Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Three Views of Cyberspace

David D. Clark

Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

January 5, 2011

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

Three views of cyberspace

David Clark

Version 3.1 of January 5, 2011

The purpose of this paper is to draw attention to an important but perhaps under-appreciated aspect of the Internet: the emergent idea of a global commons in the use of the Internet, in which people might transcend national boundaries to discuss, plan and organize to further matters of global import, whether environmental regulation, curbing epidemics, mitigating poverty, reducing risks of nuclear wars, promoting individual freedoms, etc. This paper attempts to construct a framework to assess what this commons might be, variations in its practices, the threats it faces, and both technological and political means of protecting or at least preserving it.

Cyberspace, or more specifically the Internet, is a complex, multi-faceted phenomenon, and different actors with different perspectives may perceive it in very different ways. Our perception of cyberspace and our understanding of what is happening there is shaped to a considerable extent by the lens or framing through which we interpret what we see. As a framework for analysis, this paper proposes three different lenses through which different actors seem to observe and interpret cyberspace[1]. I will argue that actors looking through these three lenses see a very different set of priorities that should shape the future of the Internet, and I will argue that the lens through we can understand an emergent or potential global commons is not as well recognized or articulated as it should be.

The first lens is national security. The imagery of this lens is that cyberspace is a place of conflict, like the sea or air. This image leads to discussion of cyber attack and defense and state-sponsored espionage. In this context, engagements in cyberspace are easily mapped into one of two categories, "attack", and "exploit", roles that are traditionally given to state-level military and intelligence actors. The international dimensions of security are obvious, as well as state-centered concerns with internal stability.

The second lens is economics, which evokes imagery of competition and investment. The international dimensions include globalization and international trade, industrial espionage, international crime and the like. The actors are both states and multi-national corporations. Protection from wrong-doing is normally provided by police, rather than the military, and states negotiate to provide a stable, international context for trade and competition. In contrast to security, the goal (as seen through this lens) is prosperity.

The third lens I called society, a broad term meant to capture a range of images centered around community and social interaction, personal concerns such as privacy, and internationally, the potential for the emergence of a global commons or a global civil

[1] I am grateful to Roger Hurwitz for the original articulation of these three lenses. His terms for the lenses were security, globalization, and the global commons, which tend to stress the international nature of the lenses. I have used the more general terms of security, economics and society.

society. The activity here is voluntary interaction among state and non-state actors in pursuit of self-selected goals. Among other things, actors assemble in the global commons to reshape the world: to shift, in small ways, the world order, and to achieve new outcomes that are not strictly economic (e.g. deal with disease), or only partially economic (improve working conditions). The sponsors of actions here are to a large extent non-state actors: NGOs, resistance nets, political activists and individuals. In contrast to prosperity, the value here is freedom.

One of the powerful implications of this third lens is that it brings into focus a set of actions within cyberspace that do not fit neatly into the dichotomy of "attack" and "exploit", or alternatively into the category of crime. When China puts a firewall around their country, this is not a cyber-attack, nor espionage, but it is something worth noting; so is blocking Twitter or Facebook, or giving anonymizing software to activists in repressive countries. There is a set of actions going on for which we currently have no name—no basket into which to put them, and which thus are not given proper attention. We should name this basket, and I suggest as a starting point the term "**cyber-contention**".

Cyber-contention

If cyber-attack is about destruction, and cyber-espionage is about theft of intellectual property, what (in general terms) is the center of cyber-contention? It is exactly about the push and pull of civil society-the attempts to empower or to regulate and restrain free association and assembly, the right of unregulated speech, and the right of private assembly. These capabilities are the hallmark of a global commons, just as competition is the hallmark of economic contention.

What is 'cyber" about all this? A broad class of actions, perhaps the most common if not the most interesting, use cyber as a tool for contention-one actor reaches through cyberspace to interact with another. Web sites protest behavior of one sort or another. People are recruited to causes, give money, send email calling for action, and so on. In this respect, the cyber phenomenon should be seen as a powerful amplifier and enabler. However, these activities do not directly change cyberspace itself.

More interesting for our consideration are those actions that attempt to bring change of one form or another to cyberspace--in particular to make it more or less open, more or less anonymous, more or less available in an unregulated form. For the rest of this document, I will mostly focus on those actions that try to reshape cyber-space, not just those that exploit it.

One reason to identify cyber-contention (and to pull it apart from the framing of cyber-attack) is that we make different assumptions about why and whether different sorts of behavior will occur. We have seen few examples of actual cyber-attack apart from a larger kinetic conflict. Some have argued that there is little justification for cyber-attack outside of a larger conflict. But cyber-contention is very different. Cyber-contention is an ongoing phenomenon. It is "what is happening" today. **So we need theories of cyber-contention--why does it happen, when does it start and stop, what are the "rules of play"?**

Two interesting questions about each framing is "who are the bad guys" and "who defends us". In the case of security, we expect the military to defend us. The United Nations has defined war as between aggressors ("bad guys") and defenders ("good guys"). In the case of economics, we expect the police to defend us, even if crime is international, and we expect our government to advocate for policies that stabilize international commerce. In the case of cyber-contention, we can easily map the actors into classes with different interests ("free speech" vs. "regulated speech"), and we can see conflicting norms playing out in different sorts of actions, but there is no clear framing of "bad guys", or "attackers". Nor is there the concept of "defense". Contention is perhaps better seen as among actors with equal standing but with different values, objectives, and norms. This observation is, by itself, not at all surprising, but it serves to remind us that with this lens, there are no police and no military as primary actors. But this begs the question of who the primary actors should be.

Blurred boundaries

Recent events (in the real world) have illustrated that all of these framings are important, and also illustrate that the boundaries are blurred. The lens of society is not distinct and strictly partitioned from the other two. First, trans-national economic endeavor is an example of voluntary association, and association for economic purposes cannot be cut apart from civil society. I will return to economic considerations below. Second, some activities that might be seen by one party as just facilitating free association might be seen by others as bordering on attack--regime-change by other means. Cyber-contention often has political goals, but they have a different character then actual war. Even if one of the actors might see cyber-contention (e.g. technical facilitation of dissidents) as leading to internal civil instability and a vector of regime change, it is not carried out with the goal of destruction of equipment nor as part of an escalating war.

I believe that the blurring of boundaries between these framings in cyberspace will be the most vexing for our military, which has in the past thought it had clear boundaries on what it should and should not do. Traditionally, the military has been positioned within a well-defined context of national security. Nations reserve to their military the use of kinetic force outside their national boundaries, and the laws of armed conflict attempt to center the use of that force on other militaries. Armies are not supposed to attack civilians wantonly, nor civilians to attack soldiers. Of course, in modern wars this convention is unraveling, but more importantly, as our military finds itself involved in activities more like nation-building, they are acting outside the framing of national security. As a result, they interact with actors on "the other side" that are not soldiers, but civilians or civilian agencies of other governments.

This effect will only be amplified in cyberspace. First, what constitutes "armed conflict" in cyberspace is not well-defined, so the boundaries defining what the military should and should not do there are vague. Second, and perhaps more important, cyber-contention that one side sees through the framing of society or a global commons (or least claims to see through this framing), such as deploying Twitter, may be seen by the other side through the framing of national security—Twitter is a destabilizing tool intended to encourage regime change. If one nation's military acts to suppress Twitter, should the military of another nation respond? If so, what might they do: could it be their role to distribute VPN software?

If another nation uses its intelligence agency for industrial espionage (which suggests the framing of economics and global competition), should our intelligence agencies respond? If so, through what framing?

Effecting change in cyberspace

Let me return to the question of how, and to what extent, actors centered in one or another lens have attempted to reshape cyberspace. Looking through the three lenses, what are the consequences of the various tussles and engagements?

Through the lens of national security, we have few examples of actual attack in the context of warlike behavior, and those that exist did not immediately trigger a lasting effect on cyberspace. The framing of national cyber-policy using terms such as "cyber-attack" and "cyber-command" may indeed have a long-term influence over the shape of cyberspace--such actions (and the choice of terms) can shift the long-term framing of cyber-space itself. **Cyber defense will change cyberspace more than cyberattack.**

Through the lens of economics, we can find more obvious changes, which have largely result from the influence of private actors. The drive to facilitate ecommerce in the late 1990's led to a call for secure (encrypted) communication between consumer and merchant, which in turn led to a tussle between commercial interests and national security advocates, who wanted to slow the deployment of easy-to-use encryption. The commercial interests prevailed. As a part of this movement, certificate-signing authorities for merchants were created, and essentially all web client and web server software was modified to support encrypted communication (in particular, the protocols SSL and TLS).

How have the actors concerned with the lens of society and a global commons changed cyberspace? The under-appreciation of this third lens is important to rectify, because it may be the case that cyber-contention, and the tussles over regulation may have more long-term influence over the shape of cyberspace than the actions that result from either the national security or economic framing. What is directly contested in this space is fundamental: it is the character of the Internet itself.

What are the characteristics of cyber-space over which these actors contend?

- Connectedness and access.
- Universality and neutrality.
- Identity and accountability.

These features, of course, are those that define the character of a civil society, and we can see cyber-contention as centered around those values.

Power

The recognition of cyber-contention as a basket of actions begs a return to a very traditional question in political science: what are the sources of power in this context; how does it emerge and for what purposes.

The direct projection of hard power by states in cyberspace seems to stop at national boundaries, except for explicit cyber-attack. Within a state, a government can effect change by direct regulation or control of the operators of cyberspace. One interesting question is whether (and to what extent) a powerful state can change the overall nature of cyberspace by making domestic changes. But at a global level, more commonly one must use other forms of power to effect change. Both the lenses of economics and society focus us, at an international level, on actions based on multilateral discussions and advocacy of collective norms, where softer forms of power are more relevant: agenda setting, control of venue and rules of negotiation, using national influence and prestige to assemble coalitions, and the like. The norms that the U.S. has defended in the context of society, such as free political speech, seem familiar and consistent with US values; that should not surprise us.

It has been argued that the US has been unwilling to cede control of the Internet to a more multi-lateral form of governance. To the extent that this fact is true, it is interesting to speculate as to whether this resistance is due to the desire to hold on to the Internet as a source of power, or a fear that the current norms expressed in the design of the Internet would be eroded by such an institution.

It is informative to consider what institutions exist consistent with the three framings, especially at the international or global level. There are formal multi-national (state-centered) institutions that deal with national security and economics: national security is addressed in many multi-national contexts, and (for example) the OECD deals with economics. But there do not seem to be many international institutions that have been organized to discuss and perhaps moderate the cyber-contention in the context of societal issues such as the emergence of a global commons.

If international state-related institutions are weak in this area, this raises the question of whether there are non-state institutions that have been constituted to address issues around the global commons, and whether non-state actors have (or can have) substantive power here. Economically motivated private sector actors have demonstrated power in economic contexts (e.g. the push for Web encryption)—what power might socially motivated actors have in this framing? In the early tussles between advocates of privacy and governments pursuing national security, privacy did not prevail. It was commercial interests in ecommerce that seem to have trumped national security concerns about encrypted communication[2]So it might seem, from a U.S. perspective, that economics trumps national security trumps societal concerns. (And we see this in the first years of the Obama administration, with concerns about economic recovery apparently trumping serious attention to cyber-security.) Security trumps economic prosperity only in moments of intense crisis.

Civil society

A term for the international dimension of the lens of society is global civil society. Civil society within a nation has traditionally been seen as the consequence of a rule of law that

[2] Shirley K. Hung. *Managing uncertainty : foresight and flexibility in cryptography and voice over IP policy* . MIT PhD, 2008.

permits free and private voluntary assembly and such underpinnings. A global civil society, to the extent it exists, does not emerge from under the wing of a benign national context, but more "in the wild". If one views international relations as a state of anarchy, then any global civil society must emerge in that context. But the international context is, of course, not a total anarchy, but a complex context of norms, treaties, agreements, empowering technologies and the like. It is from this soup of considerations that a global civil society will have to emerge and survive.

One institution that might take on cyber-contention and the fostering cyberspace as a vehicle for a global commons or a global civil society would be the United Nations. Many of the foundations of a global civil society can be seen in the Universal Declaration of Human Rights. It would be interesting to examine the Internet Governance Forum (the current UN cyber-activity) to look for evidence of leadership from the UN to advocate for values consistent with that framing document, as opposed to a venue for presenting of respective positions.

For the moment, it seems that cyber-contention is a process involving many actors, without a strong manifestation of power by any single actor or group of actors, but that interested states seem to have more focus and intention than non-state actors, even though a global commons or global civil society is a non-state phenomenon.

Perhaps more significant for the U.S. and its ability to advocate for its values, there are few examples within the U.S. government of agencies or organizations (or operating units within them) that have the mandate to protect these values. One sees national security well represented by the military and intelligence, and by matching units within (for example) the State Department. One sees economic issues well represented. But the third framing is essentially missing in action.

Internet governance

The question of "Internet governance" has received a lot of attention in various circles, and has been a topic of international debate. Many of the specific debates seem to be about narrow questions such as the allowed character sets for Domain Names, or the process for allocation of network addresses. However, these debates may be a proxy for a deeper set of debates, visible to a variable degree. The debates about governance of the Internet may actually be about the governance of the *character* of the Internet—how open, how easy to control and regulate, and so on.

Researching the outcome

I have posed a research question as finding theories of cyber-contention--why does it happen, when does it start and stop, and what are the "rules of play"? A core question is whether there is a way to predict the outcome of cyber-contention. The current Internet is defined by a high degree of open communication, and a medium degree of anonymous action. As actors contend over this character, is there any theory that can predict the outcome, or is the future totally "up for grabs"?

In the global arena, it is shared norms rather than top-down laws that define what is acceptable and what should be protected. And norms emerge and shift only so fast. One possible observation about the current world is that the rapid rate of change, which seems to be a hallmark of cyberspace, has caused society to overdrive its normative headlights.

But it seems more than that. The Internet seems to have shifted norms toward free association and other signals of civil society. So both shift and speed are factor to be considered.

One might argue that the individual empowerment that has occurred across the globe, and the empowerment of the INGOs is a phenomenon that cannot be turned back. This view would argue that cyber-contention can only go so far in imposing restrictions on the open nature of cyberspace. But is this view just an untested (untestable?) and perhaps optimistic theory, or something that might be explored and challenged through research? One consideration is the interplay of motives and actions that arise from the three different lenses. The lens of society tends to suggest that private association (anonymous action) is a good thing. The lenses of national security and economics, with their emphasis on defense, deterrence, crime and policing, seem to call for more accountability. This tension might to some small degree be resolved through technical innovation, but it may also be resolved only as a rebalancing of demands made by society on the technology.

A prediction about the future

It has been speculated that concerns over local control might lead to a "Balkanization" of the Internet, but that analogy does not capture what might actually happen. What we see today is a stable multi-state norm of "mostly open" communication, which supports an Internet with essentially the character it has today. We say "mostly open" because the French may block mention of Nazi memorabilia, the Thais may block insults to their king, and copyright holders may attempt to block the transfer of unlicensed material, but events like this do not signal the end of unregulated speech, or the end of the Internet as we know it. Free speech "mostly" survives small cuts like this.

A plausible prediction might be that a "mostly open" Internet, spanning those regions that respect this norm of unregulated communication, will continue to sit at the center of the global network. Regions that seek to impose a higher degree of regulation over speech and communication will be forced to the edge, both in the sense of technical connectivity and of social connectivity. In this respect, the shape of cyberspace may reflect a larger world order.

The pattern of "closed nets at the edge" is not unfamiliar; it is what we see today when corporations connect to the Internet. Corporations impose restrictions on what their employees do—what applications they run, whether certain sorts of communication is on the one hand forbidden or on the other hand logged, and so on. Of course, there is a societal difference—employees of "closed" employers in an "open" state can go home and do what they please on their own time. But the implications for the Internet of this "corporate

Balkanization" are that the tools for control, both technical and policy, are well-understood and already available.

Within this large "central" region of states that "mostly respect" the norm of open and unregulated speech, it is a reasonable speculation that the current open character of the Internet is a stable condition. What are the forces that might erode this open character? We can see four, and these are forces to watch.

- The call for better security. In the cause of better security, there have been calls for tighter attribution and tracking of behavior, which (if it were embedded in the core of the Internet) would be precisely the tools needed to track and regulate speech. (An example of action centered in the national security lens.)
- The protection of copyright material. Copyright holders, in their quest to prevent the sharing of pirated material, have lobbied governments to make ISPs part of the machinery of policing, giving up the names of offenders and looking at what is sent to detect "unacceptable" material. (An example of action centered in the economics lens.)
- Application designers. While the Internet, at the packet level, is open, real users do not just send packets, they invoke applications. It will be those applications that define what patterns of communication are available to non-technical users. Today, applications are mostly designed and deployed by actors with commercial interests, and the degree of "openness" is sometimes a secondary consideration in their designs. In the U.S. these actors are private, and have no obligation with respect to free speech. (These actors seem to be motivated by a mixed set of considerations.)
- The influence of those who prefer a more closed network. Of the four forces, I actually fear this the least. But if those nations that favor a more regulated Internet push for changes to the core function of the network, this would be a concern.

At the same time, we could consider and perhaps dismiss some forces that are less likely (in my opinion, but worth debate) to change the open character of the Internet.

- Commercial DPI and advertising. While there is much fear and concern about ISPs (and others) who want to track what users are doing, their motivations are revenue-seeking, not control. The more a person does on the net, the better as far as they are concerned. Only if their tools are co-opted by other actors is there a concern. We might worry about their tools, but not what they do with them today, when we consider the stability of the global commons.
- Mobility. Mobile devices today are much more closed than the "old-fashioned" PC-based Internet. One point of view is (again) that the motivations of the operators are revenue-based, but it is clear that in some countries, mobile behavior is closely tracked.
- App stores. App stores represent a "closed" market for applications, rather than the open marketplace for apps in the PC based internet. These markets represent a new point of control. However, it is not clear that this point of control is motivated to take a position with respect to the global commons and civil society.

Appendix: Examples of cyber-contention

Normative/value/control driven

- The great firewall of china.
- Blocking of Internet during Chinese ethnic unrest.
- Blocking of Youtube by a number of countries.
- Distribution of trans-jurisdictional VPN software (borders national security lens).
- TOR.
- Blocking of Blackberry in certain countries. (equivalent to blocking encrypted communication.)
- Various content blocking events as logged by Herdict.
- Proposal by China (to ITU) to allocate IPv6 addresses to countries.

Significant economic interaction/overlap

- Contention over broadband deployment: who invests, who benefits. (spills over into network neutrality debates)
- Control of unlicensed distribution of copyright information (spills over into tussle over control)
- P2P sharing
- Interconnection agreements
- Imposition of taxes (may not impact technology)
- Proprietary vs. standards-based applications.

Significant security interaction/overlap

- Calls for an "accountable Internet", or the need for "tools of attribution" as part of deterrence.
- Regulation to impose CALEA on VoIP.
- Requirements in certain countries for strong identification of users in all contexts (e.g. wifi hotspots.)

Multiple triggers

- Network neutrality debates: in part economic, in part normative.
- DNS issues (multiple character sets, TLDs, security)