Algeria, Azerbaijan, Bahrain, China, Ethiopia, India, Iran, Kyrgyzstan, Myanmar, Oman, Pakistan, Saudi Arabia, Sudan, Syria, Thailand, Tunisia, Uzbekistan, Vietnam, and Yemen) blocked at least one site in the “free expression” category. Of those countries, Syria, China, Iran, Myanmar, Tunisia, and Vietnam block a high amount with Uzbekistan, Saudi Arabia, and Ethiopia blocking a moderate amount.

Internet protection and hacktivist tools

As mentioned earlier, civic and resistance networks have been actively developing software tools to protect and preserve freedom of speech and access to information online. The ONI ran tests to capture filtering targeted against these tools and found several significant country cases. China, Iran, Yemen, Sudan, Tunisia, Oman, and Saudi Arabia all block access to a high amount of URL's in the ONI's anonymizers & circumvention category. Uzbekistan blocks access to a relatively few, though significant number of anonymizer and proxy sties, as does Vietnam, Myanmar, and Syria. China blocks access not only to know circumvention sites, but sites that are known to provide information and tutorials about censorship circumvention. In the cases of other states, we conclude that some of this filtering is the result of the use of categories built into commercial filtering products used by these regimes. Sudan, Tunisia, Oman, and Saudi Arabia all use *SmartFilter*, which has an “Anonymizer” blocking category, while Yemen uses *Websense*, which has a “Proxy Avoidance” category. The filtering system used in Iran varies between ISPs and the specific product used is currently unknown. The targeting of anonymizers and circumvention tools used by civil society (civic, resistance,

and dark) suggests states are moving to counter the Internet protection efforts described above.

Tools of Communication

States have also blocked some of the major media of communication used by all spheres of civil society, including free email services and VoIP. In both cases, the filtering may be motivated by concerns over economic protection and monopoly preservation.

However, the collateral impact of the filtering is clearly felt by civil society networks that rely on such low costs means of communicating. Iran, Syrian, Yemen, and Myanmar all block access to a small but significant number of popular free email services. The United Arab Emirates (UAE) highly targets VOIP websites for filtering. UAE and Myanmar both block the popular VOIP tool www.skype.com and the UAE is joined by Syria in blocking www.dialpad.com and www.icconnecthere.com. Vietnam also blocks 2 sites in the ONI's VOIP category (evoiz and mediarling). Jordan blocked access to skype.com in 2006, citing national security concerns.

Hacking and WAREZ

Both resistance and dark nets (and to a lesser degree civic networks) can occasionally make use of websites found in the ONI's "hacking" and "WAREZ." For civic and resistance networks, some of these websites and resources provides tools, information, and strategies associated with hacktivism that can be useful to their networking, social mobilization, and political activism. For darknets, the websites of most interest are found in the WAREZ category and relate to illicit trade in pirated software and other material, although other dark nets make use of hacker tools as well. Iran, Yemen, United Arab Emirates, Saudi Arabia, Sudan, and China all block a high amount of ONI's WAREZ and Hacking categories, Tunisia blocks a somewhat lesser amount, while South Korea, Oman, Myanmar and Azerbaijan all target a minimal amount. Hacktivist groups, such as cultdeadcow.com (Algeria, China, Iran, Yemen), hacktivism.com (Tunisia and Yemen), nmrc.org (Algeria & Yemen), and thehacktivist.com (Iran & Yemen) are also caught in

the Hacking and WAREZ net and blocked in some of these countries. In ONI's 2005 tests, Yemen did not block any sites in our Hacking category. Now, one of the two ISP's tested, YNET, blocked access to 20 of 46 URLs we tested, most likely as a result of enabling the "Hacking" category on their Websense filtering system.

Militancy, Extremists, Armed Social Movements

Not surprisingly, many states justify their filtering practices as a way to target those members of dark nets that are armed social movements – that is, either militants, extremists, or armed separatist movements. 11 states, (Algeria, Azerbaijan, China, Ethiopia, Iran, Myanmar, Pakistan, Saudi Arabia, Syria, Tunisia and Yemen) all block at least one URL that the ONI categorized as a content provider in the "militancy, military group" category. Most of these websites relate to country specific security issues involving extremist groups or organizations advocating or being associated with violent change. As mentioned earlier, Pakistan blocks all websites related to the Balochistan insurgency.

The results of the ONI's testing strongly suggest a concerted effort among some states to target the content and communicative infrastructure of global civil society, including civic, resistance and darknets. Perhaps not surprisingly, most of the states that do so tend to be democratically challenged or non-democratic regimes, as these states face the stiffest challenges from these networks. In the following two sections, we turn to a more detailed examination of evidence from blogging and blocking efforts around key periods, such as elections.

Securing and Filtering Blogs²⁶

As tools of individual self-expression, blogs and blogging have important implications for civic networks, resistance networks, and even some dark nets. First, blogs can provide a source of independent and alternative news from traditional mainstream media. This is especially important in light of the fact that many countries in the world strictly

²⁶ Thanks to Julian Wolfson for assistance in the research for this section.

control traditional print and broadcast media, but it is also relevant to areas of the world where such controls are absent. In the United States, for example, the relationship between blogging and traditional forms of journalism has been prominently debated. In non-democratic and repressive countries, blogging can provide a window onto events and issues not covered by the mainstream or government-controlled media. Not surprisingly, many dissidents and activists have been attracted to blogging.

Second, blogging can provide an easy tool for individuals and organizations to disseminate information to a global constituency, i.e., for coordination and organizational purposes. In this respect, blogging does not differ fundamentally from traditional websites, which also provide the means to publicize information worldwide. Rather, what makes blogs unique is the ease of posting and syndication. Individuals who have no expertise in computer programming and html editing can very easily update their blogs, opening up web publication to a wide audience. Additionally, those living in regions of the world with low bandwidth connections to the Internet can more easily edit blogs than websites. Indeed, new technologies allow people to update their blogs using only cell phone text messages.

Third, blogs can provide NGOs and other groups with a new means to attract support for their organizations, particularly in the area of fundraising and recruiting. Civil society networks continually struggle to get their message out, and often have a difficult time penetrating the mainstream media, particularly about their successes. Potential donors and supporters can acquire, through the window of blogging, a sense of immediacy and detailed understanding of the nature and operations of collective activities direct from the source and the field.

However, blogs and blogging do not come without potential negative implications. Because blogging can threaten state control of media, and have become a popular tool of dissidents, militants, and activists, bloggers can find themselves the object of threats, physical violence, and arrests. As will be shown below, blogging has become a focus of attention by authorities in non-democratic and repressive regimes, with many bloggers

being silenced through arrest or intimidation. Additionally, states that filter Internet communications are beginning to target blogs with increasingly refined forms of censorship, including parsing through entries and removing objectionable keywords and phrases.

The intention of the research in this section is to examine the global effort to silence bloggers. We assess where bloggers are targeted by authorities, for what reasons, and using what mechanisms of silencing (e.g., arrest). As part of the collection of information from websites, news articles, and blogs, a number of assumptions have emerged that inform our analysis.²⁷ First, the actions of states create fundamental challenges to a thorough and quantifiable examination into the issue of silencing bloggers. This is largely due to states' unwillingness to publicize the actions taken against bloggers.²⁸ Second, because bloggers at risk tend to be located in non-democratic regimes, accused bloggers are often burdened by limited or no access to legitimate justice systems. Those detained may be held without charge for an indefinite period of time, without knowledge of the charges against them or access to legal representation. When faced with a trial, it is often illegitimate. Third, repressive regimes, such as China and Iran, are the primary perpetrators targeting bloggers. Bloggers in these two states are the

²⁷ The silence associated with the arrests of bloggers provides little hard data or resources available to quantify the occurrences of attacks on bloggers by hostile state actors. To undertake this survey two methods have been used: Google searches and use of the 'Lexis Nexis' legal, news, public records and business information database. Google searches used the following keywords: "blogger arrest", "blogger arrested", "cyber dissidents", "blogger detention", "blogger trial", "blogger detained", "blogger crime", "weblog and arrest", "weblog and arrested", "web log and trial". The Google search provided a broad spectrum of information only some of which was useful for the research. To separate the data into relevant categories, an assessment was made as to whether the action taken against bloggers was associated with their online activities. Crimes that were not associated with their blogging directly were not included in the analysis. For example, the blogger arrested for robbing a bank was excluded from the data set. For searches on the 'Lexis Nexis' database a similar method was undertaken. The following keywords were used: "blogger arrest", "blogger arrested", "cyber dissidents", "blogger detention", "blogger trial", "blogger detained", "blogger crime", "weblog and arrest", "weblog and arrested", "web log and trial". The research for this section was carried out in October 2005.

²⁸ See Dean 2004; Kalathil 2003; RSF 2005; IFEX 2005

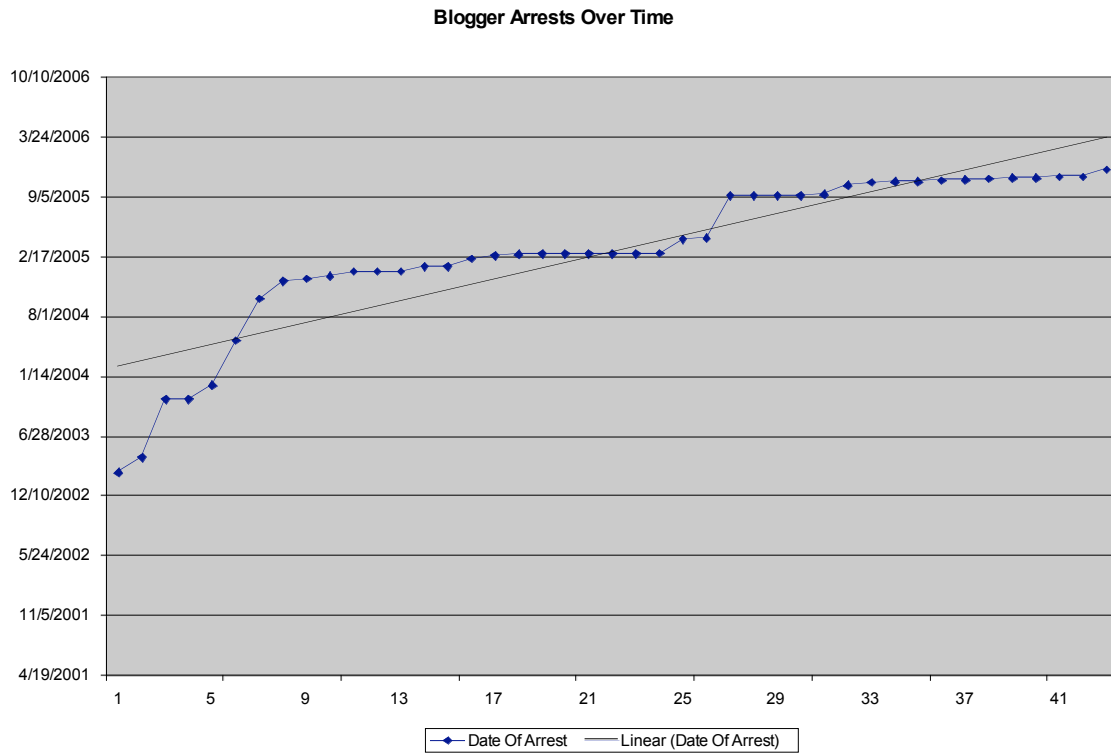
least likely to be informed of the charges against them, and the most likely to face lengthy detention, although other countries are following suit.

The targeting of bloggers by authorities has increased on an annual basis over the last five years. We examined any cases of blogger arrests dating back prior to 1995, although as blogging is a new and growing medium, we assume that few cases would have arisen before 2002. The first case of a blogger facing charges by a state was an Egyptian blogger in 2003²⁹. The blogger was charged with violating Egypt's religious laws. He was sentenced for an undisclosed prison term, and remains incarcerated. From that time onwards, the number of bloggers arrested has increased on a yearly basis, with a jump in the number of arrests in 2004 and continuing an upward trend through to 2006 (**Please see Figure 1**)

The cause for the increase in arrests of bloggers is likely due to the fact that blogging is an increasingly popular medium, particularly for dissidents and activists. As the rate of blogging has increased so has the threat by blogs to state authorities. Most non-democratic regimes place stringent controls on media and freedom of expression, including the Internet. Over the past 3 years, bloggers and the practice of blogging have created an alternative, independent source of news and media. Quite apart from the content of what is published by bloggers (which itself can be threatening), the very independence of blogging undermines state control over media. Hence it is not surprising to find an increasing amount of attention paid to bloggers and blogging by non-democratic and repressive regimes.

²⁹ Please see The Arabist of November 3rd, 2005 at <http://arabist.net/archives/2005/11/03/>

Figure 1



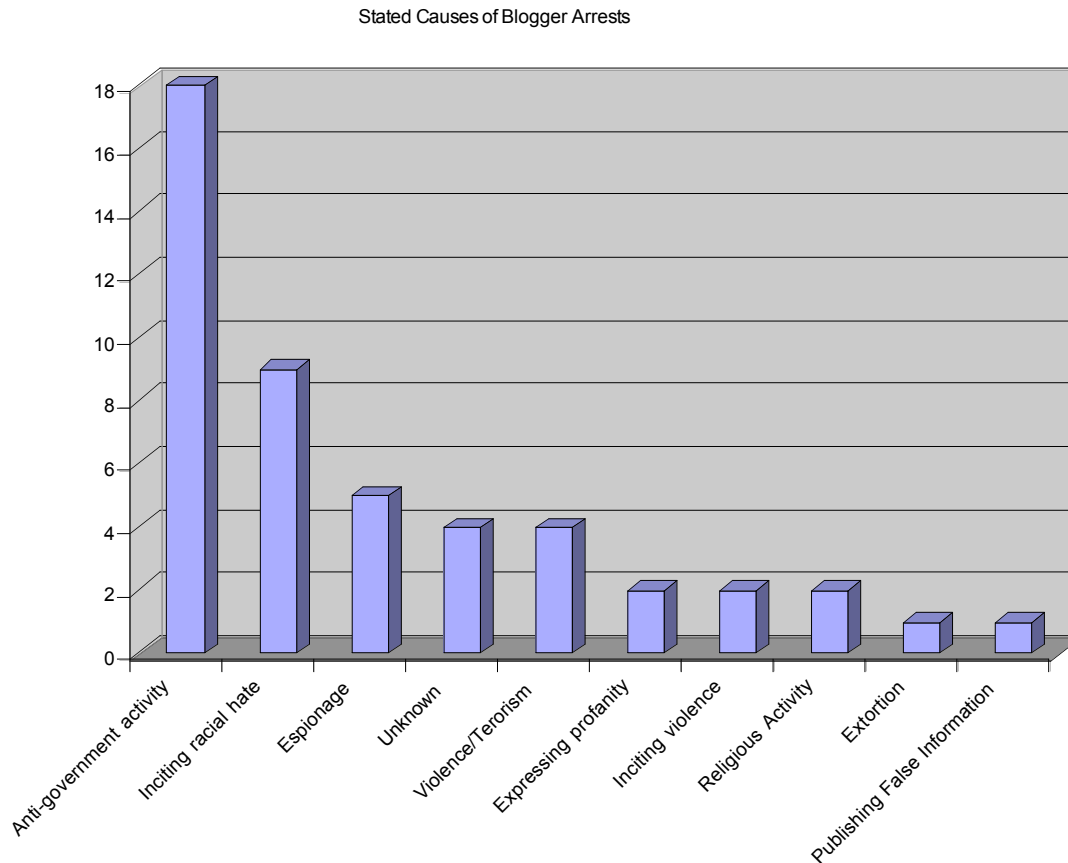
While one might assume that states target bloggers for challenging the legitimacy and authority of the state itself, we found that there are a number of key declared causes for the arrest and detention of bloggers. The most common declared cause of blogger arrests is "anti-state activity." This tends to include bloggers who challenge or insult the leadership of the state or incite anti-government activity, such as protests or violence. Inciting racial hatred and espionage are the second and third highest stated causes of blogger arrests.

(Please see Figure 2)

The limitation of this analysis is the reliance on information provided by state authorities themselves on the cause of a blogger's arrest. In numerous cases, those closely linked to the blogger have argued that the state falsified claims or made their case on trumped up charges, and did so for the sole purpose of silencing unwanted views. It is not easy to

assess the validity of these claims. It should be noted that on a number of occasions those making the claims were also charged and imprisoned soon afterward.³⁰

Figure 2

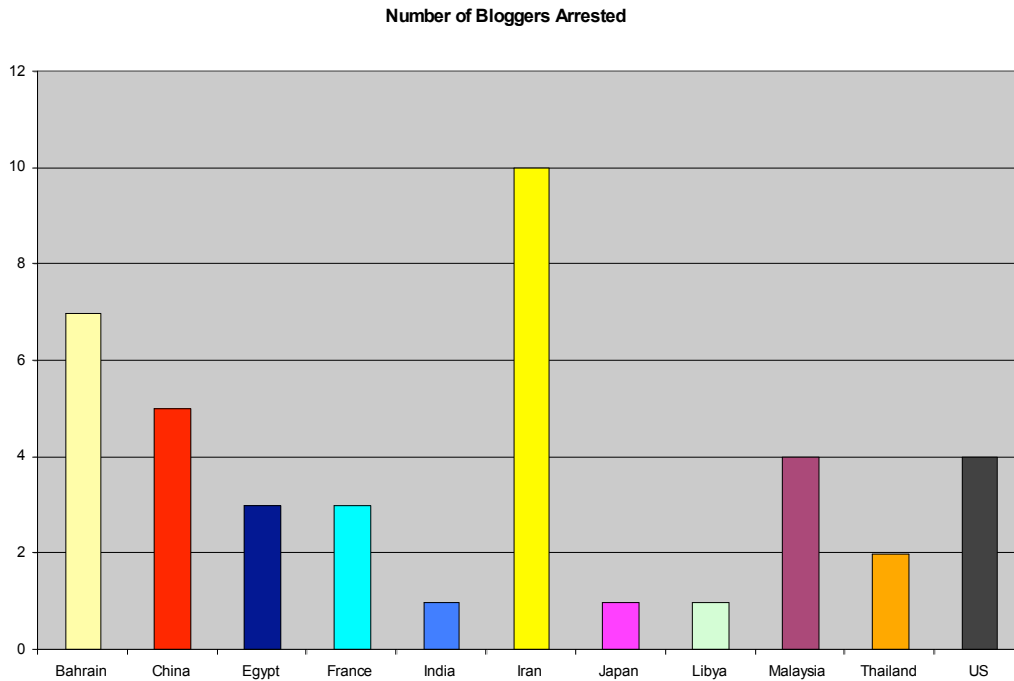


While Iran and China are key perpetrators of threats against bloggers, the effort to silence bloggers is widespread. Bloggers are facing sentences throughout Asia, Europe, North Africa and Europe.

(Please see Figure 3)

³⁰ For more information see the case of Najmeh Oumidparvar of Iran charged and imprisoned for 24 days on March 2, 2005 for post on her blog a defense of her husband, Mohamad Reza Nasab Abdolahi, previously detained for his posts to his blog. And the case of Mojtaba Saminejad, arrested in Iran on February 12, 2005 for posting articles to his blog on the arrest of three other bloggers.

Figure 3

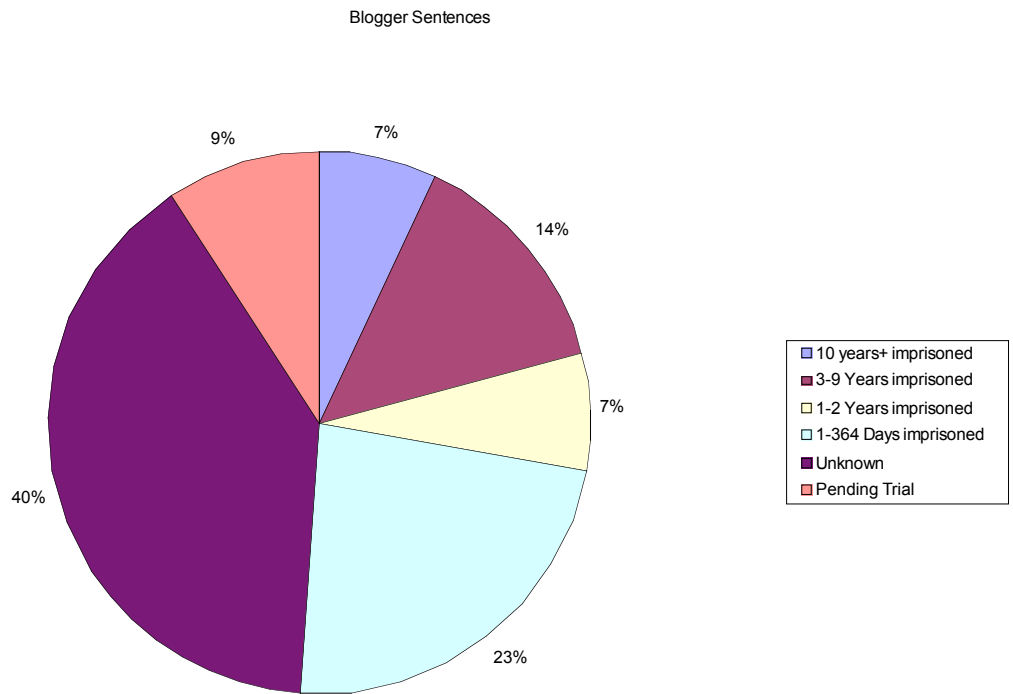


As Figure 3 illustrates, bloggers are facing charges throughout the world. While Iran remains by far the largest contributor to world-wide blogger arrests, Bahrain has prosecuted the second largest number of bloggers. China, Malaysia and the United States are not far behind.

We also found that a preponderance of sentences handed down to bloggers found guilty of a crime is for undisclosed periods of time. While the increase in the number of bloggers facing charges and arrest is in and of itself a worrying trend, perhaps more alarmingly is the finding that 40% of those arrested face charges and sentences that are not made public. Most bloggers arrested will be detained without access to legal recourse until the state, of its own volition, chooses to release information on the blogger's sentence and occasionally release the blogger either outright or pending a trial or retrial.

Of those bloggers whose sentences are public, the majority spend a maximum of one year incarcerated. Often among this group, a longer sentence was set and then shortened during appeals through the justice system. **(Please see Figure 4)**

Figure 4



Blog Filtering

One of the best indications of the political nature of blogging can be found in the extent to which blogs are subject to unlawful Internet filtering. Among two of the states that monitor and control Internet communications that the ONI has investigated, namely China and Iran, blogging has become one of their major focuses of attention, although a number of other countries filter blogs and blogging services as well.

Blogging has become especially popular in China. Although it is difficult to determine with precision the number of blogs hosted in the country, one source indicates that Chinese servers host over 20 million bloggers.³¹ These bloggers post content on topics ranging from daily diaries to political commentary, both critical and supportive of the Chinese state. However, dissidents and human rights activists have been particularly drawn to the medium of blogging. Given the nature of China's Internet filtering and surveillance regime, and the way in which blogging's instantaneous publication threatens the restrictions placed on freedom of speech in that country, it should come as no surprise that Chinese authorities have intensified their efforts to monitor and control blog content. These efforts have ranged from shutting down blogging services entirely, to filtering blogging services for objectionable content.

In March 2004, the state closed three popular, domestic blog providers -- blogcn.com, blogbus.com, and blogdriver.com -- reportedly because a blogger posted a controversial letter regarding the Tiananmen Square incident and the SARS outbreak. All three providers were eventually allowed to re-open, but were required to implement filtering mechanisms. These systems search for sensitive keywords when users attempt to post material. The ONI tested these filtering systems from computers based within China using a list of banned keywords that Chinese hackers discovered and published to a Chinese bulletin board system in August 2004. The list includes terms in categories such as national minorities' independence movements, the Tiananmen Square incident, Falun Gong, proper names of Chinese Communist Party leaders, and sensitive non-proper nouns (such as generic words relating to uprisings or oppression), and were said to be

³¹ http://www.chinadaily.com.cn/china/2007-01/11/content_781602.htm

employed by authorities on popular instant messaging services. Using this list of keywords as a basis for testing, the ONI found that Blogbus and BlogCN filtered only 18 and 19 of the keywords, respectively, while Blogdriver filtered 350 of the terms.

An analysis of the filtered content that the ONI tested shows the areas of content about which the Chinese government is especially sensitive. The filtered keywords generally fall into five categories:

- National minorities' independence movements: the well known Tibetan cause is represented as well as Xinjiang and Inner Mongolia. The inclusion of some Taiwanese politicians' names also fall into this category as they are all people who are known to support Taiwan independence.
- Tiananmen Square incident in 1989: it is referenced both by the full name, "Tiananmen massacre," the Chinese custom of referencing important events by the number of the month and the day (in this case, 6-4), and also by reference to people involved -- a mother of one of the victims who has been campaigning for human rights. The name of Zhao Ziyang, former Chinese Communist Party (CCP) general, is also included in this category.
- Chinese communist leaders: a list of the top leaders, past and present, are included along with a particularly creative rewriting of Jiang Zemin by replacing one of the characters of his name by the character for "thief."
- Falun Gong: a list of different names for Falun Gong including various spellings with characters that sound the same, often used to circumvent filtering.
- Sensitive words: a list of words referring to uprisings or suppression.

Blogs are clearly seen within China as being threatening to the state because of the ways in which they facilitate rapid and easy freedom of expression. As blogs have grown in popularity, the Chinese authorities have focused their attention on blogs, bloggers, and blogging services accordingly.

As with China, blogging has become a popular activity for dissidents and human rights activists both within and outside of Iran. By some counts, there are 65,000 individual blogs written in Persian, and numerous others written in English on Iranian issues by Iran expats located around the world. A list of Iranian blogs is archived at *Blogs X Iranians*.³² One Iranian blogger who lives in Canada, Hossein Derakshan (aka Hoder) has become a

³² <http://blogsbyiranians.com/>

very prominent blogger in the Internet activist community, and has been profiled in major media around the world.

As with China, however, blogging and bloggers have become the target of censorship by a filtering regime that ranks as perhaps second to only China as one of the world's most extensive. The 2005 and 2006 ONI's tests on Internet filtering in Iran including checks on blogs and popular blogging services. The 2005 tests were performed using sets of lists in two different categories: the ONI's general global list of blogging sites applied to all countries (of which 1 was blocked) and a high impact list of 533 Iranian-related blogs. Of the 533 blogging sites that were checked, 86 were found to be filtered. Moreover, there was a dramatic increase in the number of blogs filtered during the time frame in which the ONI conducted its tests; 35 of the 86 sites were accessible one year earlier. The ONI tested a large number of blogs on several of the large blogging domains and found that, while Iran blocks a significant number of individual blogs, the state has not taken the (technically) easier step of preventing access to the entire blogging domains. Most likely this is because the Iranian government wants to allow access to most blogging services (the exceptions being *Moveable Type* and *Live Journal*, which are blocked in their entirety) while focusing on individual blogs that threaten the regime (See Figure 19 below).

Blog Domain	Total Blocks	Partial Blocks	Sites Tested	Block Percentage
blogsky.com	9	0	29	31%
blogspot.com	96	3	257	39%
Persianblog.com	0	7	198	4%

Figure 19: Filtering of Blogging Domains in Iran.

The 2006 tests show a continuation of these trends. For example, all seven ISPs tested in Iran block access to the highly popular blog www.boingboing.net. Iran (four of seven ISP's tested) also blocks access to the popular blogger tool www.technorati.com, www.flickr.com, with all ISPs blocking access to the video posting and distribution site, www.youtube.com.

Although China and Iran are the most aggressive in terms of targeting blogs and bloggers, the ONI found evidence other countries are following suit. In Syria, for example, we tested 159 blog URLs in the Free Expression & Media Freedom category and found 117 blocked. However, all the 117 blocked blogs were hosted on Google's Blogspot and are blocked as a result of the Blogspot service in its entirety being blocked. Ethiopia and Pakistan also block all of Blogspot. In the case of the latter, the motivation to block Blogspot comes from a desire to block access to blogs hosted on the service containing imagery offensive to Islam. However, the Pakistan Telecommunications Authority has chosen to block access to these blogs by blocking all of Blogspot, thus collaterally filtering even those websites critical of the blogs containing the imagery. United Arab Emirates, Ethiopia, India, and Tunisia all block at least one Blogspot blog. Saudi Arabia, Sudan and Tunisia block access to BoingBoing, most likely as a result of those countries' use of SmartFilter which categories BoingBoing as "nudity". Like Iran, Saudi Arabia also blocks access to the video file sharing blog service, YouTube.com.

Just as blogging is becoming a popular form of self-expression and communication generally, activists, dissidents, NGOs, and other global civil society actors are also increasingly blogging. Blogs are even more efficient than typical websites in providing a quick and easy means for individuals and organizations to communicate and distribute information, especially in regions of the world with low bandwidth. Blogging is becoming increasingly politicized, particularly among non-democratic and repressive regimes, but also in the "free" and "partly free" parts of the world. The number of bloggers targeted for silencing has grown in proportion roughly to the spread and increasing popularity of blogging. In some parts of the world, blogging can be an attractive alternative to state-controlled media, but one which presents significant security risks for individuals undertaking the blogging. Blogging content is increasingly subject to Internet censorship and surveillance. Among the countries that the ONI has studied, China and Iran have the most refined systems of blog filtering in place, although there is blog filtering in other countries as well. As the tendency worldwide is towards an increase in the scope and scale of Internet censorship and surveillance, we should anticipate the number of countries targeting blogs for filtering to increase as well.

Evolving Techniques: “Just In Time” blocking, DDOS and Computer Network Attack

Since 2003, research collected by ONI indicates an increase in the number of countries applying filtering to an expanding number of categories, many of which affect civic, resistance, as well as dark nets. However, increasing awareness of filtering practices has also provoked a degree of blowback, evident in both the negative publicity in the global media targeting the worse offenders, such as China, Iran and Uzbekistan, and calls for adjusting US foreign policy to label countries following such practices as pariahs. There is, of course, a question mark over the degree to which establishing the global norm of a free and open Internet is possible, given that such a stance would contradict the concerns shared by many security agencies, in democratic and non-democratic states alike, as to the degree to which the Internet can and does serve as a sanctuary for armed social movements, and hence is in need of enhanced rather than decreased policing. Likewise, criminal exploitation of cyberspace, and particularly efforts aimed at stopping sexual exploitation of children means that calls for the complete removal of filtering are unlikely to meet with success.

It is equally true, however, that not all countries have the political will, economic clout, or natural resource base of a China or Iran. Many Third World countries are dependent on different forms of foreign assistance, or are sensitive to sanctions that may disrupt trade or the movement of migrant workers. Consequently, being labeled as a pariah, with any of the attendant negative publicity and possibility of sanctions, is of consequence. Yet controlling unwanted political agency, whether it comes in the form of pro-democracy groups, independent media channels, or armed social movements is increasingly critical, particularly in authoritarian states, or countries with less institutionalized and more fragile systems for managing political change (such as elections). Among these states, the perceived costs of maintaining a national filtering policy may be seen as either too high, too difficult to maintain, or simply undesirable for other reasons.

However, the costs of no control may be even higher. In this respect, the “color revolutions” that occurred in former Soviet republics of Ukraine, Georgia and Kyrgyzstan between 2003 and 2005 -- which leveraged the Internet and other forms of communications as means to force political change by way of mass civil action -- may be seen as milestones towards the evolution of a new form of “just in time” blocking identified by the ONI. “Just in time” blocking differs from the first generation national filtering practices of countries like China and Iran in several significant ways. First, and most importantly, “just in time” blocking is “temporally” fixed. Unlike the evolving block lists used by national firewalls, “just in time” blocking occurs only at times when the information that is being sought has a specific value or importance. Usually, this will mean that blocking is imposed at times of political change, such as elections, or other potential social flashpoints (important anniversaries, or times of social unrest). In the CIS, this kind of filtering was documented by ONI during the March 2005 Kyrgyz parliamentary elections,³³ the March 2006 Belarus Presidential elections,³⁴ and the October 2006 Tajik Presidential elections.³⁵ It has also been alleged in other regions, including the February 2006 elections in Uganda.³⁶

Second, the exact techniques by which just-in-time blocking is occurring differs greatly from traditional national firewalls. In some cases, such as in the Tajik and Ugandan elections, existing public order laws are used that require ISPs to filter out sites detrimental to national security. In Tajikistan, ISPs received orders to block two opposition websites, “...in compliance with the national concept of information security developed in year 2003” as they were deemed to “aim to undermine the state’s policies in the sphere of information.”³⁷ Similarly the Uganda Communications Commission (UCC) ordered the two national Internet providers MTN and Uganda Telecom, to block radiokatwe.com, a website critical of the government citing “*serious concerns.*”³⁸ The Uganda case came to light as the technique used by the ISP resulted in a further 657

³³ <http://www.opennetinitiative.net/special/kg/>

³⁴ <http://www.opennetinitiative.net/special/kg/>

³⁵ <http://tajikistan.neweurasia.net/?p=116>

³⁶ <http://ice.citizenlab.org/?p=190>

³⁷ <http://tajikistan.neweurasia.net/?p=116>

³⁸ <http://ice.citizenlab.org/?p=190>

completely unrelated websites that shared the same IP address being blocked. Bahrain blocked several web sites in the run-up to the country's parliamentary elections in 2006, and Yemen banned access to several media and local politics sites ahead of the country's 2006 Presidential elections. Likewise, Bahrain also briefly blocked access to Google Earth in 2006, citing national security concerns, as did Jordan in the same year with respect to skype.com.

In other cases, blocking has been accomplished by covert or special technical means. During the Belarus elections, a variety of techniques were observed, ranging from apparent errors in the propagation of domain name information, causing websites to be inaccessible from ISPs within Belarus, through to technical failures that disconnected all Internet access in Minsk during the period of street demonstrations that followed the election. One of the most often seen techniques is the use of Denial of Service attacks (DOS) against ISPs hosting targeted websites or services. This form of blocking is particularly effective as it can occur anonymously, with no demands being made, and presents investigators with the difficult task of pinpointing the source of the attack, which in at least one case was purchased from rogue hackers on the open market (in the CIS). During the Kyrgyz 2005 elections, a sophisticated DOS attack was carried out against a national ISP (El Cat) that hosted several independent (and pro opposition) media sites. "Extortion notes" requiring that the ISPs remove the opposition sites accompanied the attacks. El Cat was particularly vulnerable as it was dependent on a few relatively "narrow" connections to the Internet and as a result, the DOS attacks on the opposition sites threatened to disrupt access to all its other commercial Internet operations, which include a large number of commercial clients. In Belarus, DOS attacks were used against several opposition websites (hosted outside of Belarus). In this latter case, the attacks were not accompanied by any claims of responsibility or demands. The attacks did end shortly after the elections, as it was clear that the opposition was defeated and its street protest would not prevail.

This later form of "just in time" blocking, which takes an offensive rather than defensive character (as in most traditional forms of filtering), is likely to gain in popularity. The

expansion of broadband access, particularly in less developed countries with lower levels of knowledge of “bot nets” and other cracker attacks, will almost certainly lead to an increase in these kind of disruptions as "bot herders" exploit unprotected computers and broadband connections. Other factors also make this form of offensive blocking particularly appealing. The first is that such attacks are difficult to trace back to an exact source (particularly as they can be bought) and thus allow for “plausible deniability.” It is also difficult for individuals or non-state groups to get assistance in tracking down the source of such attacks, as they do not have access to the necessary legal instruments to do so. For example, in the Kyrgyz election case, the extortion notes sent by the attackers originated from a computer located in the US. However, to enlist US authorities’ assistance, the means to do so – Multilateral Legal Assistance Treaties (MLATs) -- need to be initiated by states. In this case, the Kyrgyz ISP affected by the attacks was told that in order to get help from the FBI (or other US law enforcement agencies) they would either have to launch a request through the Kyrgyz Ministry of Justice (or Interior), or file a civil case directly in a US state court in which the computer allegedly responsible for sending the letter was located. In both cases, bureaucratic realities and costs prevented the Kyrgyz IPS from taking any further action. These barriers, combined with the relative ease in which such attacks can be “plausibly denied” by their perpetrators, make them a potentially effective tool for preemptive attacks against information resources. Indeed, use of these kinds of attacks against "terrorist" sites is currently under active consideration by a number of states, including most importantly the United States.³⁹

³⁹ In mid 2006, the US Department of Defense was well underway in preparing the country’s first National Military Strategy for Operations in Cyberspace. While the details of the strategy are expected to remain classified, the identification of cyberspace as a distinct “domains of operations” equal to land, air, sea and space, mark an acknowledgment of its importance to national military capabilities and national security. The strategy is expected to unify and expand the Computer Network Operations that are presently distributed among several separate commands (Joint Task Force – Computer Network Operations, 67th Network Warfare Wing, as well as dedicated resources of the National Security Agency and elsewhere). In December 2006, the US Air Force announced the establishment of the US Cyberspace Command, (formally becoming the 8th Air Force), that is expected to become the global force provider for all US cyberspace operations and will include both offensive and defense Computer Network Operations. The formal announcement of this capability is expected to accelerate the emergence of similar capabilities among other military powers. Already, both China and Russia have declared doctrines for pursuing cyberspace operations. China’s doctrine of “Integrated Network Electronic Warfare” for example, considers computer network attacks as essential to developing a

Indirect filtering by way of DOS or other computer network attacks (CNA) also requires much less in way of infrastructure, and is thus less costly and less difficult to maintain than national firewalls. As a result, it opens the door for sub-state actors to engage in their own denial of access campaigns using CNA. In Russia, and the CIS, for example, winning elections is as much about mobilizing your supporters as it is about preventing the mobilization of opposition groups and parties. The relative ease and low cost of conducting DOS or other CNA makes it inevitable that such tactics will become part of the normal way in which elections campaigns are run. It is also likely that activist groups from across the political spectrum will employ these means as a way to raise awareness or cause lasting damage to their opponents and indirectly to the openness of the Internet, which will likely lead to further calls for regulation and policing. Indirectly, it may induce yet further blowback against unfettered use of the Internet by civic networks.

Conclusions

As the evidence presented in this chapter makes clear, a simple correlation between the Internet environment and the expansion of global civil society can no longer be taken for granted. While it is certain that civic, resistance, and dark networks exploded in the 1990s and early 2000s, the material and political conditions of the communications environment of the time were favorably structured for such an outcome. Largely oblivious to the unintended consequences of the Internet environment, policymakers worldwide were actively encouraging the growth and penetration of information and communication technologies worldwide through FDI and development projects. Not until the appearance and impact of civic, resistance networks, and dark nets – human rights advocates, anti-globalization activists, militants, extremists, and jihadists – did

first strike capability. Special units consisting of reservists drawn from among China's research and computational elite have been formed within the PLA, and since 2006, these units have reportedly participated in large-scale exercises. The entry of the US and major regional superpowers into cyberspace operations is likely to spur an arms race as military establishments worldwide seek to develop both offensive and defensive capabilities. The militarization of cyberspace will create further means for states to regulate and control national cyberspace and will likely lead to further restriction on both civil and "dark" networks. For an extended discussion, see Ronald Deibert and Rafal Rohozinski, *The Global Politics of Internet Securitization*, (forthcoming, MIT Press, 2008).

state military, intelligence, and law enforcement taken active measures to secure the Internet through filtering and surveillance and begin to rethink the encouragement of open and uncontrolled global communications networks. As we show above, the scope, scale, and sophistication of Internet content filtering, surveillance, and other methods of Internet control are growing rapidly and spreading globally. Although these security practices are aimed primarily at “uncivil” society, dark nets, and those actors that are considered a national security threat, the measures also affect the operational environment for civic networks as well.

It is important to underline, however, that notwithstanding these assertions of state power and control, the Internet and civic networks will likely never fully be reigned in. To borrow an old phrase, “the toothpaste is out of the tube.” A sprawling, distributed and highly potent sphere of global civic networks has been unleashed that moves in and around sovereign states. These networks of autonomous agents are highly creative and can be technologically sophisticated. Most noteworthy has been the growing solidification and international presence of a formidable transnational social movement around Internet protection. This movement has put the filtering and surveillance activities of states and corporations under an intense “sous-veillance” grid, exposing unaccountable and non-transparent practices while pushing for access to information and freedom of speech worldwide. Their efforts include grassroots research and development initiatives to build software and advance knowledge and capacity that helps secure human rights online. Although the pendulum has presently swung in the direction of state control worldwide, hacktivists are able to occasionally puncture through.

Alongside state efforts at control, as well as the emerging militarization of cyberspace, therefore, the Internet has become an object of geopolitical contestation among states and non-state actors alike across each of its layers: infrastructure, code, law, and ideas. The outcome of this competing securitization process is not clear, for state sovereignty, for human rights, or for openness on the Internet. While states have more power and legal means to directly influence the Internet, and together are creating mutually-constitutive (if not explicitly defined) norms of control, civil society actors are able to create tools and

publish information that expose and occasionally even undermine these measures. For the foreseeable future, then, we believe the Internet will have no “natural” tendency; it will be a media environment that morphs in continuous tension creating new forms of agency that in turn produce effects that shape the Internet itself. Given the multi-layered complexity of this environment, it seems apparent that no one agent will be able to dominate cyberspace entirely, but many will be able to push technologies, regulations, and norms that affect it.