Towards a cyber security strategy for global civil society?

Ron Deibert
The Canada Centre for Global Security Studies
and the Citizen Lab, Munk School of Global Affairs,
University of Toronto
www.citizenlab.org

Cyberspace is at a watershed moment. Technological transformations have brought about an architectonic change in the communications ecosystem. Cyber crime has exploded to the point of becoming more than a nuisance, but a national security concern. There is a seriously escalating arms race in cyberspace as governments scale up capabilities in their armed forces to fight and win wars in this domain. Telecommunication companies, internet service providers (ISPs) and other private sector actors now actively police the internet. Pressures to regulate the global network of information and communications have never been greater.

Although states were once thought to be powerless in the face of the internet, the giants have been woken from their slumber. How exactly governments react to these problems will determine the future of cyberspace – and by extension the communications platforms upon which global civic networks depend.

Global civil society, now increasingly recognised as an important stakeholder in cyberspace governance, needs to step up to the challenge. A constitutive moment awaits. What is required is nothing less than a serious and comprehensive *security* strategy for cyberspace that addresses the very real threats that plague governments and corporations, addresses national and other security concerns in a forthright manner, while protecting and preserving open networks of information and communication. It is an enormous challenge but also a great opportunity that, if not handled well, could end up having major detrimental consequences for human rights online. Of course, "global civil society" is not an undifferentiated whole, but an amalgam of multiple and diverse local networks. Regardless of their differences, citizens who share an interest in democracy and human rights also share common interests in a secure but open global communications space. Those common interests can lay the basis for a civil society cyber security strategy.

Prior to laying out the elements of such a strategy, it is useful to take a step back and look at some major social forces that are shaping the domain of global communications. The internet's de facto and distributed regime of governance – largely informal and driven up to now by decisions of like-minded engineers – has come under massive stress as a function of the internet's continuing rapid growth. Not only have there been continuing exponential increases in users and deeper penetration into everyday life (a recent Cisco report[1] said that by 2020, there will be 50 billion "things", meaning devices, connected to the internet), but there has been a vast growth in the developing world, as millions of new digital natives come online. With these new digital natives come new values and interests that in turn are affecting internet governance, as governments like China, Russia and India exercise their influence. The latter are now key players in several internet governance forums, and have been collectively pushing for the legitimisation of nationalised controls, such as those over the domain naming system. They also have a shared interest in limiting the voices of civil society in these decision-making forums, an interest exemplified by the push to have the United Nations and the International Telecommunication Union (a state-based organisation) take the lead on internet governance. Civic networks need to be vigilant that such a strategy does not succeed.

Another major force shaping cyberspace arises out of technological innovation and economic factors that have created the architectonic shifts in the nature of the ecosystem of global communications. Whereas before the internet was largely a self-segmented and isolated network generally separate from other means of communication, such as television, telephony and radio, all of these media have integrated into a single system of planetary communications, which we call cyberspace. The integration of these media into a common space has happened at the same time that business models and service delivery mechanisms for information and communications have changed fundamentally, with the rise of social networking, cloud computing, and mobile forms of connectivity. This paradigm shift has upset

[1] www.readwriteweb.com/archives/cisco_50_billion_things_on_the_internet_by_2020.php

the principles, norms and rules of what used to be just the "internet", with implications for freedom of speech and access to information. Today, our data is entrusted to vast transnational information empires who act as gatekeepers and increasingly arbiters of what gets communicated, and what information is accessible or not. Market considerations can easily outweigh privacy and other rights concerns, and have already made largely irrelevant so-called "end-to-end" principles that once ensured network neutrality. Even something as benign as a spam filter gone wild can end up unintentionally disrupting political communications, as our research on Apple's MobileMe filtering system[2] has shown.

More serious, however, are the ways in which the private sector is being pressured, compelled, and even *incentivised* to "police the internet" by governments looking to download their growing cyberspace controls. For example, in Canada, the Stephen Harper government is introducing an Omnibus Crime Bill[3] through parliament that would require ISPs and telecommunications companies to retain user data, process the data in ways that make it amenable to law enforcement and intelligence, and then share that data with law enforcement representatives – all without judicial oversight. Arrangements like these are not uncommon. Privacy researcher Chris Soghoian has made a career documenting[4] how private sector actors not only facilitate access to information for law enforcement, but actually derive revenues from doing so. He has also documented extensive variation among these actors on the specifics of their data retention and privacy policies. As a result, citizens using different communications services can live in entirely different universes of rights.

The downloading of policing functions to the private sector – a phenomenon known as "intermediary liability" – extends to the protection of intellectual property. At a recent meeting[5] on the internet economy organised by the Organisation for Economic Co-operation and Development (OECD) in Paris, the final communiqué argued that ISPs should take on more expansive roles chasing down copyright violators using their networks. Civil society stakeholders refused to sign on to the final communiqué largely in objection to this component. The OECD communiqué is but a reflection of a larger trend. In the United States (US), several ISPs and carriers have already taken on this responsibility as a voluntary arrangement. Across the industrialised world, it is considered standard practice for large carriers to "clean their pipes" of malicious networks and traffic that is associated with file sharing or similar "undesirable" activities. The bottom line of business now demands it.

Of course what is considered "intermediary liability" or a market imperative in Canada and the US differs quite fundamentally from Belarus, Iran, Viet Nam or China. In non-democratic countries, ISPs, telecom carriers and mobile operators are being asked to police political content, track dissidents, identify protesters, send threatening messages over their networks, and disable certain protocols used by adversaries – all as part of what my colleague Rafal Rohozinski[6] and I have dubbed "next-generation controls"[7] that we see emerging throughout the developing world. During the Arab Spring, for example, the Egyptian government took the drastic step of forcing ISPs to shutter the internet, and required the country's main mobile phone operator, Vodafone, to send mass text messages encouraging pro-regime sympathisers to take to the streets to counter the protesters. This shift towards intermediary liability is perhaps one of the greatest practical changes around internet governance in the last decade, particularly when considered in the context of growing cyberspace securitisation, of which it is a part.

The *securitisation* of cyberspace – a transformation of the domain into a matter of national security – is perhaps the most important factor shaping the global communications ecosystem today. Faced with the combined pressures above, and seemingly incessant and embarrassing large-scale data breaches, policy makers around the world are racing to develop cyber security strategies. Some are following the lead of the US, standing up within their armed forces dedicated cyber commands and laying out formal doctrines for cyberspace. Others are adopting less conventional means, including providing tacit support for pro-patriotic groups to engage in offensive cyber attacks in defence of their country, as seems to be the case in Iran, Syria, Russia, Burma and China.

Cyberspace securitisation includes a political economy dimension: there is a growing cyber industrial complex[8] around security products and services that both responds to, but also shapes the policy

[2] opennet.net/apple-mobileme-brief

[3] www.michaelgeist.ca/content/view/5808/135

[4] www.dubfire.net/#pubs

[5] www.oecd.org/document/59/0,3746,en_21571361_44315115_48173819_1_1_1_1,00.html

[6] Rafal Rohozinski is a Senior Scholar at the Canada Centre for Global Security Studies at the Munk School of Global Affairs, University of Toronto. He is a co-principal investigator of the OpenNet Initiative and Information Warfare Monitor projects.

[7] www.access-controlled.net/wp-content/PDFs/chapter-1.pdf

[8] www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159

marketplace. Corporate giants of the Cold War, like Northrup Grunman, Boeing and General Dynamics, are repositioning themselves for lucrative defence contracts, alongside an array of subterranean niche companies that offer computer network exploitation products and services. The global cyber arms trade[9] now includes malicious viruses, zero-day exploits and massive botnets. An arms race in cyberspace has been unleashed, with international implications. For every US Cyber Command, there is now a Syrian or Iranian cyber army equivalent. For every "Internet Freedom in a Suitcase",[10] there is justification for greater territorialisation of cyberspace controls.

Cyberspace securitisation has also effectively *normalised* internet censorship. What was once the province of pariah states, like China and Saudi Arabia, is now quickly becoming the norm among liberal democracies and authoritarian regimes alike. Our OpenNet Initiative[11] project tracks internet filtering and information controls in more than 40 countries worldwide. But perhaps the best insight on the normalisation of internet restrictions comes from data provided by Google. As part of its Transparency Report,[12] Google now discloses requests from governments for user data or the removal of information on its websites and services, like YouTube. The data it released for the July-December 2010 period was perhaps most remarkable not so much for confirming the usual suspects, but rather for the way it revealed that censorship is now normal among democratic countries. The governments of Germany, the United Kingdom, Brazil, Italy and others make thousands of take-down requests every year.[13] Here too, as a complement to these new developments, internet censorship services – produced primarily in the West[14] – have become a major commercial sector. When Canadian filtering software companies who provide services and products to Yemen, Kuwait and the United Arab Emirates are actually applauded[15] for their efforts by the Canadian government, we can safely say that internet censorship has become a global norm.

Rohozinski and I have summed up these cumulative forces as the coming "perfect storm" in cyberspace. With threats seemingly multiplying, and mutually reinforcing tendencies like those above growing, the prospects of extreme solutions finding widespread acceptance are high. Whether it is a proposal for an entirely new internet (as former CIA director Michael Hayden recently argued)[16] or the gradual metamorphosis of the existing open communications space into sovereign-controlled national internets, the securitisation wave is going to have major and potentially damaging consequences for civic networks. What is to be done?

First, as argued, there is an urgent need for the articulation of a cyber security strategy for civic networks. For many who would characterise themselves as part of global civil society, "security" is seen as anathema. In today's world of exaggerated threats and self-serving hyperbole from the computer security industry, it is easy to dismiss security as a myth to be demolished, rather than engaged. Securitisation is associated with the defence industry, Pentagon strategists, and the cyber security military industrial complex. Many might question whether employing the language of security only plays into this complex and the growing might of cyberspace controls.

But the vulnerabilities of cyberspace are very real, the underbelly of cyber crime is undeniably huge and growing, an arms race in cyberspace is escalating, and major governments are poised to set the rules of the road[17] that may impose top-down solutions that subvert the domain as we know it. Dismissing these as manufactured myths propagated by the power elite will only marginalise civic networks from the conversations where policies are being forged.

Civic networks need to be at the forefront of security solutions that preserve cyberspace as an open commons of information, protect privacy by design, and shore up access to information and freedom of speech, while at the same time address the growing vulnerabilities that have produced a massive explosion in cyber crime and security breaches. How can security and openness be reconciled? Aren't the two contradictory? Not at all. The answer lies in the internet itself. As my colleague Jonathan Zittrain has forcefully argued, there are open and generative self-healing and protective mechanisms that are a part of the everyday functioning of the internet itself. Zittrain's views are backed up by a recent European

[9] www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html

[10] www.nytimes.com/2011/06/12/world/12internet.html?_r=1&pagewanted=all

[11] map.opennet.net

[12] www.google.com/transparencyreport

[13] www.washingtonpost.com/blogs/blogpost/post/web-censorship-moves-to-democracies-the-west/2011/06/27/AGPi4xnH_blog.html

[14] opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

[15] opennet.net/blog/2011/07/canadian-government-lauds-uae-internet-service-provider-pervasively-censors-political-r

[16] www.nextgov.com/nextgov/ng_20110706_1137.php

[17] arstechnica.com/tech-policy/news/2011/05/france-attempts-to-civilize-the-internet-internet-fights-back.ars

security study which explained how the open and decentralised organisation that is the very essence of the ecosystem is essential to the success and resilience of the internet.[18] What is remarkable, in other words, is that the internet functions precisely in the *absence* of centralised control and *because* of the thousands of distributed, loosely coordinated monitoring mechanisms. While these decentralised mechanisms are not perfect and can occasionally fail, they should be bolstered and enhanced as part of a coherent distributed security strategy. Bottom-up, "grassroots" solutions to the internet's security problems are consistent with principles of openness, avoid heavy-handed centralised controls, and provide checks and balances against the concentration of power in cyberspace. Part of a civil society security strategy should be to find ways to facilitate cooperation among the existing, largely scattered security networks while simultaneously making their actions more transparent and accountable.

Part of the civic strategy must also include a serious engagement with law enforcement – another traditional anathema for civil society. Law enforcement agencies are often stigmatised as the Orwellian bogeymen of internet freedom (and in places like Belarus, Uzbekistan and Burma, they are), but the reality in the liberal democratic world is more complex. Many law enforcement agencies are overwhelmed with cyber crime, are understaffed, lack proper equipment and training, and have no incentives or structures to cooperate across borders. Instead of dealing with these shortcomings head on, politicians are opting for new "Patriot Act" powers that dilute civil liberties, place burdens on the private sector, and conjure up fears of a surveillance society. What law enforcement needs is not new powers, it needs new resources, capabilities, proper training and equipment. But alongside those new resources should be the highest standards of judicial oversight and public accountability. Civic networks can articulate the differences between powers and resources, and highlight the importance of public accountability to liberal democracy as an example to the rest of the world without alienating what could be an important natural ally.

The same basic premise of oversight and accountability must extend to the private sector as well. Civic networks are inherently transnational and are because of this best equipped to monitor globe-spanning corporations who own and operate cyberspace. Persistent public pressure, backed up by credible evidence-based research and campaigns – like the Electronic Frontier Foundation's (EFF) privacy scorecard[19] – are the best means to ensure the private sector complies with human rights standards worldwide. Going further, however, civic networks should make the case that government pressures to police the internet impose costly burdens on businesses that should be conceded only with the greatest reservations and proper oversight. Such self-interest-based arguments will have much greater traction with the private sector than either pleas for magnanimity or pressures of naming and shaming ever will.

Lastly, civic networks need to be players in the rule-making forums where cyberspace rules of the road are implemented. This is not an easy task. There is no one single forum of cyberspace governance; instead, governance is diffuse and distributed across multiple forums, meetings and standard-setting bodies at local, national, regional and global levels. The idea of civil society participation in these centres of cyberspace governance varies widely, and is alien to some. Civic networks will need to monitor all of these centres of governance, open the doors to participation in those venues that are now closed shops, and make sure that "multi-stakeholder participation" is not just something paid lip service to by politicians, but something meaningfully exercised by networks of citizens. The civil society rejection of the OECD final communiqué is a model in this regard.

The idea of *security* is most closely associated with the tradition of *realpolitik*, and the denizens of the national security apparatus. Global civil society, on the other hand, is most often associated with respect for rights, democracy, diversity and openness. As the securitisation of cyberspace builds momentum, it may be tempting for civic networks to either concede the terms of the security debate to the national security community, or resist it altogether. That would be a mistake. There is a long-standing and very powerful tradition of *liberal security*, associated with distributed checks and balances, respect for individual rights, and decentralisation. What is urgently required now is the translation of that tradition to the domain of cyberspace, and the practical application of its principles by citizens worldwide. Otherwise, the great gains in networking that have produced an explosion in global civil society over the last decades could gradually evaporate. ■

[18] www.lightbluetouchpaper.org/2011/04/12/resilience-of-the-internet-interconnection-ecosystem

[19] www.eff.org/pages/when-government-comes-knocking-who-has-your-back