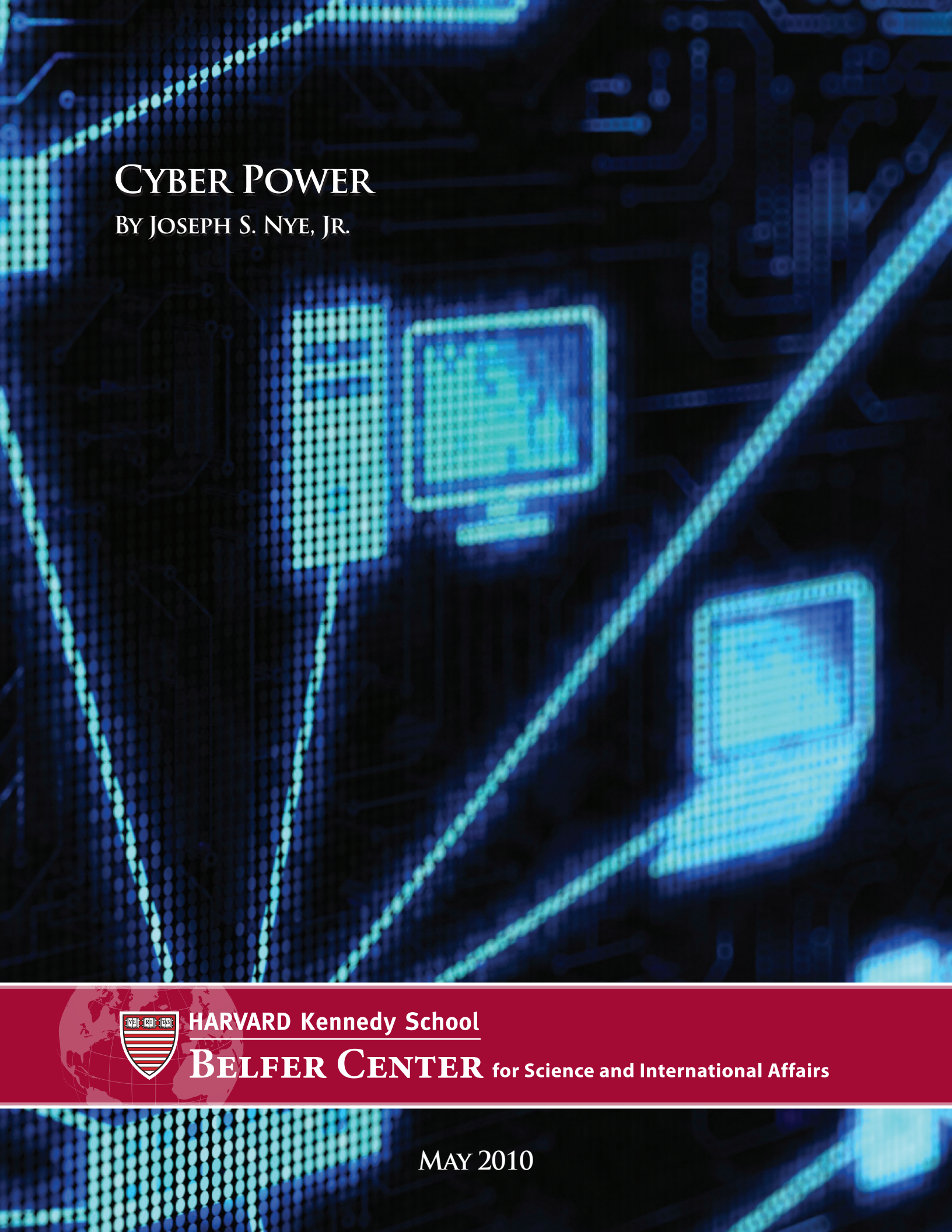

Cyber Power

By Joseph S. Nye, Jr.

HARVARD Kennedy School
Belfer Center for Science and International Affairs

May 2010

This essay is drawn from the author's forthcoming book, *The Future of Power in the 21st Century*, Public Affairs Press, 2011. The author is grateful to insights provided by fellow participants in the joint MIT-Harvard Minerva Project, a research initiative funded by the Department of Defense.
Comments invited: joseph_nye@harvard.edu

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org

Cyber Power

By Joseph S. Nye, Jr.

HARVARD Kennedy School
Belfer Center for Science and International Affairs

May 2010

Abstract

Power depends upon context, and the rapid growth of cyber space is an important new context in world politics. The low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics. Changes in information have always had an important impact on power, but the cyber domain is both a new and a volatile manmade environment. The characteristics of cyberspace reduce some of the power differentials among actors, and thus provide a good example of the diffusion of power that typifies global politics in this century. The largest powers are unlikely to be able to dominate this domain as much as they have others like sea or air. But cyberspace also illustrates the point that diffusion of power does not mean equality of power or the replacement of governments as the most powerful actors in world politics.

Information and Power Diffusion

Power transition from one dominant state to another is a familiar historical event, but power diffusion is a more novel process. The problem for all states in today's global information age is that more things are happening outside the control of even the most powerful states. In the words of a former State Department director of policy planning, "the proliferation of information is as much a cause of nonpolarity as is the proliferation of weaponry."[1]

Some observers welcome this trend as marking the decline of the sovereign state that has been the dominant global institutions since the Peace of Westphalia in 1648. They predict that the information revolution will flatten bureaucratic hierarchies and replace them with network organizations. More governmental functions will be handled by private markets as well as by nonprofit entities. As virtual communities develop on the Internet, they will cut across territorial jurisdictions and develop their own patterns of governance. States will become much less central to people's lives. People will live by multiple voluntary contracts and drop in and out of communities at the click of a mouse. The new pattern of crosscutting communities and governance will become a modern and more civilized analogue to the feudal world that existed before the rise of the modern state.[2]

Such cyber transformations are still fanciful, but a new information revolution is changing the nature of power and increasing its diffusion. States will remain the dominant actor on the world stage, but they will find the stage far more crowded and difficult to control. A much larger part of the population both within and among countries has access to the power that comes from information. Governments have always worried about the flow and control of information, and the current period is not the first to be strongly affected by dramatic changes in information technology. For example, in the fifteenth century, Johann Gutenberg's invention of movable type, which allowed printing of the Bible and its accessibility to large portions of the European population, is credited with playing a major role in the onset of the Reformation.

The current information revolution, sometimes called "the third industrial revolution," is based on rapid technological advances in computers, communications, and software that in turn

have led to dramatic decreases in the cost of creating, processing and transmitting information. Computing power doubled every 18 months for 30 years, and by the beginning of the twenty-first century it cost one-thousandth of what it did in the early 1970s.

In 1993, there were about 50 websites in the world; by the end of the decade, that number had surpassed 5 million. By 2010, China alone had nearly 400 million users. Communications bandwidths are expanding rapidly, and communications costs continue to fall even more rapidly than computing power. As recently as 1980, phone calls over copper wire could carry only one page of information per second; today a thin strand of optical fiber can transmit 90,000 *volumes* in a second. In 1980, a gigabyte of storage occupied a room; now 200 gigabytes of storage fits in your shirt pocket. The amount of digital information increases tenfold every five years.[3] What will this mean for power and governance in the 21st century?

Power

For a concept that is so widely used, "power" is surprisingly elusive and difficult to measure.[4] But such problems do not make a concept meaningless. Like many basic ideas, power is a contested concept. No one definition is accepted by all who use the word, and people's choice of definition reflects their interests and values. A commonsense place to start is the dictionary which tells us that power is the capacity to do things, but more specifically if one is interested in policy issues, power is the ability to affect other people to get the outcomes one wants. Some people call this influence, and distinguish power from influence, but that is confusing because the dictionary defines the two terms interchangeably.

As one economist put it, "one of the main purposes for which social scientists use the concept of A's power over B is for the description of the policy possibilities open to A."[5] In Max Weber's view, we want to know the probability that an actor in a social relationship can carry out his own will.[6] Even when we focus primarily on particular agents or actors, we cannot say that an actor "has power" without specifying power "to do what."[7] One must specify who is involved in the power relationship (the scope of power) as well as what topics are involved (the domain of power.) Statements about power always depend on context, and cyberspace is a new and important domain of power.

The evolution modern social science definitions of behavioral power is sometimes summarized as "the three faces of power."[8] The first aspect or "face" of power was defined by Robert Dahl in studies of New Haven in the 1950s.[9] His focus on getting others to do what they would not otherwise do is widely used today even though it covers only part of power behavior. In the 1960s, the political scientists Peter Bachrach and Morton Baratz pointed out that Dahl's definition missed what they called the "second face of power," the dimension of agenda setting, or framing issues in such a way that the issue of coercion never arose.[10] In the 1970s, the sociologist Steven Lukes pointed out that ideas and beliefs also help shape others' preferences, and one can also exercise power by determining others' wants.[11] In 1990, I distinguished hard and soft power along a spectrum from command to co-optive behavior. Hard power behavior rests on coercion and payment. Soft power behavior rests on framing agendas, attraction or persuasion.[12]

Even large countries with impressive hard and soft power resources, such as the United States, find themselves sharing the stage with new actors and having more trouble controlling their borders in the domain of cyberspace. Cyberspace will not replace geographical space and will not abolish state sovereignty, but the diffusion of power in cyberspace will coexist and greatly complicate what it means to exercise power along each of these dimensions.

Cyber Power

Power based on information resources is not new; cyber power is. There are dozens of definitions of cyberspace but generally "cyber" is a prefix standing for electronic and computer related activities. By one definition: "cyberspace is an operational domain framed by use of electronics to …exploit information via interconnected systems and their associated infra structure."[13] Power depends on context, and cyber power depends on the resources that characterize the domain of cyberspace.

We sometimes forget how new cyberspace is. In 1969, the Defense Department started a modest connection of a few computers called ARPANET, and in 1972, the codes for exchanging data (TCP/IP) were created to constitute a rudimentary internet capable of exchanging packets of digital information. The domain name system of internet addresses starts in 1983, and the first computer viruses were created about that time. The World Wide Web begins in 1989; Google the most popular search engine was founded in 1998; and the open source encyclopedia, Wikipedia, begins in 2001. In the late 1990s, businesses begin to use the new technology to shift production and procurement in complex global supply chains. Only recently has there been the bandwidth and server farms to support "cloud computing" in which companies and individuals can store their data and software on the Web. ICANN (the internet corporation for assigned names and numbers) was created in 1998, and the US government only began to develop serious national plans for cyber security in the past decade. In 1992, there were only a million users on the internet; within fifteen years that had grown to a billion.[14] In its early days, libertarians proclaimed that "information wants to be free" and portrayed the internet as the end of government controls and the "death of distance." In practice, governments and geographical jurisdictions play a major role, but the domain is also marked by power diffusion.[15]

One can conceptualize cyberspace in terms of many layers of activities, but a simple first approximation portrays it as a unique hybrid regime of physical and virtual properties.[16] The physical infrastructure layer follows the economic laws of rival resources and increasing marginal costs, and the political laws of sovereign jurisdiction and control. The virtual or informational layer has economic network characteristics of increasing returns to scale, and political practices that make jurisdictional control difficult.[17] Attacks from the informational realm where costs are low can be launched against the physical domain where resources are scarce and expensive. But conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer.

Cyber power behavior rests upon a set of resources that relate to the creation, control and communication of electronic and computer based information -- infrastructure, networks, software, human skills. This includes the Internet of networked computers, but also intranets, cellular technologies and space based communications. Defined behaviorally, cyber power is the ability to

obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. In one widely used definition, cyber power is "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[18] Cyber power can be used to produce preferred outcomes *within* cyberspace or it can use cyber instruments to produce preferred outcomes in other domains *outside* cyberspace.

By analogy, sea power refers to the use of resources in the oceans domain to win naval battles on the ocean, to control shipping chokepoints like straits, and to demonstrate an offshore presence, but it also includes the ability to use such the oceans to influence battles, commerce, and opinions on land. In 1890, Alfred Thayer Mahan popularized the importance of sea power in the context of new technologies of steam propulsion, armor and long range guns. President Theodore Roosevelt responded by greatly expanding America's blue water navy and sending it around the world in 1907. After the introduction of aircraft in World War I, military men began to theorize about the domain of air power and its ability to strike directly at an enemy's urban center of gravity without armies having to first cross borders. Franklin Roosevelt's investments in air power were vital in World War II. And after the development of inter continental missiles and surveillance and communications satellites in the 1960s, writers began to theorize about the particular domain of space power. John F. Kennedy launched a program to ensure an American lead in space and to put a man on the moon. In 2009, President Barack Obama called for a major new initiative in cyber power, and other governments have followed suit.[19] As technological change reshapes power domains, political leaders soon follow.

The cyber domain is unique in that it is manmade, recent and subject to even more rapid technological changes than other domains. As one observer put it, "the geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch."[20] It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. The costs of developing multiple carrier task forces and submarine fleets create enormous barriers to entry and make it still possible to speak of American naval dominance. While piracy remains a local option for non-state actors in areas like Somalia or the Malacca Straits, sea control remains out of the reach of non-state actors. Similarly, while there are many private and governmental actors in the air domain, a country can still seek to achieve air superiority through costly investments in 5th generation fighters and satellite support systems.

In contrast, as mentioned above, the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost. In contrast to sea, air and space, "cyber shares three characteristics with land warfare – though in even greater dimensions: the number of players, ease of entry, and opportunity for concealment…On land, dominance is not a readily achievable criterion."[21] While a few states like the United States, Russia, Britain, France, and China are reputed to have greater capacity than others, it makes little sense to speak of dominance in cyber space as in sea power or air power. If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non state actors.

Extreme conflict in the cyber domain or "cyber war" is also different. In the physical world, governments have a near monopoly on large scale use of force, the defender has an intimate knowledge of the terrain, and attacks end because of attrition or exhaustion. Both resources and mobility are costly. In the virtual world, actors are diverse, sometimes anonymous, physical distance is immaterial, and a "single virtual offense is almost cost free."[22] Because the internet was designed for ease of use rather than security, the offense currently has the advantage over the defense. This might not remain the case in the long term as technology evolves, including efforts at "re-engineering" some systems for greater security, but it remains the case at this stage. The larger party has limited ability to disarm or destroy the enemy, occupy territory, or effectively use counter-force strategies. As we shall see below, deterrence is possible, but differs because of problems of attribution of the source of an attack. Ambiguity is ubiquitous and reinforces the normal fog of war. Redundancy, resilience and quick reconstitution become crucial components of defense. As one expert summarizes the situation, "attempts to transfer policy constructs from other forms of warfare will not only fail but also hinder policy and planning."[23]

Cyber power affects many other domains from war to commerce. We can distinguish "intra cyberspace power" and "extra cyberspace power" just as with sea power, we can distinguish naval power on the oceans from naval power projection onto land . For example, carrier based aircraft can participate in land battles; trade and commerce may grow because of the efficiency of a new generation of container ships; and the soft power of a country may be increased by the visit of naval hospital ships in humanitarian missions.

Table 1: Physical and Virtual Dimensions of Cyber Power

		Targets of Cyber Power
	Intra cyber space	**Extra cyber space**
Information Instruments	Hard: Denial of service attacks Soft: Set norms and standards	Hard: Attack SCADA systems Soft: Public diplomacy campaign to sway opinion
Physical Instruments	Hard: Government controls over companies Soft: Infrastructure to help human rights activists	Hard: Bomb routers or cut cables Soft: Protests to name and shame cyber providers

As Table 1 illustrates, *inside* the cyber domain, information instruments can be used to produce soft power in cyber space through agenda framing, attraction or persuasion. For example, attracting the open source software community of programmers to adhere to a new standard is an example of soft power targeted within cyberspace.

Cyber resources can also produce hard power inside cyber space. For example, states or non-state actors can organize a distributed denial of service attack by using "botnets" of hundreds of thousands (or more) corrupted computers that swamp a company or country's internet system

and prevents it functioning. Organizing a botnet by infiltrating a virus into unguarded computers is relatively inexpensive, and botnets can be illegally rented on the internet for a few hundred dollars. Sometimes individual criminals do this for purposes of extortion.

Other cases may involve "hacktivists" or ideologically motivated intruders. For example, Taiwanese and Chinese hackers regular deface each others' web sites. In 2007, Estonia suffered a distributed denial of service attack that was widely attributed to "patriotic hackers" in Russia who were offended by Estonia's movement of a World War II monument to Soviet soldiers. In 2008, shortly before Russian troops invaded, Georgia suffered a denial of service attack that shut down its internet access. (In both instances, however, the Russian government seems to have abetted the hackers while maintaining "plausible deniability.") Other forms of hard power within cyber space include insertion of malicious code to disrupt systems or to steal intellectual property. Criminal groups do it for profit, and governments may do it as a way of increasing their economic resources. China, for example, has been accused of such activities by a number of other countries. Proof of the origin or motive of such attacks is often very difficult as attackers can route their intrusions through servers in other countries to make attribution difficult. For example, many of the attacks on Estonian and Georgian targets were routed through American servers.[24]

Cyber information can also travel through cyberspace to create soft power by attracting citizens in another country. A public diplomacy campaign over the internet is an example. But cyber information can also become a hard power resource that can do damage to physical targets in another country. For example, many modern industries and utilities have processes that are controlled by computers linked in SCADA (supervisory control and data acquisition) systems. Malicious software inserted into these systems could be instructed to shut down a process which would have very real physical effects. For example, if a hacker or a government shut down the provision of electricity in a Northern city like Chicago or Moscow in the middle of February, the devastation could be more costly than if bombs had been dropped. In some facilities like hospitals, back-up generators can provide resilience in the case of a disruptive attack, but widespread regional blackouts would be more difficult to cope with.

As the table above indicates, physical instruments can provide power resources that can be brought to bear on the cyber world. For instance, the physical routers and servers and the fiber optic cables that carry the electrons of the internet have geographical locations within governmental jurisdictions, and companies running and using the internet are subject to those governments' laws. Governments can bring physical coercion to bear against companies and individuals; what has been called "the hallmark of traditional legal systems." Legal prosecution made Yahoo control what it sent to France and Google removed hate speech from searches in Germany. Even though the messages were protected free speech in the companies' "home country", the United States, the alternative to compliance was jail time, fines, and loss of access to those important markets. Governments control behavior on the internet through their traditional physical threats to such intermediaries as internet service providers, browsers, search engines and financial intermediaries.[25]

As for investment in physical resources that create soft power, governments can set up special servers and software designed to help human rights activists propagate their messages despite the efforts of their own governments to create information firewalls to block such messages. For

example, in the aftermath of the Iranian government's repression of protests following the election of 2009, the American State Department invested in software and hardware that would enable the protesters to disseminate their messages.

Finally, as Table 1 illustrates, physical instruments can provide both hard and soft power resources that can be used against the internet. The cyber information layer rests upon a physical infrastructure that is vulnerable to direct military attack or sabotage both by governments and non state actors such as terrorists or criminals. Servers can be blown up and cables can be cut. And in the domain of soft power, non-state actors and NGOs can organize physical demonstrations to name and shame companies (and governments) that they regard as abusing the Internet. For example, in 2006 protesters in Washington marched and demonstrated against Yahoo and other internet companies that had provided the names of Chinese activists that led to their arrest by the Chinese government.

Another way of looking at power in the cyber domain is to consider the three faces or aspects of relational power.

Table 2: Three Faces of Power in the Cyber Domain

1st Face:	(A induces B do what B would initially otherwise not do)	
	Hard Power:	denial of service attacks, insertion of malware, SCADA disruptions, arrests of bloggers
	Soft Power:	information campaign to change initial preferences of hackers, recruitment of members of terrorist organizations
2nd Face:	(Agenda control: A precludes B's choice by exclusion of B's strategies)	
	Hard Power:	firewalls, filters, and pressure on companies to exclude some ideas
	Soft Power:	ISPs and search engines self monitor, ICANN rules on domain names, widely accepted software standards
3rd Face:	(A shapes B's preferences so some strategies are never even considered)	
	Hard Power:	threats to punish bloggers who disseminate censored material
	Soft Power:	information to create preferences (eg. stimulate nationalism and "patriotic hackers,"), develop norms of revulsion (eg. child pornography)

One can find evidence of hard and soft power behavior in all three aspects as applied to cyberspace. The first face of power is the ability of an actor to make others do something contrary to their initial preferences or strategies. Examples related to hard power could included the denial of services attacks described above, as well as arresting or otherwise preventing dissident bloggers from sending their messages. For example, in December 2009, China sentenced Liu Xiaobo,

a veteran human rights activist and blogger to 11 years in prison for "inciting subversion of state power," and introduced new restrictions on registration and operation of websites by individuals. As one Chinese web hosting service provider commented, "for nine years I have run a successful and legal business, and now I have suddenly been told that what I do makes me a criminal."[26]

In terms of soft power, an individual or organization might attempt to persuade others to change their behavior. The Chinese government sometimes used the internet to mobilize Chinese students to demonstrate against Japan when its officials took positions that offended Chinese views of the 1930s relationship. Al Qaeda videos on the internet designed to recruit people to their cause are another case of soft power being used to change people from their original preferences or strategies.

The second face of power is agenda setting or framing in which an actor precludes the choices of another by exclusion of their strategies. If this is against their will, it is an aspect of hard power; if it is accepted as legitimate it is an instance of soft power. For example, on the February 2010 anniversary of the Iranian Revolution, the government slowed the internet to prevent protesters sending films of protests to be seen on YouTube as they had successfully done six months earlier. As one Iranian exile commented, "It was the day the Greens grew up and learned that fighting a government as determined as the Islamic Republic of Iran will require much more than Facebook fan pages, Twitter clouds, and emotional YouTube clips."[27]

According to the Open Net Initiative, at least 40 countries use highly restrictive filters and firewalls to prevent the discussion of suspect materials. Eighteen countries engage in political censorship, which is described as "pervasive" in China, Vietnam and Iran, and "substantial" in Libya, Ethiopia, and Saudi Arabia. More than 30 states filter for social reasons, blocking content related to topics such as sex, gambling and drugs. Even the United States and many European states do this "selectively."[28] Sometimes this is accepted and sometimes not. If the filtering is secretive, it is hard for citizens to know what they do not know. First generation filtering technologies are installed at key Internet chokepoints, and work by preventing requests for a predetermined list of websites and addresses. They are often known to users, but they have been supplemented by more sophisticated technologies that are more stealthy, dynamic and targeted on opponents "just in time."[29] In some instances, what looks like hard power to one group, looks attractive to another. After riots in Xingjian in 2009, China closed thousands of websites and censored text messages which made communication more difficult for residents of that region, but it also cultivated homegrown alternatives to foreign based Web sites like YouTube, Facebook and Twitter which was attractive in the eyes of nationalistic "patriotic hackers."[30] Among American corporations, when the music industry sued more than 12,000 Americans for intellectual property theft in downloading music illegally, the threat was felt as hard power by those sued, and by many who were not sued as well. But when a transnational corporation like Apple decides not to allow certain applications to be downloaded to its I phones, many consumers are not even aware of the truncations of their potential agendas, and few understand the algorithms that guide their searches for information.[31]

The third face of power involves one actor shaping another's initial preferences so that some strategies are not even considered. When companies chose to design one code rather than another into their software products, few consumers notice.[32] Governments may carry out campaigns

to delegitimize certain ideas such as the Falun Gong religion in China and restrict dissemination of its ideas on the internet and thus make it difficult for Chinese citizens to know about it. Saudi Arabia makes certain infidel web sites are unavailable to its citizens. The United States government has taken measures against credit card companies so that internet gambling is unavailable to its citizens. France and Germany prevent discussion of Nazi ideology on the internet. Occasionally, as with child pornography, there is broad cross cultural consensus on restricting certain ideas and pictures from being available.

Actors and their Relative Power Resources

The diffusion of power in the cyber domain is represented by the vast number of actors, and relative reduction of power differentials among them. Anyone from a teen age hacker to a major modern government can do damage in cyber space, and as the famous *New Yorker* cartoon once put it, "on the internet, no one knows you are a dog." The infamous "Love Bug" virus unleashed by a hacker in the Philippines is estimated to have caused $15 billion in damage.[33] Computer networks essential to the American military are attacked "hundreds of thousands of times every day".[34] Cybercriminal groups were said to have stolen over $1 trillion in data and intellectual property in 2008.[35] One cyber espionage network — GhostNet — was found to be infecting 1,295 computers in 103 countries, of which 30 percent were high value governmental targets.[36] Terrorist groups use the web to recruit new members and plan campaigns. Political and environmental activists disrupt web sites of companies and governments. What is distinctive about power in the cyber domain is not that governments are out of the picture as the early cyber libertarians predicted, but the different power resources that different actors possess, and the narrowing of the gap between state and non state actors in many instances. But relative reduction of power differentials is not the same as equalization. Large governments still have more resources. On the internet, all dogs are not equal.

As a rough approximation, we can divide actors in cyberspace into three categories: governments, organizations with highly structured networks, and individuals and lightly structured networks. (Of course, there are many subcategories)

Because the physical infrastructure of the internet remains tied to geography and governments are sovereign over geographical spaces, location still matters as a resource in the cyber domain. Governments can take steps to subsidize infrastructure, computer education, and protection of intellectual property that will encourage (or discourage) the development of capabilities within their borders. The provision of public goods, including a legal and regulatory environment, can stimulate commercial growth of cyber capabilities. South Korea, for example, has taken a lead on public development of broad band capabilities. A reputation that is seen as legitimate, benign and competent can enhance (or conversely undercut) a government's soft power with other actors in the cyber domain.

Geography also serves as a basis for governments to exercise legal coercion and control. For example, after the Xinjiang riots in 2009, the Chinese government was able to deprive 19 million residents in an area twice as big as Texas of text messaging, international phone calls, and internet access to all but a few government controlled Web sites. The damage to business and tourism was significant, but the Chinese government was more concerned about political stability.[37] In 2010,

Table 3: Relative Power Resources of Actors in the Cyber Domain

A. Governments

1. Development and support of infrastructure, education, intellectual property.
2. Legal and physical coercion of individuals and intermediaries located within borders.
3. Size of market and control of access; eg. EU, China, US
4. Resources for cyber attack and defense: bureaucracy, budgets, intelligence agencies
5. Provision of public goods; eg. regulations necessary for commerce
6. Reputation for legitimacy, benignity, competence that produce soft power

Key Vulnerabilities: High dependence on easily disrupted complex systems, political stability, reputational losses

B. Organizations and highly structured networks

1. Large budgets and human resources; economies of scale
2. Transnational flexibility
3. Control of code and product development, generativity of applications
4. Brands and reputation

Key Vulnerabilities: Legal, intellectual property theft, systems disruption, reputation loss (name and shame)

C. Individuals and lightly structured networks

1. Low cost of investment for entry
2. Virtual anonymity and ease of exit
3. Asymmetrical vulnerability compared to governments and large organizations

Key Vulnerabilities: Legal and illegal coercion by governments and organizations if caught

when SWIFT, a private company that coordinates and logs money transfers among banks, moved key computer servers from the US to Europe, it meant that it now needed permission of the EU to hand over data voluntarily to the US Treasury for anti-terrorist purposes. When the European Parliament balked at approval of a Europe wide agreement, SWIFT announced that "there is no legal basis for us to hand over data from our European centers to the Treasury."[38]

If a market is large, a government can exert its power extraterritorially. Europe's tight privacy standards have had a global effect. When companies like Yahoo or Dow Jones have faced legal claims based on internet activity in France or Australia, they decided to comply rather than walk away from those markets. Obviously, this is a power resource available to governments with jurisdiction over large markets, but not necessarily to all governments.

Governments also have the capacity to carry out offensive cyber attacks.[39] For example, America's Tenth Fleet and Twenty-fourth Air Force have no ships or planes. Their battlefield is cyberspace.[40] Unfortunately, news accounts of "millions of attacks" use the term "attack" loosely

to refer to everything from computer port scanning to hacking (illegal computer trespassing) and defacing websites to full scale operations designed to wreak physical destruction. One should distinguish simple attacks which use inexpensive tool kits which anyone can download from the internet from advanced attacks which identify new vulnerabilities that have not yet been patched, involve new viruses, and involve "zero day attacks" (first time use.) These attacks require more skill than simple hacking. Experts also distinguish cyber exploitation for spying purposes from cyber attack which has destructive or disruptive purposes. Governments carry out activities of both types. Little is publicly confirmed about cyber espionage, but most reports describe intrusions into computer systems as ubiquitous, and not limited to governments.

There are reports of attacks related to warfare in the cases of Iraq in 2003 or Georgia in 2008, and sabotage of electronic equipment in covert actions.[41] Israel is said to have used cyber means to defeat Syrian air defenses before bombing a secret nuclear reactor in September 2007.[42] Most experts see cyber attack as an important adjunct rather than an overwhelming weapon (unlike nuclear) in inter-state wars. States intrude into each others' cyber systems in "preparation of the battlefield" for what could be future conflicts. Both American and Chinese military theorists have discussed such steps , but little is publicly stated about offensive cyber doctrines. A National Research Council Report concluded in 2009 that "today's policy and legal framework for guiding and regulating the U.S. use of cyberattack is ill-formed, undeveloped, and highly uncertain."[43] Presumably many large governments engage in such activity, though the success of such attacks would depend upon the target's vulnerabilities, and thus premature exercise or disclosure would undercut their value. "Zero day" attacks without prior warning are likely to be the most effective, and even their effects may depend on measures the target has taken to develop resiliency, some of which may not be fully known to the attacker.

Cyber attacks that deny service or disrupt systems are also carried out by non-state actors whether for ideological or criminal purposes, but such groups do not have the same capacities as large governments. In general, it is easy to mount low cost attacks such as denial of service against low value targets such as websites. Botnets of zombie computers are easy to rent, and websites are often vulnerable to such measures. But sophisticated attacks against high value targets such as defense communications systems require a higher cost of attack, which involves large intelligence agencies to intrude physically and/or crack highly encrypted codes. A teenage hacker and a large government can both do considerable damage over the internet, but that does not make them equally powerful in the cyber domain. Power diffusion is not the same as power equalization. Some government experts believe that concerted technological improvements in encryption and identity management could greatly reduce threats at the low end of the spectrum within five years.[44]

Some transnational corporations have huge budgets, skilled human resources, and control of proprietary code that gives them power resources larger than many governments. In 2009, Microsoft, Apple and Google had annual revenues of $58, 35, and 22 billion respectively, and together employed over 150,000 people.[45] Amazon, Google, Microsoft, and others are competing in the development of cloud computing, and have server farms with more then 50,000 servers. Their transnational structure allows them to exploit markets and resources around the globe. IBM, for example, derives two thirds of its revenue from overseas, and only a quarter of its 400,000 work-

force is located in the United States.[46] At the same time, to preserve their legal status as well as their brand equity, transnational corporations have strong incentives to stay compliant with local legal structures.

No such legal niceties constrain the power of criminal organizations. Some are small "strike and exit" operations, which make their gains quickly before governments and regulators can catch up.[47] Others have impressive transnational scale and presumably buy protection from weak governments. Before it was dismantled by law enforcement, the Darkmarket online network had over 2500 members across the world buying and selling stolen financial information, passwords, and credit cards.[48] Up to a quarter of network-connected computers may be part of a botnet, and some botnets include millions of computers. While estimates vary, cyber crime may cost companies over a trillion dollars a year.[49] Some criminal groups, such as the so called "Russian Business Network" may have inherited some capabilities of the Soviet state after its dissolution, and are alleged to retain informal connections with the government. According to a British official, "there were strong indications RBN had the local police, local judiciary and local government in St. Petersburg in its pocket. Our investigation hit significant hurdles."[50] Moreover, "the hacking skills of criminal groups may make them natural allies for nation-states looking for a way to augment their capabilities while denying involvement in cyber attacks."[51] The scale of some criminal operations is expensive and costly, but apparently profitable. In 2006, the US Government Accountability Office estimated that only five percent of cybercriminals were ever arrested or convicted.[52]

Terrorist groups make active use of cyber tools, as we saw earlier, though cyber terrorism narrowly defined as using virtual tools to wreak destruction (see the top row in Table 1) has thus far been rare. While there is nothing stopping terrorist groups from recruiting able computer specialists or purchasing malware from criminal groups on the internet, "cyber attacks appear much less useful than physical attacks: they do not fill potential victims with terror, they are not photogenic, and they are not perceived by most people as highly emotional events."[53] Of twenty-two plots disrupted since 9/11, all involved explosives or small arms, and "while the United States' critical infrastructure from the electrical grid to the financial sector, is vulnerable to attack through cyberspace, al-Qaeda lacks the capability and motivation to exploit these vulnerabilities."[54] Others are not so sanguine. For example, Mike McConnell, former Director of National Intelligence believes that the vulnerabilities of financial and electrical systems present a huge target for any group that wishes to wreak destruction, and that such groups will develop the capabilities to become a greater threat than other nation states. In his words, "when terrorist groups have the sophistication, they'll use it."[55]

So far, terrorists seem to have decided that for their purposes, explosives provide a tool with more bang for the buck. But that does not mean that terrorist groups do not use the internet for promoting terrorism. As we saw earlier, it has become a crucial tool that allows them to operate as networks of decentralized franchises, create a brand image, recruit adherents, raise funds, provide training manuals and manage operations. It is far safer to send electrons than agents through customs and immigration controls. Thanks to cyber tools, Al Qaeda has been able to move from a hierarchical organization restricted to geographically organized cells to a horizontal global network

to which local volunteers can self-recruit. As one expert on terrorism describes, the key place for radicalization is "neither Pakistan nor Yemen nor Afghanistan …but in a solitary experience of a virtual community: the ummah on the Web."[56]

This is an example of how cyber tools begin to blur the lines between organizations with highly structured networks and individuals with lightly structured networks. As a number of examples above have shown, individuals can easily play in the cyber domain because of the low cost of investment for entry, virtual anonymity, and ease of exit. Sometimes they act with government approval and sometimes against them. For example, before the 2008 Russian attack on Georgia, "any civilian, Russian born or otherwise, aspiring to be a cyber warrior was able to visit pro-Russia websites to download the software and instructions necessary to launch denial of service attacks on Georgia."[57] During student protests in Iran in 2009, Twitter and social networking sites were crucial for organizing and reporting demonstrations. "The U.S. government asked Twitter executives not to take the site down for scheduled maintenance. They were worried that might interfere with how Twitter was being used to organize demonstrations." Six months later, however, an unknown group called the Iranian Cyber Army successfully redirected Twitter traffic to a website with an anti-American message, and in February 2010, the Iranian government blocked most access to Twitter and other sites.[58]

It is worth noting that individual actors in the cyber domain benefit from asymmetrical vulnerability compared to governments and large organizations. They have very low investment and little to lose from exit and re-entry. Their major vulnerability is to legal and illegal coercion by governments and organizations if they are apprehended, but only a small per cent are actually caught. In contrast, corporations have important vulnerabilities because of large fixed investments in complex operating system, intellectual property, and reputation. Similarly, large governments depend on easily disrupted complex systems, political stability, and reputational soft power. While hit and run cyber strikes by individuals are unlikely to bring governments or corporations to their knees, they can impose serious costs of disruption to operations and to reputations with a miniscule investment. Governments are top dogs on the internet, but smaller dogs still bite, and dealing with those bites can lead to a complex politics.

Google and China

This complexity is illustrated by the case of Google, an American company and the government of China.[59] Early in 2010, Google announced that it was withdrawing from business in China and thus inflicted a noticeable cost upon Chinese soft power. The case involved three issues that were technically different but became linked politically: alleged efforts by the Chinese government to steal Google's source code (intellectual property); intrusion into the Gmail accounts of Chinese activists (human rights); and in response, Google's decision to stop complying with censorship of searches by Google.cn (although Google had been complying for four years.) Technically, pulling out of China did nothing to solve the first two issues which do not depend on servers located in China. But the intrusions into Gmail were becoming expensive for Google because it aspired to be the cloud provider of choice (in a competition with rivals like Microsoft) and protecting Gmail's reputation for security was more valuable than the search market in China where Baidu, a Chinese company was ahead in market share. Moreover, search in China was not a big source of revenue for Google.

Attacks designed to steal the intellectual property of foreign companies were not uncommon in China, but experts detected a new level of audacity against thirty three companies after July 2009 using sophisticated zero day attacks. It may have looked like China upped the ante, and unlike low tech companies with little choice if they wanted to stay in the China market, Google needed to preserve the soft power of its reputation for supporting freedom of expression to recruit and nurture creative personnel, and the security reputation of its Gmail brand.

At this point the American government became involved. Google alerted the White House before its announcement. Secretary of State Hillary Clinton had already been planning a speech on internet freedom, and adding the Google example raised the issue to the intergovernmental level. The Chinese government initially dismissed the issue as a commercial dispute, but the American government involvement led to political statements about the need to obey Chinese laws and complaints about American cyber imperialism.[60] Other officials referred to American efforts to maintain hegemony over internet. At the same time, other Chinese view were expressed. Some citizens deposited flowers on Google's logo, and others worried that Google's exit would hurt China if Baidu became a monopoly. "When the Chinese companies go outside of China, they will find that they fail to understand their competitors as well as they did when they were competing in China."[61] In March 2010, Google ceased its Chinese language search service inside China, and the Chinese government reasserted the supremacy of Chinese laws.

The American government, however, had used the case to ask for new norms on the internet. At the same time, it failed to say what the United States would stop doing. Many intrusions into Chinese and American computer systems are reciprocal. "Simply put, the United States is in a big way doing the very things that Secretary Clinton criticized. The U.S. is not, like the Chinese, stealing intellectual property from U.S. firms or breaking into the accounts of democracy advocates. But it aggressively uses the same or similar computer techniques for ends it deems worthy."[62] One survey of cyber experts found that the United States was the largest source of global intrusions, followed closely by China.[63] Some portion were undoubtedly by the government, but others were by private hacktivists trying to advance human rights and internet freedom in China and elsewhere in the world. Would the US be able or willing to control such hactivists? It seems unlikely in human rights cases, yet China's government sees Tibetan exiles and Falun Gong hackers as national security threats. In principle one could imagine some areas in which Chinese and American goals overlap in reality and in perception, but a private company's initiative that linked intellectual property theft and human rights hacking certainly led to a more complex political situation. Companies, governments, and individuals hackers all used various instruments available to them to struggle for their preferred outcomes in this aspect of the cyber domain.

Governments and Governance

Some see cyberspace as analogous to the ungoverned lawless Wild West, but in practice there are many areas of private and public governance. Certain technical standards related to the internet protocol are set (or not) by consensus among engineers involved in the non-governmental IETF (Internet Engineering Task Force). Whether such standards are broadly applied often depends upon private corporate decisions about their inclusion in commercial products. A non-governmental World Wide Web Consortium develops standards for the Web. The Internet Corporation for Assigned Names and Numbers (ICANN) has the legal status of a non-profit cor-

poration under American law, though its procedures have evolved to include government voices (though not votes). In any event, its mandate is limited to domain names and routing management, not the full panoply of cyberspace governance. National governments control copyright and intellectual property laws, though they are subject to negotiation and litigation, sometimes within the frameworks of the World Intellectual Property Organization and the World Trade Organization. Governments also determine national spectrum allocation within an international framework negotiated at the International Telecommunications Union (ITU). Above all, national governments try to manage problems of security, espionage, and crime within national legal frameworks, though the technological volatility of the cyber domain means that laws and regulations are always chasing a moving target. The imperfect governance of cyberspace can be categorized as a "regime complex" of loosely coupled norms and institutions somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages.[64]

The cyberspace domain is often described as a public good or a global commons, but these terms are an imperfect fit. A public good is one from which all can benefit and none excluded, and while this may describe some of the information protocols of the internet, it does not describe the physical infrastructure which is a scarce resource located within the boundaries of sovereign states. And cyberspace is not a commons like the high seas because parts of it are under sovereign control. At best, it is an "imperfect commons" or a condominium of joint ownership without well developed rules.[65]

Cyber space can be categorized as what Elinor Ostrom terms a "common pool resource" from which exclusion is difficult and exploitation by one party can subtract value for other parties.[66] Physical bandwidth and trust in information are shared resources. Government is not the sole solution to such common pool resource problems. Ostrom shows that community self organization is possible under certain conditions. However, the conditions that she associates with successful self -governance are weak in the cyber domain because of the large size of the resource, the large number of users, and the poor predictability of system dynamics (among others). In its earliest days, the internet was like a small village of known users, and an authentication layer of code was not necessary and development of norms was simple. All that changed with burgeoning growth. While the openness and accessibility of cyberspace as a medium of communication provide valuable benefits to all, disruptive behavior in the form of crime, attacks, and threats creates insecurity. The result is a demand for protection that can lead to fragmentation, "walled gardens," private networks, and cyber equivalents to the 17th century enclosures that were used to solve the that era's tragedy of the commons.[67]

Providing security is a classic function of government, and some observers believe that increasing insecurity will lead to an increased role for governments in cyberspace. Many states desire to extend their sovereignty in cyberspace, and seek technological means to do so. As two experts have put it, "securing cyberspace has definitely entailed a 'return of the state' but not in ways that suggest a return to the traditional Westphalian paradigm of state sovereignty." Efforts to secure the network help to facilitate its use by burgeoning non-state actors, and often entail devolution of responsibilities and authority to private actors.[68] For examples, banking and financial firms have developed their own elaborate systems of security and punishment through networks of connectedness, such as depriving repeat offenders of their trading rights, and raising

of transactions for suspect addresses. Governments want to protect the internet so their societies can continue to benefit, but at the same time, they want to protect their societies from what comes through the internet. China, for example, is described as developing its own companies that it can control behind its firewall, and planning to disconnect from the global Internet if it is attacked.[69] Nonetheless, China — and other governments — still seek the economic benefits of connectivity. The tension leads to imperfect compromises.[70]

If one treats most hacktivism as a nuisance, there are four major cyber threats to national security, each with a different time horizon and with different (in principle) solutions: economic espionage, crime, cyber war, and cyber terrorism. For the United States, at the present time, the highest costs come from the first two categories, but over the next decade, the order may be reversed. According to President Obama's 2009 cyber review, theft of intellectual property by other states (and corporations) was the highest immediate cost. Not only did it result in current economic losses, but by destroying competitive advantage, it jeopardized future hard power.[71] As we saw above, cyber criminals are also a significant current burden on the economy. Looking further ahead, as other states develop their capacities for cyber attack on critical infrastructures and are able to deprive American military forces of their information advantages, the costs to American hard power could be significant. And as terrorist groups that wish to wreak destruction develop their capacity to do so, they could impose dramatic costs. The remedies for each threat are quite different.

Cyber war can be managed through inter-state deterrence, and offensive capabilities plus resilience if deterrence fails. At some point in the future, it may be possible to reinforce these steps with evolving rudimentary norms.[72] In the case of war, fighting would be subject to the discrimination and proportionality criteria of existing laws of armed conflict, though there are problems of distinguishing civilian from military targets, and being sure about the extent of collateral damage. Some observers argue that because of the difficulty of attribution of the source of an attack, deterrence does not work in cyber space. However, while interstate deterrence is more difficult in cyber, it is not impossible.

Many think of deterrence in terms of the nuclear model that prevailed for the past half century, in which the threat of punitive retaliation is so catastrophic that it deters attack. But nuclear deterrence was never this simple. While a second strike capability and mutual assured destruction may have worked to prevent attacks on the homeland, they were not credible for issues at the low end of the spectrum of interests. Lying somewhere in between these extremes lay extended deterrence of attacks against allies and defense of vulnerable positions such as Berlin in the Cold War. Nuclear deterrence was supplemented by other measures (such as forward basing of conventional forces); a variety of signaling devices in the movement of forces, and a learning process that occurred over the decade and led to areas of agreements ranging from non-proliferation to managing incidents at sea.

Cyber attacks lack the catastrophic dimensions of nuclear weapons attacks, and attribution is more difficult, but inter-state deterrence still exists. Even when the source of an attack can be successfully disguised under a "false flag," other governments may find themselves sufficiently entangled in interdependent relationships that a major attack would be counterproductive. Unlike the

single strand of military interdependence that linked the U.S. and the Soviet Union in the Cold War, the United States, China, and other countries are entangled in multiple networks. China, for example, would itself lose from an attack that severely damaged the American economy, and visa versa.

In addition, an unknown attacker may be deterred by denial. If firewalls are strong, or the prospect of a self enforcing response seems possible ("an electric fence"), attack becomes less attractive. Offensive capabilities for immediate response can create an active defense that can serve as a deterrent even when the identity of the attacker is not fully known. Futility can also help deter an unknown attacker. If the target is well protected, or redundancy and resilience allow quick recovery, the risk to benefit ratio in attack is diminished. Finally, to the extent that false flags are imperfect, and rumors of the source of an attack are widely deemed credible (though not probative in a court of law) reputational damage to an attacker's soft power may contribute to deterrence.

Cbyer terrorism is a harder case. As we have seen, cyber attacks are not the most attractive route for terrorists today, but as groups develop their capacity to wreak great damage against infrastructure over the coming years, the temptation will grow. Since attribution will be difficult, improved defenses such as pre-emption and human intelligence become important. At a more fundamental level, many experts believe that the long term solution is a program to re-engineer the internet to make such attacks more difficult than under today's structure that emphasizes ease of use rather than security. Some suggest special "opt in" incentives for private owners of critical infrastructure (eg., finance and electricity) to join secure systems rather than rely on the open internet (which would continue to exist for those with lower stakes and willing to tolerate greater risks.)

Cyber crime can also be reduced by similar approaches that make access to some systems more difficult than they are today. In addition, it may be possible to develop degrees of international cooperation to limit cyber crime analogous to efforts to discourage piracy at an earlier era. At one time, many governments found it convenient to tolerate some pirates and even charter privateers (until the Declaration of Paris in 1856), and today some governments have similar attitudes toward crime on the internet. Russia and China, for example, have refused to sign the Council of Europe Convention on Cyber Crime which has been signed by 27 countries. But attitudes may change over time if costs exceed benefits. For example, "Russian cyber-criminals no longer follow hands-off rules when it comes to motherland targets, and Russian authorities are beginning to drop the laisser faire policy."[73] While the immediate prospects for the convention are not promising, it is possible to imagine coalitions of the willing that set a higher standard, and work together to raise the costs for those who violate an emergent norm, much as occurs with financial money laundering regulations or the proliferation security initiative.

Internet espionage is likely to continue unabated unless there are new state approaches. Spying is as old as human history, and does not violate any explicit provisions of international law. Nonetheless, at times governments have established rules of the road for limiting espionage, and engaged in patterns of tit for tat retaliation to create an incentive for cooperation. Experiments have shown that partners in prisoners dilemma and public goods games can develop cooperation in repeated play over extended periods.[74] While it is difficult to envisage enforceable treaties in

which governments agree not to engage in espionage, it is plausible to imagine a process of iterations (tit for tat) which develop rules of the road which could limit damage in practical terms. In the words of Howard Schmidt, the American cyber security chief, "one of the key things has been going back to the countries that it appears its coming from and saying: if it's not you, you need to investigate this."[75] Failure to respond can be followed by measured retaliation. Under international legal doctrine, proportionate countermeasures can be taken in response to harm originating from a state even if the government is not behind it. While less than perfect, efforts can be made to deal with non-state actors by holding states responsible for actions that originate within their sovereign boundaries. To avoid escalation or "defection lock-in," it helps to offer assistance and to engage in discussions that can develop common perceptions, if not fully agreed norms. Such "learning" is still at an early stage in the cyber domain.[76]

At this stage, large scale formal treaties regulating cyber space seem unlikely. Over the past decade, the UN General Assembly has passed a series of resolutions condemning criminal activity and drawing attention to defensive measures that governments can take. For more than a decade, Russia has sought a treaty for broader international oversight of the Internet, banning deception or the embedding of malicious code or circuitry that could be activated in the event of war. But Americans have argued that measures banning offense can damage defense against current attacks, and would be impossible to verify or enforce. Moreover, the United States has resisted agreements that could legitimize authoritarian governments' censorship of the internet. Nonetheless, the United States has begun informal discussions with Russia.[77] Even advocates for an international law for information operations are skeptical of a multilateral treaty akin to the Geneva Conventions that could contain precise and detailed rules given future technological volatility, but they argue that like minded states could announce self governing rules that could form norms for the future.[78]

Normative differences present a difficulty in reaching any broad agreements on regulating content on the internet. As we saw earlier, the United States has called for the creation of "norms of behavior among states" that "encourage respect for the global networked commons," but as Jack Goldsmith has argued, "even if we could stop all cyber attacks from our soil, we wouldn't want to. On the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense."[79] From the American point of view, Twitter and YouTube are matters of personal freedom; seen from Beijing or Teheran, they are instruments of attack. Even on the issue of child pornography where norms of condemnation are broadly shared, governments are more likely to act unilaterally through national filtering technologies rather than issuing a take-down notice to the service provider and relying on legal prosecution by the hosting state. For example, Australia has imposed "some of the toughest internet filters proposed by any established democracy."[v] Self help remains the dominant norm.

Conclusion

Struggles among governments, corporations, and individuals are not new, but the low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics. Changes in information have always had an important impact on power, but the cyber domain is both a new and a volatile manmade environment. The characteristics of cyberspace reduce some of the power differentials among actors, and thus provide a good example of the diffusion of power that typifies global politics in this century. The largest powers are unlikely to be able to dominate this domain as much as they have others like sea or air. But cyberspace also illustrates the point that diffusion of power does not mean equality of power or the replacement of governments as the most powerful actors in world politics. While cyberspace may create some power shifts among states by opening limited opportunities for leapfrogging by small states using asymmetrical warfare, it is unlikely to be a game changer in power transitions. On the other hand, while leaving governments the strongest actors, the cyber domain is likely to increase the diffusion of power to non-state actors, and illustrates the importance of networks as a key dimension of power in the 21st century.

Notes

1 Richard Haass, "The Age of Nonpolarity," *Foreign Affairs*, May/June 2008

2 Alvin Toffler and Heidi Toffler, *The Politics of the Third Wave*, (Kansas City, Andrews and McMeel, 1995); Esther Dyson, *Release 2.1: A Design for Living in the Digital Age* (New York, Broadway, 1998)

3 *The Economist*, "Data, data, everywhere," Special report on managing information, February 27,2010, p4

4 For a classic exploration of this problem, see James G. March, "The Power of Power," in David Easton, ed., Varieties of Political Theory (Englewood Cliffs, NJ: Prentice-Hall, 1966), 39-70. Other classic articles on power by Robert Dahl, John C. Harsanyi, Hebert Simon and others are collected in Roderick Bell, David V. Edwards and R. Harrison Wagner, eds., Political Power: A Reader in Theory and Research (New York: Free Press, 1969). For a more recent survey, see David A. Baldwin, "Power and International Relations," in Walter Carlsnaes, Thomas Risse, and Beth A. Simmons, eds. *Handbook of International Relations* (London: Sage Publications, 2002),

5 John Harsanyi, "The Dimension and Measurement of Social Power," reprinted in K.W. Rothschild, *Power in Economics* (Harmondsworth, Penguin Books, 1971), p. 80

6 Max Weber, *The Theory of Social and Economic Organization* (New York: Oxford UP, 1947), 152.

7 Jack Nagel, *The Descriptive Analysis of Power*, (New Haven, Yale University Press, 1975), p. 14

8 Peter Digeser has used the term "fourth face" to refer to Michel Foucault's view that subjects and social practices are the effects of a power that one cannot escape, and knowledge presupposes power, but he admits that "Foucault's use of power departs significantly from ordinary usage." See "The Fourth Face of Power," *The Journal of Politics* 54, 4 (November 1992), 990. See also Michael Barnett and Raymond Duvall, "Power in International Politics," *International Organization* 59 (Winter 2005), 39-75 for an abstract fourfold typology that also goes beyond the three "faces of power" categories.

9 Robert A. Dahl, *Who Governs: Democracy and Power in an American City* (New Haven: Yale UP, 1961).

10 Peter Bachrach and Morton Baratz, "Decisions and Nondecisions: An Analytical Framework," *American Political Science Review* (September 1963), 632-42. William H. Riker developed a somewhat similar concept that he called "herestetics" which "involves structuring the situation so that others accept it willingly." See "The Heresthetics of Constitution-Making: The Presidency in 1787, with Comments on Determinism and Rational Choice," *American Political Science Review* 78, 1 (March 1984), 8.

11 Steven Lukes, Power: *A Radical View*, 2nd ed., London, Palgrave

12 For elaboration of his argument, see J.S. Nye, *Soft Power: The Means to Success in World Politics*, (New York, Public Affairs Press, 2004)

13 Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009).

14 Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in Kramer, cited, 52.

15 See Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford UP, 2006).

16 Libicki distinguishes three layers: physical, syntactic and semantic. See Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009), 12. However, with applications added upon applications, the internet can be conceived in multiple layers. See Marjory Blumenthal and David D.Clark, "The Future of the Internet and Cyberpower," in Kramer, cited.

17 I am indebted here to Jeffrey R. Cooper and his unpublished work on "New Approaches to Cyber-Deterrence"

18 Kuehl, in Kramer, cited, 38.

19 Ellen Nakashima and Brian Krebs, "Obama Says He Will Name National Cybersecurity Advisor," *Washington Post*, May 30, 2009.

20 See Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in Kramer, cited, 253-274, esp. 256.

21 Franklin Kramer, "Cyberpower and National Security," in Kramer, cited, 12.

22 LTC David E. A. Johnson and Steve Pettit, "Principles of the Defense for Cyber Networks," *Defense Concepts* 4, 2 (Jan 2010), 17.

23 Martin C. Libicki, *Cyberdeterrence and Cyberwarfare* (Santa Monica: RAND, 2009), xiii. See also William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009).

24 Interviews with US government officials, March 2010.

25 Goldsmith and Wu, cited, 180 ff.

26 "Don't mess with us," *The Economist*, January 2, 2010, 31.

27 Robert F. Worth, "Opposition in Iran Meets a Crossroads On Strategy," *New York Times*, February 15, 2010.

28 As documented by the Open Net Initiative. Richard Waters and Joseph Menn, "Closing the frontier," *Financial Times*, March 29, 2010.

29 Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, 1 (March 2010), 25-27.

30 Sharon LaFraniere and Jonathan Ansfield, "Cyberspying Fears Help Fuel China's Drive to Curb Internet," *New York Times*, February 12, 2010.

31 See Goldsmith and Wu, cited, 115; and Jonathan Zittrain, "A fight over freedom at Apple's core," *Financial Times*, February 4, 2010.

32 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

33 Goldsmith and Wu, cited, 165.

34 General Keith Alexander, head of Cyber Command, testimony to the Senate Armed Services Committee . No author, " Attacks on Military Computers Cited," *New York Times*, April 16, 2010.

35 McAfee Report, "Unsecured Economies: Protecting Vital Information," Davos, 2009. See also, Tim Weber, "Cybercrime threat rising sharply," BBC News website. http://news.bbc.co.uk/2/hi/business/davos/7862549.stm

36 Munk Centre for International Studies, University of Toronto, "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor* (March 2009).

37 Sharon LaFraniere and Jonathan Ansfield, "Cyberspying Fears Help Fuel China's Drive to Curb Internet," *New York Times*, February 12, 2010.

38 Stanley Pignal, "US presses Brussels on terror data swaps," *Financial Times*, February 3, 2010.

39 See Owens, Dam, and Lin, eds., cited.

40 Richard Clarke, "War From Cyberspace," *The National Interest* online, October 27, 2009.

41 See for example, John Markoff, "Old Trick Threatens Newest Weapons," *New York Times*, October 27, 2009; and Shane Harris, "The Cyberwar Plan," *National Journal*, November 14, 2009, 18ff.

42 Richard A. Clarke and Robert K. Knake, *Cyberwar* (New York: Harper Collins, 2010), Chapter 1.

43 See Owens, Dam, and Lin, eds., cited above, p 27

44 Interviews with U.S. government officials, March 2010.

45 "Clash of the Clouds," *The Economist*, October 17, 2009, 81.

46 Steve Lohr, "Global Strategy Stabilized IBM During Downturn," *New York Times*, April 20, 2010.

47 See Tyler Moore and Richard Clayton, "The Impact of Incentives on Notice and Take-down," Seventh Workshop on the Economics of Information Security (June 2008), http://weis2008.econinfosec.org/MooreImpac.pdf.

48 Testimony of Steven R. Chabinsky before the Senate Judiciary Committee Subcommittee on Terrorism and Homeland Security, November 17, 2009.

49 Frederick R. Chang, "Is Your Computer Secure?" *Science* 325 (July 2009), 550.

50 Chris Bronk, "Toward Cyber Arms Control with Russia," *World Politics Review*, January 19, 2010.

51 McAffee Inc., *Virtual Criminology Report 2009* (Santa Clara, CA: 2009), 12.

52 Clay Wilson, "Cybercrime," in Kramer, cited, 428.

53 Irving Lachow, "Cyber Terrorism: Menace or Myth?" in Kramer, cited, 450.

54 Robert K. Knake, "Cyberterrorism Hype v. Fact," Council on Foreign Relations Expert Brief, February 16, 2010, http://www.cfr.org/publication/21434/cyberterrorism_hype_v_fact.html.

55 McConnell quoted in Jill R. Aitoro, "Terrorists nearing ability to launch big cyberattacks against the U.S," *Nextgov*, October 2, 2010, http://www.nextgov.com/site_services/print_article.php?StoryID=ng_20091002_9081

56 Olivier Roy, "Recruiting Terrorists," *International Herald Tribune*, January 11, 2010.

57 McAfee Inc., cited, 6. See also Project Grey Goose, "Russia/Georgia Cyber War – Findings and Analysis," October 17, 2008, intelfusion@hush.com.

58 Michael B. Farrell, "Iranian Cyber Army Hack of Twitter Signals Cyberpolitics Era," *The Christian Science Monitor*, December 18, 2009, http://www.csmonitor.com/layout/set/print/content/view/print/269741.

59 See Kathrin Hille and Joseph Menn, "Patriotism and politics drive China cyberwar," Financial Times, January 14, 2010; John A. Quelch, "Looking Behind Google's Stand in China," Harvard Business School, *Working Knowledge*, February 8, 2010. I am also endebted to an unpublished paper by Roger Hurwitz, February 2010.

60 Mark Landler and Edward Wong, "China Says Clinton Harms Relations With Criticism of Internet Censorship," *New York Times*, January 23, 2010.

61 David Barboza, "China's Booming Internet Giants May be Stuck There," *New York Times*, March 24, 2010.

62 Jack Goldsmith, "Can we stop the global cyber arms race?" *Washington Post*, February 1, 2010.

63 John Markoff, "Cyberattack Threat on Rise, Executives Say," *New York Times*, January 29, 2010.

64 Robert O. Keohane and David G. Victor, "The Regime Complex for Climate Change," Discussion Paper, Harvard Project on International Climate Agreements (Cambridge: Belfer Center for Science and International Affairs, 2010).

65 The metaphor is from James A. Lewis. See also, "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" (Washington, D.C.: Center for Strategic International Studies, 2008).

66 See Elinor Ostrom, Joanna Burger, Christopher Field, Richard Norgaard, and David Policansky, "Revisiting the Commons: Local Lessons, Global Challenges," *Science* 284, 5412 (April 1999), 278, for a challenge to the Garrett Hardin's 1968 formulation of "The Tragedy of the Commons," *Science* 162, 3859 (December 1968), 1243.

67 Elinor Ostrom, "A General Framework for Analyzing Sustainability of Social-Ecological Systems," *Science* 325 (July 2009), 421. See also Roger Hurwitz, "The Prospects for Regulating Cyberspace," unpublished paper, November 2009.

68 Deibert and Rohozinski, cited, 30.

69 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, cited above, p146

70 See Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven: Yale UP, 2008).

71 See Melissa Hathaway, "Strategic Advantage: Why America Should Care About Cybersecurity," Discussion Paper, Harvard Kennedy School (Cambridge: Belfer Center for Science and International Affairs, 2009). See also Barack Obama, cited, May 29, 2009.

72 See Clarke and Knake, cited above, for a discussion of the limits of arms control, and possible norms.

73 Joseph Menn, "Moscow gets tough on cybercrime," *Financial Times*, March 22, 2010.

74 Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984). See also David Rand, Anna Drebner, Tore Ellingsen, Drew Fudenberg, and Martin Nowak, "Positive Interactions Promote Public Cooperation," *Science* 325 (September 2009), 1272.

75 Joseph Menn, "US cybercrime chief wary on provoking China and Russia," *Financial Times*, March 5, 2010.

76 For a description of the gradual evolution of the learning that occurred in the nuclear area, see Joseph Nye, "Nuclear Learning and U.S.-Soviet Security Regimes," *International Organization* 41, 3 (Summer 1987).

77 John Markoff, "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia," *New York Times*, April 16, 2010

78 Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis and Clark Law Review* 11, 4 (2007), 1059.

79 Jack Goldsmith, "Can We Stop the Global Cyber Arms Race," cited.

80 Waters and Menn, cited.

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org