Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

# Tools of Engagement: Mapping the Tussles in Cyberspace

**David D. Clark**

Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

March 12, 2010

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.

# Tools of engagement: mapping the tussles in cyberspace

**David Clark**

**MIT CSAIL**

**Version 4.3 of March 12, 2010**

This work is funded by the Office of Naval Research under award number N00014091059 and N000140810898. Any opinions, findings, and conclusions or recommendations expressed in this email are those of the author (s) and do not necessarily reflect the views of the Office of Naval Research.

## Table of Contents

# 1 Introduction: objective

This paper has been prepared as part of *the Explorations in Cyber International Relations* project being carried out at MIT, Harvard and collaborating institutions. The goal of this paper is to lay the groundwork for the exploration of a fundamental thesis of the project: that the emergence of cyberspace as a phenomenon has shifted the motivations of the various actors that play on the international stage, it has added to the "tools of engagement" that these actors use as they interact, and it has created or empowered new sorts of actors that must now be taken into account in any theory of international relations.

This paper, which should at this point be seen as a working draft, incomplete and anecdotal rather than scholarly and thorough, attempts to catalog by example the range of actors and the tools they use as they interact around and in cyberspace. Through these anecdotes, I illustrate classes of actors who either have a motivation to *shape* cyberspace, or who seem to have undergone a shift in power (up or down) by the emergence of cyberspace, and who are responding to or exploiting this situation.

Using various examples, we can start to catalog some of the means by which different actors can exercise influence in cyberspace, and as well understand the new actors that seem to have significant power to influence. At a high level, we want to explore three related questions.

- What are the tools of influence, both direct and indirect, and to what extent does cyberspace create distinctive behavior? Is there anything new?
- Are there new actors that appear as players in the space of influence—actors that a traditional state actor would not regularly expect to deal with?
- When influence is exercises, what actors are the preferred targets of that influence?

## 1.1 A catalog of the actors:

<u>The creators of cyberspace and the Internet.</u>

- Internet Service providers (e.g. ISPs like Comcast, Verizon, Level3, ATT, Cogent, etc.)
- Computing Service providers (e.g. Amazon Web Services, "cloud computing), etc.)

- Higher-level service providers (e.g. Content Delivery services such as Akamai, or Social network sites such as Facebook)
- Equipment suppliers to the above (e.g. Cisco, etc.)
- The rich supply chain behind them (chips, software, etc.)

### Private sector actors

Some of the actors in this category are established industries that have been strongly affected by the Internet.

- Telephone companies and their suppliers
- The music industry
- Radio
- The video/movie/TV industry
- "Brick and mortar" merchants of various sorts, such as book-sellers
- The "print media" industries: newspapers, magazines, etc.
- Publishing generally
- The advertizing industry
- Gambling, pornography and other marginal social activities.

Other actors (or activities) in this category include those that have emerged as a result of Internet/Cyberspace, for example:

- Computer games, massive multi-player games, virtual worlds.
- Online auctions (eBay, etc.)

### Governments

Governments, as the traditional actors on the stage of international relations, are clearly important in this analysis.

### International governance organizations

This special class of NGOs includes standards bodies, such as:

- IETF
- ITU

The category also includes actors concerned with governance of cyberspace, such as:

- Internet Governance Forum
- ICANN

### Illegitimates

This category includes classic crime categories such as confidence games, extortion, fraud, identity theft, etc. It also includes emerging state and non-state actors using tools such as terrorism.

<u>NGOs</u>

<u>Individuals</u>

One of the hypotheses of the ECIR project is that the Internet (and cyberspace taken broadly) seems to have shifted the balance of power toward certain actors, such as NGOs and the individual.  One of our goals is to look at these actors (and how they benefit from and influence cyberspace) in an attempt to validate or refute that point of view.

## 1.2 Shared concerns

A classic (and very oversimplified) catalog of actors and their interests positions *states* as cooperating or confronting each other in a global context, and the *state* and the *citizen* balancing their rights and obligations domestically. Using this model, we could collect the various concerns of the actors into three categories:

- Personal concerns: the concerns of the citizen within his regime of jurisdiction.
- Communal concerns: the matters that devolve to the state within each jurisdiction.
- Global concerns: the concerns that transcend national boundaries, and that may require states to interact among themselves.

A second hypothesis, central to framework put forward in this paper, is that a distinctive aspect of the "cyberspace" story is that since the essence of cyberspace is the interaction among groups of communicants, there is a further set of concerns I call "shared concerns", which characterize the process by which the terms of interaction are established in a way that meets the needs of all the parties to the extent that they are willing to interact.  Part of what is distinctive about cyberspace is the importance of these shared concerns, and the tools that both participants in the interaction and interested third parties use to influence how those shared concerns are resolved.

These shared concerns manifest directly when parties interact in cyberspace—issues such whether the parties must identify themselves to each other, whether the communication is to be kept private or revealed, and so on. Governments and other third parties (by which I mean parties that are not directly included in the interaction) are also concerned with how shared concerns are negotiated and resolved. For example, governments may want to carry out lawful wiretap independent of the interests of the communicating parties to have a private conversation. Rights holders such as the Recording Industry Association of America (RIAA) will be interested in preventing the unauthorized sharing of copyrighted material independent of the interests of the communicating parties to do so. And criminals will be interested in observing ongoing communication, pretending to be a party in a communication (a form of identity theft) and so on.

Taking into account the importance of these concerns, we now have five categories, the classic three I listed above, plus:

- Shared concerns: the concerns of the direct communicants in cyberspace.
- Third-party concerns: the concerns of those (outside the government) who would shape those shared concerns to their own objectives.

These concerns can speculatively be diagrammed as follows, where the boxes represent the concerns (and the actors that manifest those concerns), and the arrows indicate common patterns of interaction among the actors.

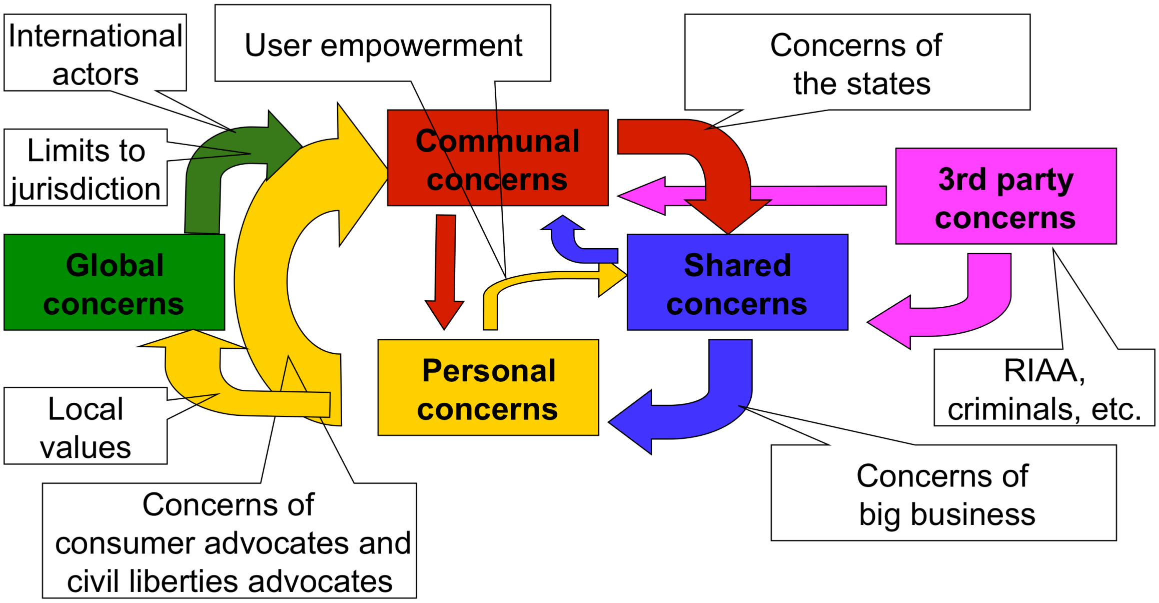

**Figure 1: A space of concerns and interactions**

Thus, we see the state, with its role to define and preserve the communal concerns that have been delegated to it, exercising influence over the way shared concerns are resolved. We see, in the interplay when individuals and larger actors (e.g. corporations) interact, a possible imbalance that causes the shared concerns to be resolved in a way that is in tension with personal concerns such as privacy. We see those personal concerns being "aggregated" by advocacy groups and brought to the attention of the state, with the goal of elevating them to communal concerns to which the state attends. And we see interactions at the global level involving traditional state-state issues (trans-border crime, national security) and as well cultural and social concerns that are much centered on the individual as on the formal state institutions, and which are elevated to the level of global concerns by the actions of individuals: benign activities such as blogging on cultural, political or "regional identity" issues, and hostile activities such as web site defacement and "patriotic hacking".

### 1.3 Selected case studies:

With this introduction, I will now explore a set of examples or case studies involving various actors important to the shape of cyberspace:

- Private sector actors influenced or shaped by cyberspace
- Individuals
- Businesses that operate "in" cyberspace
- Service providers
- Governments
- Application designers
- Non-state actors

# 2 Private sector actors affected by cyberspace

## 2.1 The telephone industry

The apparently stable telephone industry has been subjected to a number of shocks during the latter half of the 20th century, as first computing and then computer networking emerged, along with new forms of telephony such as cellular. In the United States, starting with the divesture of the local operating companies from ATT in early 1980s, the industry has been subjected to major restructuring. Divesture, of course, was not driven by computing or anything "cyber", but by a change in perception about the nature of competition, and the parts of the telephone system that might or might not be natural monopolies.

While approaches to competition and new technologies such as cellular have certainly disrupted the pre-existing industry, the Internet has been a very important driver of change. The telephone industry was perhaps the first major pre-existing industrial sector to "collide" with the Internet. Sometime in the mid-1990's it became clear that the Internet had the capability to carry voice, a capability that has become known as Voice over IP, or VoIP.  At the time, residential access to the Internet was dial-up service, which is not really fast enough to carry packetized voice, so there were doubts and differences of opinion about the importance of VoIP to the home. However, the technology out of which the backbone of the Internet was built was fast enough to carry lots of voice calls, so the use of an Internet backbone for voice was practical. This led to early technical innovation by small providers of VoIP, and as well to a number of strategic actions by larger actors.

### 2.1.1 Posturing about VoIP

In the early days of VoIP, the behaviors and actions were not about deployment so much as posturing.  Telephone companies, even as they expressed doubt about the technical feasibility of VoIP, declared their intent to convert over from circuit switched networks to packet switched networks. One reason to assert this was to try to drive down the cost of circuit switching hardware, which was much more costly (with perhaps much higher margins) than Internet routers. In fact, the conversion of the telephone system to a packet system may have as much to do with cost as with intrinsic superiority.

Another reason to declare that the future was packets was to escape from some of the regulatory burdens associated with the “old” circuit network. In particular, in the mid-1990s there was a regulatory transfer payment (“access charge”) from the long distance to local exchange carriers. The justification for this was that long distance was historically viewed as a luxury, but basic local phone service as a necessity. So a “tax” on long distance was imposed to subsidize local phone service. The tax was substantial—as much as $.25/minute. (Today, the actual cost of domestic long distance is less than $.01/minute.) The long distance providers concluded that if this tax were removed from long distance, then people would make many more long distance calls, which would make them more profitable. They argued that “packet-based” telephone service did not qualify as a service subject to this tax, so that if they converted they would no longer be subject.

In fact, it seems as if their goal was not to convert, but to use this assertion as a bargaining chip to drive the subsidy rate down. Behavioral evidence suggests that the FCC concurred in this objective, and did not reject the claims of the long distance providers. Over perhaps 10 years, this subsidy essentially went away, which may have deprived the local exchange carriers of almost half their total income. The costs of basic phone service presumably went up, and profits went down.

### 2.1.2 The curious case of the Telecoms act of 1996

In 1996, the Telecoms act of 1996 was passed, representing the first major overhaul of telecom legislation in over 50 years. It is notable in a number of respects. First, it almost totally failed to acknowledge the Internet. Second, it presumes that long distance telephone service was and would continue to be a healthy competitive service. Third, it presumes that the telephone industry would remain the monopoly owner/operator of circuits to the residence, thus ignoring the potential of the cable industry to be an effective competitor. All three of these core assumptions proved totally misguided.

Based on the assumption that the only useful data path into the home was the copper pairs of the telephone company, the Telecoms Act crafted a devil’s bargain, which is that if the incumbent local exchange carriers, or ILECs (or Baby Bells) would allow competitors to lease their copper pairs and sell services to the residence, the ILECs would be allowed to enter the long distance business. The FCC was empowered to determine when an ILEC had passed the “unbundling” test in a market and could enter that long distance market.  This act triggered substantial capital investment in so-called competitive local exchange carriers, or CLECs, which proceeded to flounder as the ILECs created various impediments to effective local loop unbundling. The ILECs challenged the legality of local loop unbundling, even though they had been a party to crafting the devil’s bargain, and finally the Supreme Court  ruled against the concept (although it is alive and well in other parts of the world), thus vitiating the bargain. At the same time the ILECs argued effectively that they should be able to enter the long distance market.

Inspection suggests that long distance service is a commodity business based on large, up front sunk costs, and that the market was in fact not able to sustain competition. The then existing long distance providers essentially all went out of business or exited the market, including MCI and ATT, leaving long distance as a service provided by the ILECs. (In most countries, the idea of a local exchange carrier and a separate long distance carrier does not exist.) At the same time, the ILECs found themselves facing a "facilities-based" competitor that they (and the law) had not contemplated—the cable industry. We thus see competition in the market that was presumed a natural monopoly (the provision of circuits to the residence), the failure of competition in the market where it was assumed to be sustainable (long distance voice), and the emergence of the Internet as a compelling service that the framers of the Telecoms Act had chosen to ignore.

While this story is interesting (and offers a cautionary tale about the wisdom of embedding in a law a presumption about where market failure will occur), it begs the question of whether anything *new* actually happened. The tools of engagement were quite traditional—legislation written by industry lobbyists, which often happens when the goal of a law is to balance the interests of industry players, litigation to challenge a law (even if your own lobbyists helped write it), incentives in law to encourage the deployment of private capital (essentially all of which was lost in the rise and fall of the CLECs, now almost extinct), and the use of a regulatory agency (the FCC) as the actual source of administrative rule-making and interpretation of the law (a large number of times).

Perhaps the two notable facts about this story are as follows. First, of course, this whole story is about who will control access to the home, and thus (even though the law failed to recognize the Internet) who will control the nature of the residential Internet experience. It was an attempt to shape the deployment of capital, away from facilities construction (in one point of view), and toward the creation of competitive service providers that would be beholden to the telephone industry for their actual circuits—the facilities. One of the major worries about the law was that it would not motivate investment in what came to be called "broadband", which has in fact been driven by competition from the cable industry, not by the CLECs using the copper pairs of the telephone industry.

The second notable aspect of this story concerns the interplay of the private sector and the FCC. Rulings by the FCC subsequent to the law were almost always challenged in court, which greatly slowed down any strategic moves by the industry conceived by the law (which may have had the side-effect of favoring the cable industry as it proceeded mostly unaffected by this tussle). However, the FCC repeatedly took advantage of an authorization in the law that allowed them to forebear from imposing regulation, which allowed them to "protect" the growing Internet from regulation and to seek its natural form free of regulatory presumption of what that form should be.

### 2.1.3 The specification of VoIP

In the early days of VoIP, some of us predicted that innovation in Internet-based telephony would occur along two paths, which would diverge and then (eventually) converge again. One path was the innovation in the features of the service offering once the end point did not have to mimic a "black phone" (sometimes called POTS), but could have new interfaces and computational power. Video, higher quality audio, logging, conferencing, etc. might appeal in the market. The other path would be the cost reduction of POTS-compatible VoIP.

Research tended to focus on the first path, since it seemed more novel, innovative and exciting. However, when the resulting work tried to make its way into the standards bodies, representatives of the phone company would participate and pull the standard back toward the alternative of VoIP that was POTS-compatible. It could be argued that this was because of a strategic desire to prevent the definition of any VoIP standard that would challenge the consumer's concept of what a telephone call is, or it could just be that the representatives from the phone company themselves could not conceive of any such thing. Whichever point of view you take, standards for innovative services were slow to emerge, either from the IETF or the ITU. Some of the most successful "human-to-human voice" applications arose not from standards bodies, but from company-specific innovation, such as Skype and Apple iChat. These systems do not attempt to interwork with any other Internet-based voice systems, and do not fully attempt to "replace" your traditional phone product. They just cannibalize the POTS market in passing. (It should be noted that the damage to the traditional wire-line voice business from these services is probably much less than the damage from mobile and from POTS-compatible VoIP. )

This story illustrates the use of the standards process by a "traditional" service provider trying to shape the new Internet experience to a) benefit their traditional model, and b) remove service innovation as a market differentiation. It is unclear if this effort slowed down the deployment of advanced services in voice, but it may have slowed down interoperable products.

### 2.1.4 Quality of Service

The development of tools for Quality of Service (QoS) in the Internet is an interesting "side-show" to the development of VoIP. The term QoS describes a set of technical mechanisms that can provides services suited to different applications. Applications such as VoIP and interactive games will benefit from a network service that attempt to control the latency of delivery (and the variation in latency, called *jitter)* across the network. Some bulk data transfer will benefit from a service that goes as fast as possible when the network is idle, but which defers to higher priority traffic if the network becomes fully loaded. The early work on development and standardization of QoS mechanisms was funded by various governments, as well as the private sector. QoS was integrated into many Internet products (e.g. routers) and is being used in some corporate intranets and private parts of the Internet, but it has not emerged as a product over the public Internet. The reasons for this failure are debated, but seem to include a lack of an economic model for cost recovery, and more specifically for revenue sharing among the various ISPs that make up the public Internet. Most recently, QoS has been seen by some not as a tool to improve the selective treatment of different applications, but as a tool to be used by ISPs with market power to degrade selective applications. Some proposals for regulation of the Internet, under the rubric of *network neutrality*, might limit or prohibit uses of QoS. It is possible that the government may prohibit the use of that which it paid to invent, although this outcome is perhaps an extreme and unlikely alternative in the current debates.

### 2.1.5 Generalization

The overall story of the telephone industry and the Internet is a story of a industry with a history of a low rate of innovation, protection of profitability through regulatory rule-making, and a tradition of being the 800 pound gorilla, encountering an industry with exactly the opposite features. It fought a war using tools that were conventional by its norms—lobbyists, regulatory pleadings, industry-wide deployment of capital, etc. Its attempt to preserve its traditional way of life had already been disrupted by divestiture, with which it was dealing poorly. But its actions, which were generally seen as stalling tactics and spoiling tactics, did not serve it well. Parts of the industry that had been seen as the ultimate "safe stock", like ATT, essentially went bankrupt (for many reasons, of which the Internet and "cyberspace" were only one). They lost market share to an industry (cable) that they could not bring themselves to take seriously. Competition and the pressures on margin caused them to vitiate their research labs (Bell Labs, ATT labs), which had both been their source of innovation and a crown jewel of U.S. industrial research. Those companies that survived (e.g. Verizon) came out transformed, and in no way resembling their earlier form (New England Telephone). Whatever tools of engagement they used, those tools were not (at least in the long run) successful in protecting their corporate goals. The new-comer's tools: tools of innovation, of "engineering around" regulation, and of venture-backed investment seem to have been the effective ones, both in shaping the Internet and in shaping the survivors.

For all of the efforts of all the parties, it seems as if the Internet did not change in major ways. It now has a new application, VoIP, which is not a novel event. QoS, which was thought to be an important bit of enhancement to the infrastructure, has not happened, and while VoIP over the public Internet may offer slightly lower quality as a result, the natural growth in Internet capacity over time has made VoIP viable without QoS. Perhaps the most significant change to the Internet has not yet played out—the movement of interactive voice communication to the Internet drew the attention of law enforcement and intelligence agencies, who realized that they no longer had the technical means to carry out lawful intercept, more commonly called "wiretap". Pressures to augment Internet technology with tools for wiretap will lead to contentious debate, and might end up shifting the locus of control over communication is major ways. I return to this circumstance later.

## 2.2 The recording industry—the story of music

The recording industry, perhaps like the telephone industry, did not at first recognize the disruptive potential of the Internet. It strongly resisted the creation of a legal distribution channel for music across the Internet (presumably to preserve the existing distribution channels) and when illegal music sharing emerged, instead of taking this as a wake-up call as to what their customers wanted, they tried to stamp it out. The resulting battle (which is often told as the story of Robin Hood and the Sherriff of Nottingham) alienated a generation of music consumers, and validated the idea of music sharing as legitimate misbehavior. (Like speeding, if everyone does it and the norm is misaligned with law, it is very difficult to impose control. The music industry, in my view, facilitated the emergence of this new norm by their retro actions, and now has to live with it.)

The music industry has a long history of effective lobbying in Washington to preserve their objectives, specifically the protections provided by copyright. Their first tactics, when faced with the threat of the Internet, was to turn to this traditional tool for them, as well as to technical tools to control (prevent) copying and other forms of theft.

### 2.2.1 Digital Millennium Copyright Act (DMCA)

Much has been written about the DMCA, and many points of view have been offered. This is a very brief and possibly slanted view. A major goal of the DMCA was to make it illegal to reverse-engineer and "break" technical means designed to protect material covered by copyright. Protection schemes such as regional locks on DVDs, or the use of encryption to protect broadcast (e.g. by cable or satellite) of copyright material were regularly (and quickly) broken. This law made that illegal.

One of the effects (whether intentional or accidental) of the law was to make various sorts of research illegal—research that tried to understand how the Internet actually worked by trying to dissect the parts. The law has been used (variably and with variable success) to repress the publication of various papers and the distribution of various sort of software. Since software for illegal sharing of music has as often as not emerged from the academic research community, the music industry does not have much sympathy for research, and the dislike is mutual, which fosters the Robin Hood mentality.

One of the consequences of this, of course, is that the "hacker innovation" of reverse engineering has moved overseas, and the rights-holding industries have lost access to the research community as an asset in their quest.

I do not know that there is anything unique about "cyberspace" in this story, except that it is a story about technical innovation vs. preservation of the "old ways". It illustrates the tension between law-making on the one hand, the jurisdictional limits to law on the other hand, and technical innovation on the third hand. It is worth noting that the U.S. advocacy of the strong commercial interests centered around the entertainment industry and "Hollywood" are often not well-received overseas, where artistic creativity is more seen as a cultural than a commercial undertaking.

The U.S. has not been very effective in pushing its point of view at the multi-national and diplomatic levels, and copyright enforcement is spotty overseas, which makes the "flight from law" easier. The U.S. works to find an effective way to deal with this, which spills over even to discussions about theft of industrial intellectual property. It could be argued that the "industry-created" norm of Robin Hood theft from the entertainment industry has weakened our ability to negotiate more broadly about IPR, but I cannot substantiate that speculation.

### 2.2.2 Private sector subpoenas

Part of the battle over online music centered on the identification and confrontation of those who offer to share copyrighted music. The DMCA crafted another devil's bargain between the ISPs and the music industry[1]. The ISPs (and those who host content for others) wanted to avoid the risk of contributory liability, and sought protection somewhat like common carriage. The result was the "takedown" doctrine, in which an ISP or hosting provider is free of any burden of liability if they will agree to accept and respond to a "takedown" notice, and remove offending content or compel their customer to do so. (e.g. on pain of disconnection). The ISP also was obligated under certain circumstances to reveal the identity of the customer hosting the offending content, in order to facilitate lawsuits and other direct actions.

The ISPs may not have been happy with the idea that they could be compelled to "turn in" their customers, but because it was a legal requirement they could comply without having to make any judgments, which shifted the burden of judgment away from them. In this respect, they liked the clarity of a court order.

I think the specific nature of the Internet both triggered this problem and shaped the tools of engagement. The Internet offers a degree of anonymity and "action at a distance" that invites marginal anti-social forms of behavior. It would be interesting to see if we can find any scholarly study of the rise of music sharing, and the norms that surround it. The music industry only slowly tried to shift or counteract the emerging Robin Hood norm, by putting the creative artists (as opposed to the reps for the distribution channels) in front of the consumers in PSAs and the like, and by allowing the emergence of legal distribution channels such as iTunes.

### 2.2.3 Generalization

The music industry may have been transformed forever. The loss of the revenues from the high-margin distribution channel may mean that the music industry can no longer "spend a person into stardom", as they did with created figures like Madonna. The era of the high-profile super-group may be over. The era of the creative artist earning a working living by direct engagement with his/her audience through the Internet may be one of the most significant emerging phenomenon, and a damaging

[1] The Online Copyright Infringement Liability Limitation Act, part of the DMCA and sometimes referred to as DMCA 512.

outcome from the perspective of the music industry.  The retail distribution channel has seen major bankruptcies.

While the international dimension of this may initially seem less that consequential from the point of view of national security, I that the consequences may radiate further than one might think, and (at a minimum) illustrate the limits on the ability of the U.S. to put forward a U.S. industry point of view internationally.

## 2.3 The PC industry and broadband

The PC industry (typified by Intel for hardware and Microsoft for software—Wintel for short), grew up in a world of limited regulation and relatively unfettered investment and innovation. In the late 1980's or perhaps 1990, these players had a troubling insight, which was that the high-end customer for their products was no longer the business world, but the consumer, with his appetite for games, video, and other sorts of high-end image rendering. These "high-end" experiences were tied directly to the availability of broadband access to the Internet, so their industries were dependent on another industry sector (broadband access) with whom they did not have any traditional business relationship (customer, strategic partner, ownership, etc.)  This realization led to a series of actions by the Wintel alliance to drive the deployment of residential broadband.

Perhaps the most notable, given their past history of limited regulation and disdain for the actors in Washington, was their decision to come to the government and call for a national initiative to drive broadband internet deployment. Whether the specific outcome was use of public sector funds, or incentives of other sorts (e.g. tax credits), or just an increased national visibility for the objective, debates over broadband policy suddenly became highly visible in Washington.

Another tack was to try to use the regulatory machinery (both state and federal) to compel the deployment of broadband (at the time, ISDN) by phone companies. This led to some very perverse behavior on the parts of certain ISPs, such as pricing models for ISDN that actually discouraged consumers from buying the product, and filling unused underground ducts with concrete to render them useless in case the regulators tried to force them to deploy new products.  The use of the tools of regulation by one private sector player to influence another private sector actor did not make friends across that interface.

The ISPs responded by asking Wintel to make capital investment in broadband deployment, which (I am told) was an idea most regrettably ridiculed by the Wintel folks, again making no friends.

Another approach was to send a "broadband evangelist" from Wintel to hector the representatives of the technology office from the various telephone companies. It is not clear if this made any difference, but it did serve to keep the issue in front of the phone companies.

A final approach taken, in particular, by Intel, was to build prototype hardware (e.g. cable modems) to demonstrate feasibility, with the declared intention (on which they made good) to exit the market if the traditional supplier to the cable market would step up with products of their own. The also agreed to forward-price key components (e.g. DSL chips) if the telco and cable companies would make volume commitments. (With 110M U.S. homes, volume pricing is important here.) In fact, Intel does not dominate the market for chips in this segment—the chip that makes up a cable modem comes from a company named Broadcom. But Intel, off the record, expresses satisfaction with this outcome: the margins are low on that chip, and it stimulates sales of high-margin processor chips.

While the market for Wintel is obviously international, to this point the action between Wintel, governments and broadband suppliers has been seen as a local domestic issue in each country. There do not seem to be international issues that rise to a significant level. At a secondary level, or course, multi-national actors like the OECD track broadband deployment in the OECD countries, and try to position broadband deployment as some sort of multi-national horse race. Claims of the sort that "the U.S. is 20th in broadband penetration" are used to whip up interest in public sector involvement. (It would be interesting to discover, who (e.g. which countries and which agencies within which countries) encourage the OEDC to track this data. )

### 2.3.1 Generalization

These stories illustrate that in the capital-intensive parts of cyberspace, one exerts influence in large measure to the extent one expends capital or influences how it is expended.

Perhaps the factor that is distinctive about this story is not that it concerns cyberspace, but that it concerns companies that are mutually dependent but that do not sit as buyers and sellers in a common value chain. Another factor is the need for substantial capital. Certainly, the objective of the actors here was to change the shape of cyberspace—specifically to accelerate the deployment of residential broadband. In retrospect, the technical approach was tactically wrong (ISDN was not a success in the market) but perhaps strategically useful. Wintel did not make friends in the telco space, but those issues fade with time.

These stories illustrate interactions among private sector companies to try to shape cyberspace, but they do not illustrate the use of new tools of engagement created by cyberspace. In fact, the tools of engagement used by these traditional actors seem very traditional. To find examples of the use of cyberspace as a tool of engagement, we might be better off to look at those who appear to have been empowered by the emergence of cyberspace, which include the individual, NGOs, and certain classes of illigitimates.

# 3 The individual and his place in cyberspace

## 3.1 The user as creator

### 3.1.1 Peer production—Wikipedia and its kin.

Much as been written about this phenomenon. In particular, the book by Benkler[2] is a good starting point. The utility of cyberspace as the platform that allows various sorts of collaborative production is well-understood.

How has this influenced cyberspace? Is there evidence of "influence"? When individuals act individually, one would not naturally expect to see intentional influence. We will either see influence because the individuals have been marshaled for a cause by the designer of the activity, or emergent shaping of cyberspace.

Wikipedia is a designed activity. Its cause was not to reshape cyberspace in any technical sense, but to shift power away from controlling editors and to the people. It was to inspire people to put forth effort by giving that effort an outlet; a reward for that effort. It is a demonstration (one of many) that simple economic rewards are not the only ones for which people will strive. In this respect, it is a cause that is deeply radical from the perspective of the traditional, economically-based content producers. It demonstrates a hypothesis that cyberspace may be a tool that can generate great social good that is difficult for a traditional economic actor to appropriate. Social value may go up, but "money generation" may go down.

Secondary consequences of systems like Wikipedia are to sensitize users to the issues of intellectual property rights, and to lend support to projects such as the creative commons, which (again) has as its cause the movement of control from the traditional rights-holders to the individual creators of content.

### 3.1.2 Peer-to-peer content sharing

The sharing of music, video and the like could be taken as an emergent social phenomenon. It was nucleated, of course, by the creation and dissemination of free software for the purpose, but the magnitude of the phenomenon seems to dwarf the predictable consequences of the programs. This phenomenon was discussed above, but it is worth noting that this collective behavior has actually changed the shape of cyberspace, by putting increased demands on the "upstream" access capacity of broadband access links, and by shifting the patterns of use more broadly in ways that made ISPs re-engineer parts of their networks.

### 3.1.3 Flash crowds

The use of texting and Twitter to organize protests, gatherings and other sudden mass events is another example of emergent social behavior that was probably not contemplated by the designers of the technology.

[2] Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press (2007)

### 3.1.4 The many faces of Facebook

Facebook is a Web-based application that has been wildly successful, connecting tens of millions of users in a massive social network. There are a number of ways to look at Facebook.

First is the idea of the movement of the personal context into cyberspace so that computer-based activities there can be shaped by that context. If my social network is on line, and not just in my head, then activities in cyberspace can take this context into account and shape themselves accordingly. We will worry about the consequences as the computer makes clumsy decisions about how to interpret the context (for example, privacy concerns), but it is a major shift.

Second is the idea of the user-constructed artifact, of the sort discussed above. The social network built inside Facebook is a massive, peer-produced artifact that, again, seems to dwarf the magnitude of the software itself.

Third is the emergence of an online identity in which the user has made a social investment, so that it is costly to abandon. As we worry about the issues of identity, privacy, freedom of action and accountability, we will have debates about what sort of identity offers a good balance among these concerns. A government-issued ID is robust, but raises many concerns about tracking, etc. The self-constructed identity one builds in facebook may be a much closer analog to the way we manifest ourselves in the real world.

Fourth is the question of who owns my social network. Facebook centralizes this within the system, and as a result owns my social network in practical terms. An alternative would be a set of open standards to build a cross-provider social network, which might bring a greater social good but less monetary returns to appropriate. The standards of the "Open Social" project[3] illustrate this alternative.

Fifth, and related to the above, is the context of the social network as a platform (whether open or more closed and controlled) for third party innovation—an illustration of the characterization of cyberspace as a recursive layer-cake of platforms, each with its own character of openness, flexibility, stability, economic implications and the like.

Sixth is facebook as an example of the more general phenomenon of meta-data: data in cyberspace that describes something else. It could describe other data, or (in the case of facebook) the user. The emergence of meta-data warrants a separate discussion.

[3] See http://www.opensocial.org/, visited 12/31/09.

## 3.2 Shaping cyberspace by citizen participation in self-reporting

### 3.2.1 Broadband

While the large traditional actors (e.g. Wintel and telco) may have used traditional tools to engage each other over the shape of cyberspace (and in particular the deployment of broadband), other actors have used the Internet directly to reach out to and invite participation from the citizenry. One mode of involvement is to ask users of the Internet to measure the performance they actually get (and report this to a central logging site, along with which provider they use. This approach has been used by the private sector, e.g. the site run by the Communication Workers of America[4], and by the public sector, e.g. the broadband mapping site run by the state of Massachusetts[5]. The CWA site performs a speed test for the user, then compares the results with those of other users and other averages from other countries, and then asks "Disappointed with your speed? Tell Congress. We need a national high speed Internet policy". They provide a draft letter you can send to your representatives in Washington[6].

The invitation to use the Internet as a tool to express an opinion is not novel, but the mix of allowing the user to first measure his own experience to shape that opinion is more interesting.

### 3.2.2 Tracking of content blocking and filtering

The Herdict project of the Berkman Center allows individual users to report instances where they cannot reach specific sites/content on the net. These activities serve several related purposes, to gather data at a scale otherwise hard to do, to generate information that shines a light on behavior deemed inappropriate, and to elevate citizen awareness of blocking as an issue by involving them in the process of tracking and reporting.

# 4 The individual and the business

When individuals (often like-minded) interact in cyberspace, whether the interaction is simple communication (e.g. a phone call) or more complex interaction (e.g. augmenting Wikipedia), the alignment of interests tends to produce harmonious sorts of outcomes in what I am calling the resolution of the shared concerns. However, the interactions we often see are between an individual and a larger, typically corporate actor: online commerce, information outlets, search, and the like. And often, interaction among individuals is mediated and shaped by a corporate actor interposed "in the middle": Facebook, Twitter, etc. The interests of all these actors—the corporate and the individual—may not be so well aligned. If

[4] See http://www.speedmatters.org/, visited 12/1/09

[5] See http://maps.massgis.state.ma.us/broadband/broadband_survey_map.htm., visited 1/2/10.

[6] See http://www.unionvoice.org/campaign/highspeedpolicy, visited 1/2/10

they are sufficiently at odds, the interaction may not occur. But what we see today is interactions of sufficient value that they are completed, but with some suspicion on both sides. These interactions tend to produce a different sort of outcome in the resolution of shared concerns. In particular, since corporate actors are normally seen as having more power in any negotiation that occurs about the resolution of shared concerns (whether that negotiation is explicit, or is of the implicit "take it or leave it" sort), other actors can be found intervening to try to balance the outcome as these interactions are framed.

## 4.1 Privacy and revelation

Many websites ask the visitor to reveal various things about them as a condition of participation. This revelation is justified on the grounds that it allows the web site to better serve the visitor, and it also serves the interests of the web site, most commonly in that it allows targeted advertising. Information may be implicit (e.g. a web site can estimate the physical location of a customer with very high accuracy using only the IP address of the visitor), or as a side-effect of actions on the site (e.g. Amazon tracking past searches and purchased to make recommendations, or explicit (where a visitor may be asked to give a zip code, age, or SES quantifiers.

All of these actions raise concerns about privacy, which the visitor individually does not have much power to negotiate. Privacy policies are long-winded and vague, and threaten great degradation of service if the user chooses to take advantage of any offered "opt-out" alternatives. This has led various groups that advocate for the concerns of citizens to push governments to lay out ground rules for the scope of resolution of privacy concerns in cyberspace. (In the language of my diagram, to elevate individual concerts to the status of communal concerns in order to bound the negotiation over shared concerns.) For example, in the U.S. the Electronic Privacy Information Center (EPIC) states as its goal "Focusing public attention on emerging privacy and civil liberties issues". Their tools of engagement, as indicated on their web site, include litigation, the filing of complaints and amicus briefs, and aggressive reporting.

### 4.1.1 The P3P initiative of the W3C

Another approach to dealing with the negotiation of shared concerns about privacy is the Platform for Privacy Preferences (P3P)[7] project of the World Wide Web Consortium (the W3C). The P3P protocols allow a browser (representing the interests of a user) and a web site to negotiate automatically about the wishes of the two parties with respect to privacy issues.

### 4.1.2 TOR

The TOR system is designed to allow anonymous browsing. It is the current embodiment of a concept called Onion Routing, so called because a message from a sender to a receiver is sent indirectly through a series of helpful intermediate nodes. The message is encrypted multiple times by sender, using the encryption key of

[7] See http://www.w3.org/P3P/, visited 1/1/10.

each intended intermediate node in turn. Each intermediate node "undoes" one of the encryptions, revealing the address of the next node, and then modifies the message to hide the source address. So no node along the path can see both the original sender and the ultimate receiver. The image behind the term "Onion Routing" is that at each stage, the intermediate node peels one layer (of encryption) off the message.

Onion routing is clearly a "tool of engagement" designed to protect the privacy of individual users from the monitoring and control of actors (such as ISPs and their masters) who can observe the packets passing through the network. There are two interesting points about TOR, and the concept of onion routing. The first is its origin: it was designed by U.S. government researchers, specifically at the Naval Research Laboratory. The government itself sometimes likes to be anonymous, for example when looking at the web sites of terrorist organizations. Second, TOR is an example of a "peer-produced" artifact, in the spirit of Wikipedia or social networks. A large collection of intermediate nodes is required to make TOR work, ideally scattered across many legal jurisdictions. In practice, these are contributed by different individuals and organizations across the globe, who add a node to the TOR system in order that the world have a anonymity system. By making the system available to anyone, the U.S. government gets a global platform it can use itself.

## 4.2 Other examples

Here are some other examples of issues that arise in the resolution of shared concerns when individuals interact with other entities.

**Authentication of the service**. While the user might wish to negotiate that a web server use a secure encrypted protocol, as opposed to sending the web page in the clear, the protocols do not allow this to be negotiated. The decision rests solely with the web server. This decision affects both privacy and authentication—unless secure protocols are used, a connection from a user to a server can be redirected to a substitute (false) server with no easy way to detect the mis-direction. For example, CNN does not use secure connections, so the consumer has no assurance that they are talking to the real CNN. The consumer has no power to negotiate this.

**Advertizing**. Many Web sites contain advertisements. A few web sites allow a user to negotiate a fee to have the ads removed[8], but for most, the ads are mandatory. This leads to an arms race in which motivates consumers download programs that strip ads out of the web pages as they are delivered. This action is not just a convenience, but a security measure. Most web sites that host ads do not directly negotiate with the advertisers, but work indirectly through ad aggregators. This means that they do not have control over exactly which ads appear on their page. If the site hosting the advertisement is malicious or insecure, loading the ad can download malware, which can cause the computer visiting a apparently trustworthy

[8] For example, www.wunderground.com, which charges a modest $5/year to remove all the ads.

web site to be corrupted. This example is only a small part of the “advertising story”, a complex value chain of actors who do not necessarily trust each other.

# 5 Direct action in cyberspace—the strategic role of the ISP

Internet service providers, or ISPs, play a critical and distinctive role: by their collective investments and their operations they create what comes to be the Internet. They are competitors but they must cooperate. They want to achieve a return on their investments, but that goal may sometimes be at odds with the basic nature of the Internet that they create (or so some may argue)[9]. While some idealists might hope that the ISP could be viewed only as a passive carrier of packets between end-points, in fact the ISPs are active players in defining the rules of engagement in cyberspace.

## 5.1 Peeking is irresistable

One recurring area of contention is whether the ISPs have the right to look at what the users are sending. There are parts of the packet at which they have to look, of course; they have to examine the address on the packet to see where to send it. The analogy that has been used is that of an envelope—they can look at the outside but not open it. However, another analogy is a post-card—all parts of it are visible. In a technical sense packets are more like post-cards, unless the contents have been encrypted. And the temptation to peek is substantial.

A limited form of peeking is to look at another part of the packet header, the port number, because this give a hint as to the application the end-point is using: Web, VoIP, file transfer, video, etc. ISPs argue that looking at this information is valuable because it allows them to build models of behavior to better predict user demand. However, this information can also be used to track forms of behavior that might be deemed unsuitable by one or another party, and perhaps block or degrade them. In response to this possibility, some new applications (such as some peer-to-peer file sharing applications) intentionally randomize the port numbers (which is consistent with the Internet standards but not previously common practice). This sort of action makes it harder for ISPs to determine what the users are doing, and presumably harder for others (such as regulators) to determine the same facts.

A more substantial sort of peeking is to look inside the payload of the packet (as opposed to the header) and look at such things as the URL of the Web page that a user is retrieving. By doing this, the ISP can learn a great deal about the behavior of the user, and potentially map the user into one or another demographic category. This sort of information can be used to improve the selection of advertisements

[9] Of course, there are non-commercial actors that implement parts of the Internet, including universities, corporations building networks for their internal use, and governments. This discussion focuses on the actors that sell Internet service as a commercial undertaking.

delivered to the user, which in turn sustains a higher price per ad impression. (This illustrates another aspect of the "advertising story".)

In response to this sort of peeking (which is properly called Deep Packet Inspection or DPI), there have been calls to prohibit this sort of behavior, a clear example of what I have called the aggregation of individual concerns in order to elevate them to communal concerns. ISPs have tried to mitigate some of the fears about this sort of peeking by delegating the task to a third party (e.g. companies such as Phorm and Nebuad), but this tack has not been sufficient to still the protest over this sort of behavior. The web provides a rich source of information about these two companies and the protests they have triggered. The shape of the tussle is a classic example of the interactions illustrated in my figure: the ISP used its privileged role as a large, dominant actor to try to impose this outcome on the consumers, and the consumers elevated their concern to a communal concern and sought protection from the government.

## 5.2 Should they control?

The telephone companies have the legal status of common carriers. This concept in law goes back to the middle ages, and has been used to define the responsibility of actors as diverse as inn-keepers, truckers, and telephone companies. In brief, common carriers are obliged to serve all comers, and in exchange are given protection from the potentially illegal actions of their customers.

Internet Service Providers in the U.S. are not deemed to be common carriers under the law. This means that they can pick and choose their customers, potentially limit what their customers want to do, but might acquire some liability for what customers do. U.S. ISPs have worked hard to obtain legal protection from the mis-behavior of their customers (e.g. the DMCA with respect to music sharing), but have avoided being classified as common carriers. In fact, almost all ISPs today do examine and block certain traffic—for example certain ports (see above) are associated with applications that are essentially never used but which represent security vulnerability. Traffic to these ports is very commonly dropped. (And this fact does imply some peeking).

However, when ISPs are seen to exercise more explicit and visible control over what their users are doing (e.g. the recent case of Comcast disrupting BitTorrent transfers), there are calls for regulatory or legislative intervention. The terms "network neutrality" and "network management" are associated with this current debate.

While there are many reasons to worry about "non-neutrality", the one most often put forward is that an ISP may block or degrade the traffic of certain applications (or certain application providers) because the ISP has a similar offering that competes with the one being blocked.

## 5.3 Other actions open to ISPs

Because ISPs control topology, the computation of routes, and packet forwarding, there are many other actions they can and do take that define the nature of cyberspace.

- **Selective routing and duplication/deflection of traffic**. ISPs, either by modifying the behavior of their DNS servers, or by modifying their routing and forwarding mechanisms, can intentionally "deflect" traffic so that it does not end up where the sender intended. This intervention (if in a somewhat benign form) is common, as when a user at a hotel or WiFi hot-spot starts their browser, attempts to go to any web page, and ends up at a page requesting payment.
- **Negotiation of interconnection agreements with other ISPs.** ISPs compete, but they must interconnect if the Internet is to function as a global system. The process of negotiation among ISPs is complex, and can lead to a range of outcomes variably beneficial to one or another of the parties. The large ISPs can have a significant influence over the cost structure of the smaller ISPs. This is a form of inter-actor engagement within one family of actors, but a similar sort of negotiation occurs when content producers bargain to connect to ISPs.

This discussion of ISP power is very U.S. centric. The International landscape is discussed below.

## 5.4 The Domain Name System (DNS)

The Domain Name system is critical to the operation of the Internet. It provides the service by which domain names (such as mit.edu), or the names in URLs are translated into Internet addresses. The system was designed to be highly decentralized and hierarchical. The top level of the DNS (the "root") is operated by a collection of commercial and volunteer actors. Many of the Top Level Domains (TLDs), such as .com or .org, are operated by commercial, for profit entities. Other TLDs, such as the country code TLDs, may be operated by an agent appointed by the government in question. The lowest level servers, where queries are usually first sent for resolution, are usually operated by the ISPs that provide Internet access for the customer. Each such server is a significant point of control for its operator.

In the early days of the Internet, the function was thought to be very simple—a mapping from a character string to a number. However, over time the DNS has been used by a number of actors for a variety of more complex purposes. Owners of names (e.g. the name "google.com" or "mit.edu) may set up the DNS to give different answers depending on who makes the query and where they are located. Thus, looking up the name "google.com" in different countries will often direct the user to the address of a server specific to that country, in the language of that country.

One of the most contentious aspects of the DNS was the realization that names can have monetary value. Owners of names that correspond to trademarks view those names as valuable, and will both pay to use them and fiercely defend their misuse.

The transition of the DNS from a volunteer service run by the research community to a commercial service has been rocky. When the U.S. government orchestrated the transition of the DNS away from the research community, they established an organization called the Internet Corporation for Assigned Names and Numbers, or ICANN. ICANN found itself in the position of controlling the revenue opportunities of other actors by the decisions it took with respect to the authorization of new names.

In particular, the creation of new Top Level Domains, or TLDs, has tremendous revenue implications.  We are familiar with the TLDs com, edu, org, and the national country codes. ICANN asserts that it has the right to control whether new names are created. When a new name is created, for example biz, or info, trademark holders are motivated to claim their names in those new spaces, for which they pay. So each new TLD is a money-making opportunity for the organization that controls it.

Other issues have been challenging for ICANN, such as the decision as whether to allow TLDs in other character sets than the English alphabet used by default in the early Internet. If such names are allowed, it might either create yet new revenue opportunities, or the name might be restricted to be a mirror of a name in the default alphabet (e.g. country code names in the native character set of that country. Some organizations have started to register TLDs in international characters, to some extent as a protest over ICANN's actions in the area[10].

ICANN's power to control the DNS is tenuous.  Some operators of DNS servers have added new names to their server, without waiting for ICANN to act. Such action is variously seem as a legitimate response to the autocratic and illegitimate power asserted by ICANN, or the beginning of the unraveling of the global coherence of the Internet. Passions run high.

A particular version of modifying a local DNS server is called *redirection.* The term describes a circumstance in which a DNS has been modifies so that a name (often a name that does not belong to any legitimate user) is translated or resolved by the DNs server into the address of a server. One reason to do this is financial. If a user mis-types a name (say by typing ww. Instead of www. at the beginning of a URL, he can be directed to a page with advertizing relevant to the name he was trying to type. Another reason to do this is a part of securing the Internet—some botnet infections try to connect to their controller by looking up an un-registered DNS name. By redirecting such names to a monitoring page, security researchers can track the progress of a bot-net infection. The extreme form of redirection (which is normally not implemented by a commercial ISP, but seems to have occurred at locations such as hotels) is to redirect legitimate and popular DNS names such as Google.com to a different server which then passes data between Google and the client. In the security community, this is known as a "man in the middle attack", since it allows the machine in the middle to observe and modify any part of the

[10] See, for example, http://www.idru.org/, visited 1/2/10.

communication without easy detection. There is much contention about redirection[11].

## 6 The government as an interested actor

Governments have many objectives, and have many tools at the disposal. Many of the tools are "traditional", in that they do not seem to exploit the specific features of cyberspace—they are the tools that include policy-making and legislation, investment in R&D, procurement standards, and the like. However, governments can act directly in cyberspace, and can (depending on the law in any particular country) compel direct action by other actors.

### 6.1 Direct power—the use of force

The military organizations of many countries are now exploring the options for the direct use of power in cyberspace. The most obvious tools today are denial of service (DoS) attacks on cyber-resources, infiltration of resources as a means both for espionage and for direct disruption as a part of an offensive action, and physical attacks on critical cyber-resource. The distinctive nature of cyberspace raises some questions about the appropriate application of the laws of war, a issue which is under active study at this time.

### 6.2 Other direct uses of power—control of domestic actors

Within any country, the state can exercise its powers (legislative, regulatory, etc.) to impose mandatory obligations on their various domestic actors related to cyberspace.

Most obviously, almost all countries now have Internet Service Providers and almost all have domestic content hosting services. These actors can be required to take such actions as turning off the Internet at times, releasing to the state information related to customer identity, what content is being retrieved, and the like.

#### 6.2.1 Domestic surveillance

Governments may attempt to compel ISPs to log or monitor online behavior on their behalf. For example, in the U.K. there is a proposition (put forward by their GCHQ) to install DPI devices in ISPs to log user data[12].

#### 6.2.2 Blocking content—blocking access

In a number of countries, ISPs have been required by their government to block access to the Internet, or to certain Internet sites or applications. As a recent example, China shut down Internet service in a region where there was ethic unrest.

[11] See, for example, http://blogs.techrepublic.com.com/networking/?p=1012, visited 1/210.

[12] See, for example, http://www.theregister.co.uk/2009/05/03/gchq_mti/, visited 1/1/10.

The efficiency with which the ISPs executed this requirement made clear that they were prepared to do this—the relationship between the government and the ISP seems to be rather more entangled in China than in the U.S. Another example is the blocking of YouTube videos in Thailand as part of a dispute over an insult to the king of Thailand. Again, the Thai ISPs moved to carry out this order without any tension that was visible to the outside world. Many countries seem to view ISPs as obligated to carry out the mandates of the state.

Some attempts to block access to content have an international component. On the occasion of the posting on YouTube of material deemed offensive to the king of Thailand, the Thai government demanded that YouTube remove the content worldwide. YouTube did agree to block access to the content to users inside Thailand, but would not agree to any broader demands. Thailand responded by instructing their ISPs to block access within Thailand to all of YouTube. This situation persisted for a while, until the larger matter of the insult was negotiated. It is not clear if the world or the Thai citizens were more harmed by this blockage. This example illustrates a country attempting to exercise influence at an international level by their control over actors within their borders. In general, efforts of this sort have not been too effective. As I discuss below, to the extent that governments have influence in the space of international cyber-relations, it will be indirect.

## 6.3 Government influence over higher-layer trans-national actors

The mention above of YouTube reminds us of an important class of actor in this space, the providers of "higher-level" service—not the ISPs but companies like Google, Facebook, Flicker or Twitter, or content delivery networks like Akamai. These companies often have significant national presence within many countries, and can thus be subjected to local control. However, over-aggressive attempts to exercise this sort of influence can have the adverse effect that the company in questions removes all its presence (staff and equipment) from the country. Such an action does not remove the influence of the company from the country, since the Internet provides trans-national access unless it is specifically blocked. The consequence of a company exiting a country may be an increase in the ease of blocking the content (since it now comes over international circuits) but also a substantial increase in domestic costs (since the international circuits are usually the most expensive in the Internet). The result may be a tussle between political values on the one hand and cost-effective operation on the other hand. However, both the transnational corporations and the nations will explore what tools they have in this emerging space. This tussle space may be one of the more distinctive of those that arise in cyberspace, even though the goal is often only a change in domestic behavior (e.g. blocking the sale of Nazi memorabilia in France), rather than a broader goal of international change.

## 6.4 The government's role in the creation and shaping of the Internet.

The U.S. government, of course, played a critical role in the initial creation of the Internet, by funding the research that made it happen. The initial funding came from

ARPA, a research organization within the Department of Defense, and later funding came from the U.S. National Science Foundation. In the U.S. it is hard for the government to try to set a research direction using the NSF, because the NSF by policy is a somewhat independent foundation setting its own research objectives, based on community input. In other countries, goverments find it easier to translate their objectives for the future of cyberspace into mission-oriented research programs.

### 6.4.1 The U.S. attempt to slow the deployment of encryption and facilitate wiretap

This story is a long one, and well documented in sources such as the book by Diffie and Landau[13], and the PhD thesis by Hung at MIT[14]. In short, the U.S. National Security Agency, working together with other agencies interested in maintaining the ability to carry out surveillance and lawful intercept, used a variety of tools to slow the commercial deployment of Internet encryption. By classifying encryption as munitions, they were able to use the International Traffic in Arms Regulations (ITAR) to prevent the export of software that incorporated encryption. Most vendors, unwilling to maintain two versions, domestic and export, chose (at least for a while) not to include encryption. As the pressure for secure communications increased, they argued for "key escrow", in which parties would voluntarily give their keys to the government (under a formula designed to provide protection) so that they could be obtained with a court order. This approach was contentious and unpopular, and seemed to make no sense in the larger, international arena. Recognizing that software incorporating encryption was becoming more widespread overseas, and bending to pressure for more secure domestic communication (in particular in support of commercial development of Internet-based e-commerce), the NSA and their partners essentially reversed position and dropped any effort to slow deployment.

However, they maintained a strong interest in being able to carry out lawful intercept, or wiretap. In particular, for Internet-based phone calls, or VoIP, they have fought hard to maintain the capability they have with the traditional telephone system.

An early approach was to approach the IETF, and request that the IETF develop standards that defined how the Internet could be "tapped". They were rebuffed in this effort, as documented in an interesting IETF RFC, where the IETF stated that they were an international body, not just a U.S. body, and they did not want to be seen as bending to a U.S. centric policy to shape the Internet[15]. In response to this rebuff, the government approached the goal via two paths. First, they developed a

[13] Diffie, Whitfield, and Susan Landau. *Privacy on the line*: *The politics of wiretapping and encryption.* MIT Press. Second edition 2007.

[14] Hung, Shirley. *Managing uncertainty: foresight and flexibility in cryptography and voice over IP policy.* PhD, MIT Political Science Department, 2008.

[15] See Internet RFC 2804, IETF Policy on Wiretapping , May 2000.

multi-government call for the capability, so that it was not seen as a U.S.-centric objective. Second (after much groundwork), they used the power of the FCC to directly mandate that certain sorts of Internet phone calls must be subject to the relevant law, Communications Assistance for Law Enforcement Act (CALEA). This obligation imposed on the VoIP providers had the effect, of course, of requiring equipment vendors to add wiretap capabilities to their equipment, which in turn required the definition of new standards.

# 7 Sovereignty, jurisdiction, and international engagement

## 7.1 Direct actions

There are certain international venues in which state actors have the authority to act directly. These include international standards bodies such as the ITU, and other formal international venues such as the Internet Governance Forum, both of which derive from the United Nations. While state actors do have the authority to act directly in those venues, the process is one of negotiation and diplomacy—a set of tools very familiar to anyone who studies the ways states engage. While the topics of discussion (e.g. the allocation of Internet addresses) may be distinctive to cyberspace, the tools of engagement are very traditional.

## 7.2 Indirection action

Much of cyberspace is a private sector construct. Even though in some countries the ISPs may be indistinguishable from the state, most of the relevant venues for trans-national engagement are creatures of the private sector. These include the important standards-setting bodies for the Internet, in particular the IETF. While some of these venues such as the IETF do not preclude direct participation by government personnel, in most cases, as discussed above with respect to wiretap, they will find it difficult to have any influence.

The most promising approach to exercise influence in this space is (again) to influence or appropriate the power of relevant domestic private actors. Thus, in a venue where ISPs from different countries meet, a country can attempt to have their ISP carry forward a position of the state. As a practical matter, ISPs do not gather in venues that have much strategic influence—the IETF, for example, is mostly populated by representatives of equipment suppliers and (to some extent) academics. This fact suggests that one limit on the ability of any particular state to have influence in this space will depend on whether they have a domestic equipment supplier or a tradition of academic research in this area.

Influence in this space is clearly a “soft power” phenomenon. The IETF does not decide by simple voting, but a rather socially complex “sense of the meeting”, and participants who have not earned respect through the quality of their contributions may find that they are effectively sidelined. Even countries as powerful as the United States, which dominates the Internet equipment market (with Cisco, Juniper, etc.) often struggles to achieve its national goals, such as standards that implement lawful intercept of Internet traffic.

It also seems clear that some factors of soft power, such as culture and political values, play powerfully here. A country with a tradition of censorship will find that its technical proposals are subjected to hostile scrutiny, as well as countries with extreme (pro or con) positions about protection of copyright.

### 7.2.1 Diluting or growing influence?

A country that appropriates its domestic industry to put forward positions of the state runs the risk of harming the power and influence of that industry. For example, equipment suppliers that seem to act as agents of their state may lose market share, due to fears of disruption in the behavior of the products. Suppliers must invest much effort in building the reputation of their indigenous industry, and this reputation can be lost easily.

However, private industry can enhance the reputation and influence of the state if (for example in the developing world), the equipment suppliers are seen as part of a positive public/private outreach that links development to the vendor. The Chinese equipment supplier Huaiwei is developing a strong market presence in the developing world (e.g. in Africa), which can be seen as part of a larger move by China to increase its respect and influence in the area. It is possible, over time, that China might be able to aggregate the direct state power of these countries to exert influence in international venues.

## 7.3 Imposition of cross-border regulation

A recurring issue with the Internet is whether nation states can impose restrictions on Internet activities that require actions by actors outside the jurisdiction. Typically, nations will argue that the actor of interest is actually subject to the rules of their jurisdiction. Here are some examples.

### 7.3.1 France and Nazi memorabilia

France has laws that prohibit the sale or possession of Nazi memorabilia. When France discovered that such materials were being sold on Internet auctions, the demanded of the auction sites that they not display this material to French users, nor allow them to purchase them. The auction operator (Yahoo), was taken to court in France, where they had enough of a presence that they were compelled to respond. Initially, they argued that this was not their responsibility and that it was technically infeasible, but the court (and experts advising the court) found that for perhaps 70% of French users, their IP address indicated unambiguously that they are in France. So Yahoo was ordered to monitor the source address of their users, and limit the access of users with those IP addresses.

### 7.3.2 The "Chinese proposal" for address allocation

In the above example, the use of the source IP address could localize a user as being in France for only about 70% of French users. For countries interested in tracking the jurisdiction of their users, this is a low percentage. A few years ago, the Chinese put forward a proposition (without explicitly stating that the goal was clarification of jurisdictional boundaries) that when the Internet is converted from IPv4 to IPv6, the addresses should be first allocated to countries, and then to ISPs within the countries. This approach would make the jurisdiction of users much easier to determine, and might also give governments more leverage to apply pressure to ISPs, by threatening to withhold numbers. So far this proposal has not gained much favor internationally.

## 7.4 Actions to encourage competitiveness and national industrial advantage.

In the era of global economics, an important space of international interaction, perhaps more important than the traditional factors of "strength for war", is a nation's capacity to prosper in economic terms. Others can debate the extent to which cyberspace has been a key driver in the globalization of production and trade. Perhaps it is just a coincidence in time. In any case, we see today that the interactions in cyberspace will mirror both the current ambivalence about national protectionism vs. global openness, as well as reflecting the fundamentals of the political economy.

U.S. does not seem to do take many actions to enhance their industrial advantage in cyberspace, except in minor ways, for example keeping control of DNS. Other nations seem to have have more active policy initiatives here.

### 7.4.1 Protection of intellectual property rights

One area in which the U.S. have been very active. The U.S. position is motivated by a believe that innovation is seen as being linked to strong property rights: patents, copyrights, trade secrets and the like. We see important manifestations of these issues in cyberspace today, with the entertainment industry (especially in the U.S.) claiming that theft of content via cyberspace is a material factor in inhibiting creative innovation. We see tensions today as the U.S. argues for a very constraining regime of property rights protections, perhaps losing some influence in the process.

The particular feature of cyberspace that seems relevant here (aside from the apparent ease of duplication and sharing without respect to the rights of the owner) is that cyberspace has elevated *knowledge* as a first-tier element of competitive advantage, and thus a central focus of property disputes. While in centuries past we might have argued over land, and more recently argued about inventions with a tangible manifestation, today we argue over things with no physical manifestation at all. So all the controls will have to be in cyberspace. This fact leads rights-holders (especially in the U.S.) to advocate for laws that make ISPs their agents in policing the transfer of online objects. Online espionage is thought to be rampant, with penetrations carried out both by governments and private sector actors.

Given the centrality of property rights as a component of innovation and economic growth, we can see a tussle of fundamental proportions, between those on the one hand who want the network to be open and free of constraints on how it can be used, and those who see controls in the network as essential to the stable protection of property rights. These interests may align with the interest of the state with respect to taxation. This tussle will occur both *around* and *in* cyberspace.

### 7.4.2 Other examples

Another class of action is the use of anti-trust or anti-competition regulation in various parts of the world (e.g. the EU) to shape the behavior of powerful cyber-actors such as Microsoft and Intel. It might be worth an examination of whether such actions appear to modify the behavior of these actors outside the scope of regulation.

## 7.5 Protecting state revenues.

Perhaps expressing a Western point of view, a stable economic environment includes dependable rules of commerce, protection of property rights, and a stable currency. The government, in order to provide these factors, raises revenues by imposing taxes on its citizens. It is worth looking at taxation at it relates to state and non-state actors.

The power of taxation depends (for the moment) on traditional national boundaries and clear jurisdiction. There are complex rules that govern the rights of citizens to take assets outside the scope of a taxing authority, the tolerance of tax havens, and the like. Taxation, and tax avoidance, is a well-honed system today.

With respect to citizens, cyberspace offers at least the option of both wealth accumulation and transactions that occur in a virtual world, with no clear jurisdictional locus. People now "earn a living" in cyberspace, doing such (perhaps surprising) tasks as designing clothing for avatars. Today, this money has to be exchanged into currency of one or another real jurisdiction to purchase real materials (like food). However, in the future, we could imagine that all of the financial transaction occurs in cyberspace. This might drive a move away from a sales tax to a value added tax, where the provider of the value pays the tax in whatever jurisdiction where it is generated. This will make sense for real good, like food, but will still be ambiguous for virtual goods, or "cyber-goods". If one buys music, or a book, that never has a tangible manifestation, within what jurisdiction did that activity take place? There will surely be tussles over the right to tax such transactions. On what basis will they be resolved?

Perhaps broader than the question of taxation is the point that some virtual worlds have economies larger than some developing nations, and the currencies associated with those games are associated with no state entities, and operate under policies controlled by private entities. Private entities are creating spaces that have both currencies and their own social contracts, somewhat independent of any traditional government control.

Pragmatically, countries are not likely to give up a traditional source of tax-related revenue. There has been a struggle, now perhaps abating, about protecting the valuable taxes that flow into certain countries (especially developing countries) from incoming international telephone calls. Incoming telephone calls include a fee that represents a payment (in hard currency, in many cases) from the sender (e.g. in the U.S.) back to the receiving country. A call that might actually cost much less that $.10/minute to deliver might be priced at $1.00/minute, which is a hefty profit. VoIP eliminates these pricing options, and as expats flocked to the Internet to call home, some countries instructed their ISPs to block VoIP, or passed laws outlawing VoIP. In contrast, the U.S. (which was a significant source of these revenues) has been a vigorous proponent of making Internet calling settlement-free. The state can be just as protective of an obsolete pricing model as a private sector player.

With respect to commerce, small and medium size transactions are increasingly stabilized (and to some extent insured) by credit card companies, rather than by courts of the land. Credit card companies provide fraud protection, arbitration of merchant disputes, and the like. In this respect, we have seen a significant privatization of the traditional governmental role of stable markets. These actors do depend to some extent on the power of government standing behind them, but it is worth exploring this balance. There is a fee hidden inside all credit card transactions, which is the private sector equivalent of a tax to compensate the companies. To the extent they compete on fees, we could see an interesting analog—governments competing to provide stable services for the lowest taxes. (Historically, when trading was a physical phenomenon, markets tended to move to countries with lower taxes but stable commercial practices.)

These speculations aside, governments are not lightly going to abandon their ability to tax, and we can imagine international engagement in this area, both diplomatic "outside" cyberspace to define rules of the road for taxation (and to control the potential of double or multi-taxation), and as well engagement inside cyberspace, with attempts to monitor transactions, or to enforce reporting requirements on transactions, so that they can be taxed according to the rules.

With respect to corporations, a number of considerations may arise. One secondary consideration is that if a country tries to impose political constraints on a trans-national company, and essentially drives that company out of the country, it might lose any power of taxation over that company.

# 8 Application design and standards

The role of the ISP is well understood in defining the character of the Internet. The role of the application designer is perhaps under-appreciated. ISPs can look at and potentially block or manipulate what is sent, but the application designer can determine what is sent in the first place. The application designer can determine which parts of messages are encrypted, which are signed to prevent modification, and which parts are sent unprotected. The application designer can determine the basic communication patterns of the interaction: whether a data transfer is done directly from the sender to the receiver or is staged through a relay, whether the transfer is replicated for robustness or subjected to third-party validation for security. If there are relay points in the communication, the application designer can add mechanisms to the protocols that reduce the need for total reliance on that relay, or can put forward a design that presumes total trust in the relay. By decisions such as these, the application designer can shift the power equation that links all of the actors that participate in implementing the application. However, there has been little methodical study of this context.

## 8.1 Email as a case study.

Email, as designed in the early days of the Internet, moves mail from a sender to a receiver using a set of intermediate forwarding servers, called Message Transfer Agent, or MTA. The benefit of using MTAs is that the computer of the sender and the computer of the receiver need not be connected to the Internet at the same time. Email was designed as an open protocol where any actor can implement all of the parts, including the MTA function. The design does not include an end-to-end confirmation that the mail has been delivered, so it presumes trust in the MTAs, but the open architecture was intended to let the user pick a relay that is deemed trustworthy. While most users of email just use the mail service (MTA) provided by their ISP, many use the MTA of their employer, or a web-based mail service such as Google (gmail) or Hotmail, and there are many for-profit providers of mail that can be used.

## 8.2 Designs that centralize power

In contrast to the "open design" of email, commercially designed applications such as AIM or Facebook are set up in a way that it is more or less necessary to use the servers provided by the designer. In this way, they maintain their position in the midst of the activities of their users, which presumably brings them commercial benefits.

## 8.3 Publius: information dissemination that resists censorship

The Publius system[16] is an example of a system designed to diffuse control, rather than centralize it. It is an information dissemination system that uses highly replicated servers that hold partial replicas of the document being disseminated, with the objective that the document can survive the deletion of a number of the servers (or the removal of the content from a number of servers). Publius was designed in the research community and serves as proof of concept, but did not take off in production, as TOR did.

## 8.4 The role of the government in application design

The U.S. government funded the original development of the Internet, and the resulting shape of the Internet is a direct consequence of the goals it proposed and

[16] Waldman, M., Rubin, A. D., and Cranor, L. F. 2000. Publius: a robust, tamper-evident, censorship-resistant web publishing system. In *Proceedings of the 9th Conference on USENIX Security Symposium - Volume 9* (Denver, Colorado, August 14 - 17, 2000). USENIX Security Symposium. USENIX Association, Berkeley, CA, 5-5.

supported: an open, general purpose platform that shifted power toward the edges, and away from the operators and other potential sources of control.

Early applications such as email were designed as a part of this funding, but the government then seemed to lose interest in trying to shape the Internet by investment in preferred designs. One reason for this may be that the government has no agency that is responsible for articulating and achieving these sorts of goals. NSF is not a government mission agency, but a community-driven science foundation. DARPA funded the early work, but as a military agency chose to carry the full responsibility for defining the government's posture with respect to cyberspae. The Department of Commerce has tried to represent the government's interest with respect to Internet governance, but is not a technical agency. The State Department represents the government at standards setting venues such as the ITU, but does not fund development. Rather, its tradition is to identify and advocate for interests put forward by other parts of the government.

If the government believes that certain values are of interest to it, such as free dissemination of information (in some cases) and high level of control over dissemination of information (in other cases) it could invest in the design and deployment of applications that embody these values.

# 9 The power of non-state actors

We have noted elsewhere that cyberspace seems to have empowered a new set of actors, including the individual, trans-national groups centered on common interests, and recognized NGOs. The question here is a narrow and specific one: do any of these actors exercise *influence* in any of the spheres in which state actors move, or is their empowerment simply from the ability to *use* cyberspace.

At first glance, aside from the international standards-setting bodies discussed below, it is hard to find many such actors with influence. There are actors that monitor the state of the Internet, looking for activities such as the blocking of content or repression of dissidents, and the cataloging of these actions may serve to shift the balance of soft power as one or another country is reported as displaying unpopular political values.

I discussed above the power of the "higher-layer trans-national actors". Current examples seem to suggest that it is very hard for nation states to limit the behavior of these actors (e.g. the use of Twitter in Iran), except by the use of "blunt instruments", such as the turning off of the Internet in a region of China during recent ethnic unrest. It is worth observing the extent to which different state actors are willing to exercise such blunt controls, as the world becomes more dependent on the utility of cyberspace.

## 9.1 Crime and criminals

An important class of non-state actors is criminals. Cyberspace has greatly reshaped the landscape of crime, although the basic nature of crime (theft, extortion, etc.)

seems familiar. But some of the changes are significant. Criminals, in a form of "venue-shopping", can seek countries with weak laws or weak enforcement. The ability of criminals to work at arms length, and with limited consequences to betrayal, allow multi-national "crime production lines" to form. Criminals offer and bid for "factors of production" on Internet web sites and chat rooms. Again, states act outside cyberspace, for example negotiating treaties about tracing of identity across jurisdiction boundaries, and bringing pressure on nations to increase their efforts at enforcement. However, there is some real suspicion that for certain countries (especially corrupt and "failed state" governments), crime is a major source of funds, compared to other sources of taxation, and that crime is better taxed than eliminated. Given this, countries must also call for action inside cyberspace, with greater attention to direct tracing of identity, "forensic quality" accountability, and better controls to increase the cost of crime. If criminals cannot be held accountable, we must take direct action to increase their costs of doing business.

The apparent limits on the ability of governments to control certain sorts of cyber-misbehavior have led to private action that might be called vigilante justice. Certain actors[17] assemble lists of ISPs and servers that seem to be sources of spam, and make these lists available to other operators of MTA to use as they please. Many MTA operators take these lists and use them as a basis for shunning providers that are considered "spammer-friendly".

A hypothesis to be explored and tested in this overall project is that cyberspace has empowered a range of actors, including various international actors. Many NGOs and issue-centric organizations seem to have benefitted from the ability to assemble a constituency of like-minded individuals from around the world using the tools of cyber-space. However, from the perspective of this paper, there seem to be few examples of such groups trying to *influence* cyberspace. These groups are users, but not shapers. There are some exceptions to this generalization: Reporters without Borders (www.rsf.org) reports on abuses of Internet access by governments, and other issues related to the use of cyberspace by reporters. But most of these organizations will not factor into this analysis.

## 9.2 Standards organizations

Organizations such as the ITU have a specific charter to shape cyberspace by the setting of standards. Different such organizations have different charters, each giving it different standing in this space.

The ITU is a unit of the United Nations, and the formal representative to the ITU from the U.S. is from the State Department. Traditionally, the ITU set telephony standards, and in most countries the telephone provider (the PTT) was a state-run organization, so this relationship made sense. The role of the ITU in the shaping of the Internet (essentially non-governmental) is more tangled.

[17] For example, see http://www.spamhaus.org/, visited 1/1/10.

The IETF is essentially a self-decreed standards body that sets most of the influential standards defining the Internet. Most of the attendees (who are nominally expected to attend as individuals) come from companies that supply equipment, although operators and academics are also represented. Governments do not have a major presence.

The ISO is a commercial, rather than a governmental, recognized standards-setting body. It has been relatively inactive in setting relevant standards, after the failure of their major project to define the OSI network standards.

## 9.3 International governance organizations

### 9.3.1 Internet Governance Forum

The IGF is a U.N. sponsored forum intended to allow countries to discuss their concerns and objectives for the Internet. It does not seem to be organized with the objective of taking action or having real power, but as a venue for discussion and debate.

### 9.3.2 ICANN

Much has been written about ICANN, both pro and con. This is a very short summary. When the U.S. government orchestrated the transition of some specific aspects of Internet governance from the research community, they set up a corporation called the Internet Corporation for Assigned Names and Numbers, or ICANN. ICANN is explicitly empowered to make a specific set of decisions, most notably concerning the DNS. Much politics swirls around ICANN. The basis of their authority is constantly debated. So far, it seems to have held. If it fails, not clear what fills the vacuum.

# 10 Summary—tools of engagement

## 10.1 Tussles "in" cyberspace

For many actors, the tools of choice have been the familiar ones of law, regulation, shaping investment, and the like. However, for certain sets of actors and certain sort of tussle, the tools of engagement are deployed within cyberspace itself, as illustrated by several of the previous cases. Tussle in cyberspace is "asymmetric warfare", in that different actors have different tools, and each uses their tools in an attempt to blunt the tools of their adversaries.

### 10.1.1 ISPs

ISPs own the routers and the circuits. The control the topology and the routing, and can determine where traffic goes. They can observe what they forward, and can change it (perhaps not usefully.) They often control the DNS server used by their customers. These are very powerful tools, as described earlier.

### 10.1.2 Application designers

Application designers, by their choice of protocols, have many tools at their disposal. They can choose protocols that encrypt what is sent, which prevents the ISPs from much effective peeking. Even if they do not encrypt, they can sign, which prevents the ISP from making any changes. The application can be designed to give the end-user choice over which service provider to use (e.g. with email), or to restrict the user to the services of the application designer (e.g. with most games, many Instant Message systems and the like).

### 10.1.3 End-users

To the extent that the design of the application offers any choices to the end-user, the end-user can exercise those choices in ways that impose discipline on the service providers. If users can select among email providers, they may choose providers that seem more trustworthy, less intrusive, or the like.

### 10.1.4 Encryption

Encryption is a tool that an application designer can use (or can offer as a choice for the end-user to use) to blunt the controls of the ISP. However, encryption can affect many other tussles. For example, in the U.S. there is an SEC regulatory requirement that all communication among brokers and between brokers and clients be logged. If the communication is encrypted, logging is meaningless. So the design of (for example) instant messaging systems must allow a logging system to be inserted into the middle of the communication, even though for other actors such as the ISPs that carry the traffic, allowing them to peek at the contents seems most inappropriate. Once considerations like this are recognized, the resulting design considerations can be rather complex.

### 10.1.5 Cross-industry influence

Companies traditionally engage by fitting along a common supply chain, or by forming strategic alliances. In the capital-intensive area of broadband deployment, these tools have not been adequate, and companies have used other techniques such as trying to persuade regulators to impose obligations on other actors.

## 11 Conclusions

Cyber-enthusiasts tend to conclude that the cyber-cat is out of the bag, the state actors have to a large extent lost control of what happens in cyberspace, and are powerless to have influence. This summary conclusion is probably too simplistic. We see both state actors and non-state actors becoming more sophisticated at extending their influence. More and more, the influence will not be through direct action (such as turning off the Internet), but through indirect means that depend on soft power. A conclusion that is perhaps more realistic but also optimistic is that the desire of various states to increase their influence will cause them to polish the rough edges off of some of their political values over time. Like a country trying to join the EU or NATO, there is a price to pay in terms of conformity.

While attention to the potential use of direct (military) power in cyberspace is important, it should not be allowed to distract us from the larger sweep of issues, issues that may in practical terms be more important in shaping the relative power of different nations in cyberspace.

## 11.1 Regulation

Regulation (e.g. by the FCC) has traditionally been a “trump card” in the government arsenal. The reasons why regulation is effective are sometimes taken as obvious, and have perhaps been less well studied than they should have been. The traditional targets of regulation, like the phone companies, grew up in a tradition of submitting to regulation, had sunk cost assets that made them “easy to find and hard to flee”. The stable industry structure allowed a stable co-evolved regulatory structure to emerge—the telephone as an industry was regulated by the matching bureau in the FCC and the states.

In contrast, small companies innovating in the Internet context had very different attributes: they morphed the shape of their product, they did not fit into stable definitions of markets segments to which regulatory obligations could be applied, they moved overseas if pushed to hard (Skype has no real presence in the U.S., as did the early providers of unwelcome encryption technology), and general confounded the early attempts of the regulators even to come up with a framework for regulation, let alone impose specifics.

While the government is gaining sophistication in this area, the balance of power does seem to have shifted in a fundamental way.

In other countries, where the entanglement of the telephone (and Internet) companies and the government is greater, the governments have had greater success imposing their wishes on the Internet. This variation might make a good comparative case study.