

Cyber Power

By Joseph S. Nye, Jr.

For a concept that is so widely used, “power” is surprisingly elusive and difficult to measure.¹ 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.”² In Max Weber’s view, we want to know the probability that an actor in a social relationship can carry out his own will.³ Even when we focus primarily on particular agents or actors, we cannot say that an actor “has power” without specifying power “to do what.”⁴ 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.) 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.” The first aspect or “face” of power was defined by the Yale political scientist Robert Dahl in studies of New Haven in the 1950s, and it 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. 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.

One can also distinguish power along a spectrum to command to coercive behavior. If power is the ability to affect others to obtain the outcomes one prefers, one can affect others through coercion and payment or attraction and persuasion. Hard power behavior rests on coercion and payment. Soft power behavior rests on framing agendas, attraction or persuasion. The spectrum of behaviors is represented below. ⁵

Hard Soft

Command> Coerce Threat Pay Sanction Frame Persuade Attract <Co-opt

For example, suppose a school principal does not want a teenager to smoke. Under the first face of power, the principal could threaten the student with fines or expulsion to change her desire to smoke (hard power) or spend hours persuading her not to smoke (soft power). Under the second face, the principal could ban cigarette vending machines (a hard aspect of agenda control) or use public service advertisements about cancer and yellow teeth to create a climate of opinion where smoking becomes unpopular and unthinkable (soft power). Under the third dimension of power behavior, the principal could hold a school assembly in which students discuss smoking and vow not to smoke (soft power), or go further and threaten to ostracize the minority who smoke (hard power). In other words, the principal can use her hard power to stop students' smoking, or use the soft power of framing, persuasion and attraction. The success of her soft power efforts will depend upon her ability to attract and create credibility and trust.

Even large countries with impressive hard power, 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 be a sovereign state or a powerful country.

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.”⁶ 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 are created about that time. The World Wide Web begins in 1989; Google the most popular search engine is 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.⁷ 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 still play a major role, but the domain is marked by extreme power diffusion.⁸

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.⁹ 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. 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 can be defined in terms of a set of resources that relate to the creation, control and communication of electronic and computer based information -- infrastructure, networks, software, human skills, but this has the limitations of any definition of power in terms of resources. 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.”¹⁰ 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.¹¹

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.”¹² 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.”¹³ While a few large states like the United States, Russia, and China 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.”¹⁴ The offense has the advantage over the defense. The larger party cannot disarm or destroy the enemy, occupy territory, or effectively use counter-force strategies. Deterrence is limited and difficult 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.”¹⁵

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 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 of corrupted computers that swamps 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 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, Latvia suffered a distributed denial of service attack that was widely attributed to “patriotic hackers” in Russia who were offended by Latvia’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. 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 government 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 proxy servers in other countries to make attribution difficult. For example, many of the attacks on Latvian and Georgian targets were routed through American servers.¹⁶

Cyber information can also travel through cyberspace to create soft power by attracting citizens in another country. A public diplomacy campaign over the internet such as we described in Chapter 4 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 as costly as 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." The threat of lawsuits made Yahoo control what it sent to France and Google remove 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 to lose 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.¹⁷

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 other governments to create information firewalls to block them. 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 the table 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 2007 protesters in Washington marched and demonstrated against Yahoo and other internet companies that had provided the names of Chinese activists to the Chinese government.

Another way of looking at power in the cyber domain is to consider the three faces or aspects of relational power described in Chapter 1.

Table 2
Three Faces of Power in the Cyber Domain

1st face: (A makes 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: delegitimize some ideas (eg. Falun Gong) and punish dissemination

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 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.”¹⁸

In terms of soft power, an individual or organization might attempt 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.¹⁹ 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. By some estimates, at least [] countries use highly restrictive filters and firewalls to prevent the discussion of suspect materials.²⁰ Sometimes this is accepted and sometimes not. If the filtering is secretive, it is hard for citizens to know what they do not know. 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.”²¹ 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.²²

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, “code becomes law”, and few consumers

notice.²³ 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 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 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.²⁴ The United States government suffered millions of intrusions into its computer systems last year. Criminal groups are said steal over \$1 trillion via the internet in a year. 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.²⁵ 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. 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, but this is a

useful first approximation for descriptive purposes.) Governments, and particularly large governments, remain the most powerful.

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 disruptable 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

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 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.²⁶ In 2010, 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.”²⁷

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 internet activity that only lightly touched on 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.²⁸ For example, America's Tenth Fleet and Twenty-fourth Air Force have no ships or planes. Their battlefield is cyberspace.²⁹ Unfortunately, news accounts of “millions of attacks” use the term “attack” loosely to refer to everything from hacking (illegal computer trespassing) or 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 a few 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,³⁰ but little is known publicly about “preparation of the battlefield” for what could be future conflicts. Both American and Chinese military theorists have discussed such steps (as we saw in Chapter 2), but little is confirmed. Presumably many large governments engage in such activity, though the success of such attacks will 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.

Cyber attacks that deny service or disrupt systems are also carried out by non-state actors whether for ideological or criminal purposes, but it is unclear that such groups 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 may 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.

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.³¹ Amazon, Google, Microsoft, and others are competing in the development of cloud computing, and have server farms with more than 50,000 servers. Their transnational structure allows them to exploit markets and resources around the globe. At the same time, to preserve their legal

status as well as their brand equity, they 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.³² 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.³³ Up to a quarter of network-connected computers may be part of a botnet, and some botnets include millions of computers. Cyber crime may cost companies over a trillion dollars a year.³⁴ Some criminal groups, such as the so called “Russian Business Network” may have inherited some capabilities of the Soviet state after its dissolution. Moreover, “the hacking skills of criminal groups may make them natural allies or nation-states looking for a way to deny involvement in cyber attacks.”³⁵ The scale of some criminal operations is expensive and costly. In 2006, the US Government Accountability Office estimated losses caused by cybercrime at \$50 billion, with only five percent of cybercriminals ever arrested or convicted.³⁶

Terrorist groups make active use of cyber tools, 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.”³⁷ Others are not so sanguine. For example, Mike McConnell, former Director of National Intelligence believes “when terrorist groups have the sophistication, they’ll use it.”³⁸

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. 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.”³⁹ While governments can monitor and interfere with these virtual networks, skilled operatives have learned various techniques of deception in the game of cat and mouse.

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.”⁴⁰ 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.⁴¹

Thinking back to our discussion in Chapter 3 of the ways in which asymmetrical interdependence helps to produce power, 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 disruptable 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 disproportionate 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 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.⁴² 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); efforts to break into the G-mail 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 G-mail 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. Moreover, search in China was not a big source of revenue for Google.

No one can be sure why Google acted as it did. 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.⁴³ 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. The Shanghai city government worried about its reputation and the forthcoming World Fair. After a few weeks, both China and Google adopted a lower profile.

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 Clinton criticized. We are not, like the Chinese, stealing intellectual property from U.S. firms or breaking into the accounts of democracy advocates. But we are aggressively using the same or similar computer techniques for ends we deem worthy."⁴⁴ One survey of cyber experts found that the United States was the largest source of global intrusions, followed closely by China.⁴⁵ Some portion were undoubtedly by the government, but others were by private hackers 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 hackers? It seems unlikely in human rights cases, yet China's government sees Tibetan exiles and Falun Gong hackers as 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.

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 has always had an important impact on power, but the cyber domain is both a new and 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. 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 that we will turn to in the next chapter. 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.

¹ Steven Lukes, *Power: A Radical View*, 2nd ed., London, Palgrave,

² John Harsanyi, "The Dimension and Measurement of Social Power," reprinted in K.W. Rothschild, *Power in Economics* (Harmondsworth, Penguin Books, 1971), p. 80

³ Max Weber, 1947 p. 152

⁴ Jack Nagel, *The Descriptive Analysis of Power*, (New Haven, Yale University Press, 1975), p. 14

⁵ For elaboration of this argument, see J.S. Nye, *Soft Power: The Means to Success in World Politics*, (New York, Public Affairs Press, 2004)

⁶ 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, National Defense University Press, 2009,

⁷ Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in Kramer et al., eds, cited, p 52

⁸ See Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford, Oxford University Press, 2006

-
- ⁹ Libicki distinguishes three layers: physical, syntactic and semantic. See Martin Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, RAND, 2009. p 12; but 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, et al. eds, *Cyberpower and National Security*
- ¹⁰ Kuehl, in Kramer, cited above, p. 38
- ¹¹ Ellen Nakashima and Brian Krebs, "Obama Says He Will Name National Cybersecurity Advisor," *Washington Post*, May 30, 2009.
- ¹² See Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in Kramer et al, eds. *Cyberpower and National Security*, pp253-274, especially p 256.
- ¹³ Franklin Kramer, "Cyberpower and National Security," in Kramer et al, eds., p. 12
- ¹⁴ LTC David E. A. Johnson and Steve Pettit, "Principles of the Defense for Cyber Networks," *Defense Concepts*, Vol 4, No 2, p. 17.
- ¹⁵ Martin C. Libicki, *Cyberdeterrence and Cyberwarfare*, Santa Monica, RAND, 2009, p 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, National Academies Press, 2009.
- ¹⁶
- ¹⁷ Goldsmith and Wu, cited above, p. 180 ff
- ¹⁸ "Don't mess with us," *The Economist*, January 2, 2010, p. 31
- ¹⁹ Goldsmith and Wu, cited above, p 99
- ²⁰ [Berkman Center data]
- ²¹ Sharon LaFraniere and Jonathan Ansfield, "Cyberspying Fears Help Fuel China's Drive to Curb Internet," *New York Times*, February 12, 2010.
- ²² See Goldsmith and Wu, p. 115, and Jonathan Zittrain, "A fight over freedom at Apple's core" *Financial Times*, February 4, 2010
- ²³ Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999
- ²⁴ Goldsmith and Wu, p. 165
- ²⁵ Munk Centre for International Studies, University of Toronto, *Tracking GhostNet: Investigating a Cyber Espionage Network*, Toronto, March 2009 <http://www.inforwar-monitor.net/ghostnet>
- ²⁶ Sharon LaFraniere and Jonathan Ansfield, "Cyberspying Fears Help Fuel China's Drive to Curb Internet," *New York Times*, February 12, 2010
- ²⁷ Stanley Pignal, "US presses Brussels on terror data swaps," *Financial Times*, February 3, 2010
- ²⁸ See NAS study cited above.
- ²⁹ Richard Clarke, "War From Cyberspace," *The National Interest* online, October 27, 2009.
- ³⁰ 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, p 18ff
- ³¹ "Clash of the Clouds," *The Economist*, October 17, 2009, p. 81
- ³² 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>
- ³³ Testimony of Steven R. Chabinsky before the Senate Judiciary Committee Subcommittee on Terrorism and Homeland Security, November 17, 2009.
- ³⁴ Frederick R. Chang, "Is Your Computer Secure?" *Science*, vol 325, July 31, 2009, p. 550
- ³⁵ McAfee Inc, *Virtual Criminology Report 2009*, Santa Clara, CA, 2009, p 12
- ³⁶ Clay Wilson, "Cybercrime," in Kramer et al, eds., cited above, p. 428
- ³⁷ Irving Lachow, "Cyber Terrorism: Menace or Myth?" in Kramer et al, eds. p 450
- ³⁸ 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
- ³⁹ Olivier Roy, "Recruiting Terrorists," *International Herald Tribune*, January 11, 2010
- ⁴⁰ McAfee Inc, *Virtual Criminology Report*, 2009, cited above, p.6 See also Project Grey Goose (intelfusion@hush.com) "Russia/Georgia Cyber War – Findings and Analysis," October 17, 2008.
- ⁴¹ 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>

⁴² 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

⁴³ Mark Landler and Edward Wong, “China Says Clinton Harms Relations With Criticism of Internet Censorship,” *New York Times*, January 23, 2010.

⁴⁴ Jack Goldsmith, “Can we stop the global cyber arms race?” *Washington Post*, February 1, 2010

⁴⁵ John Markoff, “Cyberattack Threat on Rise, Executives Say,” *New York Times*, January 29, 2010