CHAPTER VI:
CULTIVATING INTERNATIONAL CYBER NORMS

By Martha Finnemore

CULTIVATING INTERNATIONAL CYBER NORMS

Martha Finnemore

Coordinating activity in cyberspace has become a crucial challenge. Virtually every sector of society in a wide array of countries now relies on Internet communication to carry out the most basic functions of modern life. Businesses, militaries, government at all levels and citizen groups of every imaginable kind now depend heavily on, and indeed cannot function without, an efficient and secure Internet.

This varied array of stakeholders holds a varied set of ideas about how cyberspace should be used and governed. Military and security professionals envision using the Internet to coordinate counter-terrorist activities and combat organized crime. They want rules to allow these actions. However, this alarms many privacy advocates who, in turn, want rules to protect against precisely this kind of surveillance. Meanwhile, various national governments hold different views about the legitimate uses of the Internet and are pushing hard for rules that reflect their preferred vision. For example, governments in Russia and China see internal dissent and anti-government writings disseminated on the Internet as a threat. Both have curtailed free speech and access to the Internet as part of their vision of "cyber security" – a view the United States is not likely to embrace. Without some basic "rules of the road," conflict between these competing values and visions will intensify. The essential resource of cyberspace cannot reliably perform the functions that we all depend on without agreed upon Internet norms.

This chapter analyzes the tasks involved in cultivating new norms and rules for cyberspace. Drawing on efforts to develop norms on other issues, we can see broad patterns in the kinds of norms that are likely to succeed and the strategies that are likely to prevail. Findings of this chapter include:

- Successful norms are likely to be simple and clear, obviously useful and relatively easy to follow. Overly complex and technical prescriptions

are unlikely to reach the very broad audience needed to ensure some of the most basic elements of a safe and secure cyberspace.[1]

- "Grafting" cyber norms onto existing, well-established normative frameworks, for example human rights norms or laws of war, may increase chances of success. Building on existing norms can help to make the new cyber norms seem intuitive and sensible to diverse audiences and enhances compliance.
- Multipronged and multilevel approaches to norm dissemination also seem particularly suited to cyber security. Pushing for new norms in multiple venues, among diverse audiences simultaneously will probably yield more timely progress than concentrating on some single norm-building enterprise, like a single treaty negotiation.
- Where possible, norms can and should be buttressed by appropriate laws at national, local and even international levels. Norms and formal laws should be treated as complementary tools, and a judicious use of both will yield the best results.
- Technical assistance and funding to help key actors "do the right thing" in cyberspace will greatly increase compliance.

These strategies may seem intuitive and obvious, but are difficult to implement. The cyber realm presents some unique challenges for norm development. Few issue areas penetrate every aspect of society as thoroughly as the Internet. Coordinating such diverse stakeholders with such varied values will not happen quickly or easily. To illustrate some of the challenges, this chapter briefly analyses norm promotion issues in two areas: developing norms around civilian protection and Internet freedom. Cultivating cyber norms may best be viewed a continuing challenge rather than a discrete task. Cyber insecurity is likely to be a chronic condition that must be constantly managed rather than a single problem to be solved and put to rest. As a consequence, cyber norms must continually evolve, and mechanisms to promulgate new norms must be developed.

Norms and Law

One common reaction to coordination problems, particularly in the international sphere, is to negotiate a treaty and make binding or "hard" law on the topic. There are obvious advantages to this. Treaties have the force of law. Theoretically, there should be enforcement by governments of their provisions. Treaties also offer at least an illusion of clarity since they usually spell out details of the agreement and explain rules in great detail. But negotiating treaties can be a slow and cumbersome process, ill-suited to fast-changing issues like cyber security and Internet governance. Governments may also not be the best or only actors to be making rules in this area since so much of the technology is in private hands.

Norms offer another tool to coordinate action. Norms may be defined most simply as shared expectations of proper behavior.[2] Shared expectations among actors can be dynamic and change quickly to suit the needs of those relying on them. As expectations rather than legal obligations, they invite broad participation. Actors who may feel nervous about being bound by formal laws may be willing to engage with groups governed by norms. Over time, these initially reluctant states, firms and individuals may become socialized into deeper acceptance of the norms. Compliance becomes internalized as people get used to the expectations, see their utility and come to share them more fully than they did when they joined the group.

Characteristics of a Successful Norm

As we develop new norms for cyberspace, it will be important to pay attention to both the form and content of a proposed norm. The successful spread of new norms is greatly facilitated if the norm, itself, is *clear*, *useful* and *do-able*.

Clarity. Norms are easier to spread, and more likely to spread successfully, if they are organized around clear principles. Absolute prohibition norms often have a leg up on this dimension, but other norms can also be simply stated. "Do not litter" and "clean up after yourself" are norm formulations that are simple, straightforward, and easy to remember and understand. They also might have clear applications to cyberspace. Establishing norms of responsibility for maintaining secure networks would build on these general, well-established norms of social life. "Clean up your networks" would thus be a clear, simple and potentially useful cyber norm.

Few issue areas penetrate every aspect of society as thoroughly as the Internet. Coordinating such diverse stakeholders with such varied values will not happen quickly or easily.

One potential pitfall of these simple imperatives could be the lack of specific responsibility. Who is responsible for maintaining clean networks? States? Businesses? Individuals? The usual answer is everyone is responsible – just as no one is allowed to litter, no one is allowed to have insecure networks. But saying everyone is responsible may mean that no one actually takes responsibility, creating a classic collective action problem.

Again, the parallels with similar norms may help in cyberspace. In other realms, norms like these create overlapping and therefore redundant responsibility. There may also be overlapping and redundant pressures to comply. If one litters, one expects nasty looks and comments from others, so the norm has some social enforcement thanks to social pressures and expectations to conform. Dirty behavior is embarrassing and hurts reputations of both individuals and business. The social norm also has a legal backstop: One can be fined individually for littering. But ultimately government clean-up crews pick up trash when no one else does. Change in littering behavior thus started at the social level with social norms; enforcement is a backstop, not the driving force behind less litter. A similar configuration of norms and laws might be helpful in cyberspace.

A complex and technical problem like cyber security might not obviously lend itself to simple norms, but that is the challenge. Simplicity and clarity must be manufactured by the norm promoters. One way to do this is to distill a few core principles about cyber security, each of which is relatively simple. This has worked in other complex issues. Trade is probably one of the messiest and most complex bodies of international rules and law, but buried within it are still some rather simple, clear norms about "most favored nation" status and "national treatment." The laws of war have similarly become enormously detailed and elaborated. However, while only a few lawyers know all the rules, every soldier knows the basic norms of noncombatant immunity, and targeting norms about discrimination and proportionality. Cyber norms would certainly benefit if a few basic expectations could be clearly and simply articulated.

Utility. People are more likely to adopt norms if they can see clear connections between norm-following and desired outcomes. Adopting new norms is usually not costless for adopters. At a minimum, adoption by apex actors (governments, CEOs, heads of organizations) usually commits them to elaborate persuasion and enforcement efforts downstream in their country, business or organization. If government officials sign a treaty or endorse a multilateral effort committing the

United States to carbon reduction, child literacy or weapons build-downs, they still face domestic political battles internally to get a wide array of other national actors (governors, local officials, companies, Congress) to sign on. This would certainly be true of cyber norms, which would likely require broad cooperation inside states, societies and the private sector.

One powerful tool for persuading actors to incur these costs is a strong argument or narrative about how adopting the norm will produce desired results. Such an argument or narrative would have at least two components. First, it would need to convince people that cyber security is really important to their well-being in some meaningful and immediate way. Some audiences may be harder to convince than others. Cyber professionals will probably be easy to persuade on this score, although they may disagree about the right "fix" or best norms to address the problem. To the extent that broader groups whose concerns are less immediately or obviously linked to cyber security need to cooperate, this narrative will be crucial. People need to be motivated to incur costs to adopt these norms. They need to be convinced that the threats are real and the costs of non-adoption are high.

Second, this narrative would need to convince people that complying with the proposed norm would actually produce the desired result. Climate change efforts stalled on failures of this kind. There were direct and active challenges to the causal factual connections norm promoters were claiming. The counter-narrative by norm opponents disputed the link between human activity and climate change. If human activity is not causing climate change, why adopt carbon restrictions? In the case of cyber security, people would need to believe that complying with the new norms would actually reduce vulnerabilities. To the extent there is uncertainty about whether the norm with work or result in advertised benefits, selling the norm will be harder.

Cyber hygiene norms look particularly ripe for this kind of narrative. Under such norms, users would recognize the broad negative impact of their own failure to take simple steps to ensure cyber security by preventing their own computers from becoming hosts for malware. Implementing cyber hygiene norms will require broad cooperation by a great many diverse social actors. Part of the norm promotion process will have to be some kind of public education about the dangers of botnets and insecure networks more generally. Just telling people there are abstract threats to unnamed others if they do not clean up networks may not do the trick. A narrative that links this to real damage to themselves and others they know will be more effective.

Do-ablility. New norms are more likely to be respected and change behavior if people see clear and easy ways to comply. People are more likely to comply with a "do not litter" norm if trash and recycling receptacles are easy to find in public spaces. Countries are more likely to implement childhood vaccination programs if they have funding and public health professionals to carry it out. Making it easy for people to "do the right thing" is an important ingredient in any norm cultivation effort.

Of course, in many situations, "doing the right thing" may be quite difficult. If it were easy, the desired norm would probably have arisen naturally and one would not need a big norm cultivation effort. Difficulties in implementing a norm, even when it is clear and its utility is understood, can come from several sources. Often there are *political* problems in compliance. Responsible government officials who adopt a norm may not be able to persuade legislatures to enact needed laws. If the law is unpopular politically, government officials who adopt a norm may not get reelected. And, of course, getting parties to agree on a common norm in the first place may also face serious political challenges.

There may be *economic or financial* problems with compliance if it is expensive and money is scarce (which it usually is). Securing networks domestically will cost money. Questions of who will bear those costs – business, government or individuals – may be a bone of contention. Securing networks abroad may also involve serious economic costs. Many of the states that are big sources of cyber crime, like Moldova and Belarus, are relatively poor. Persuading them to adopt new cyber norms may not be enough; they may need financial assistance.

Compliance may also be complicated if the *technology or basic knowledge* required to comply is missing. Again, this may be a problem both domestically and abroad. However, technical assistance programs may also be an opportunity. These efforts do more than disseminate technical knowledge. They can also be powerful socializing tools and opportunities to spread "best practices" on the Internet. These socialization effects have been amply documented in other policy areas. The International Monetary Fund, World Bank and bilateral state aid all involve massive technical assistance designed to socialize people into new best practices in finance, development, human rights and the environment, as well as delivering technology. While never 100 percent effective, these efforts do have demonstrable effects and shift expectations in desired directions.

Those cultivating cyber norms will encounter difficulties of all three types. Politically, there are likely to be roadblocks. Any clear formulation of cyber norms is likely to prompt objections from somewhere. Implementing these norms is bound to cost money, which always opens avenues for objection and fights. National, state and local governments may not want to appropriate money for this purpose, particularly when change is expensive. Businesses are likely to raise similar objections. At all levels of government, there is likely to be some shortage of expertise, and the usual measure of technical and bureaucratic foul-up in implementing whatever norms are crafted. Although this list of obstacles may sound daunting, it is normal. Most norm promotion efforts face similar problems, and a great many of these efforts succeed.

Stages of Norm Cultivation

Creating successful new norms usually involves at least three sequenced tasks or stages: 1. norm articulation and promulgation; 2. norm dissemination; and 3. norm internalization, institutionalization and enforcement.

Norm promulgation. One of the most common, and commonly successful, strategies for promulgating new norms is to build on existing, widely accepted norms. "Grafting" or piggybacking on existing robust normative frameworks could help legitimate new norms for cyberspace. It makes them seem familiar and intuitive, thus increasing prospects for compliance. Promoters of a norm that states "access to the Internet is a basic human right," for example, might try to graft this new norm onto existing human rights norms. Promoters could argue that, in the contemporary world, Internet access is an essential component of and prerequisite for securing many of the core rights in the U.N.'s Universal Declaration of Human Rights and the U.N.'s International Covenant of Civil and Political Rights. Norms about conflict or war in cyberspace will be easier to promote if they build on and fit with existing norms about discrimination, proportionality and non-combatant immunity.

Many potential cyber norms might be complementary – they might deal with different types of cyberspace problems and thus might rarely conflict. For example, cyber norms about warfare are not likely to conflict with cyber hygiene norms. In some situations, though, we should expect stakeholders to propose opposed or conflicting norms that reflect their different values and goals. For example, Western states have generally promoted Internet freedom norms that require unfettered access to

online information and freedom of expression. Such norms conflict with many of the "information security" norms being proposed by authoritarian states like Russia and China. Information security, for authoritarian states, often means restricting both freedom of expression on the Internet, and access to information emanating from sources considered hostile, such as political dissident groups. To authoritarian states, Internet freedom, as the West understands it, is a threat and may constitute an act of ideological aggression against other states' core interests. Western states, by contrast, object to efforts to "secure" or restrict information in this way as a violation of basic rights.

Simply articulating new norms is not enough to change behavior. Norms need adherents, and actors will lobby hard for their preferred norms, looking for support. The process might be thought of as a "norm marketplace" in which U.S. cyber norms compete with Chinese and Russian ones, or military cyber norms compete with norms that focus on commercial and free speech.

Like products in a market, new cyber norms will compete, both with other norms and for time and attention of stakeholders whose support is required to change behavior. Changing expectations, attitudes and ultimately behavior takes work. Norms often fail, not because anyone particularly dislikes them, but for lack of enthusiasm. The size and power of the norm promoter will also influence its success. The United States clearly has advantages here. American power means people will pay attention to U.S. norm preferences and may allow the United States to induce or coerce others into following. Of course, the content of the norm, itself, may influence its success. Norms that make technical sense in addition to promoting popular values should have an advantage. Thus, which norms are adopted by which actors depends on a variety of factors – the content of the norms, the power or politics of their sponsors and the characteristics and needs of adopters.

One can imagine several possible outcomes to a competition and selection process. Clear winners might emerge; perhaps some variant of "national responsibility" for all cyber activity on one's soil would be widely accepted. Several winners might emerge. We could get "norm blocs" if large groups of countries or companies cluster, each focused on a different norm. Some of the related norms onto which cyber norms could be grafted have this "bloc" character. Different European Union (EU) and U.S. norms about privacy, for example, are two such competing norm frameworks. This creates some conflict, as indicated by debates post-9/11 over sharing airline passenger information, and the result may not be entirely stable. Norm cultivation processes also often get stuck at suboptimal equilibria. Think about the United States' continued adherence to non-metric systems of measurement. Perhaps there are no winners, which could leave us with no "shared expectations of appropriate behavior" at all. Thus, the norm cultivation process may never leave this promulgation stage.

One way to intervene in this process might be to devise forums in which to negotiate norm definitions. Again, this could unfold in more and less centralized ways. A centralized apex process to negotiate wide-ranging cyber norms would have the virtue of broad participation and, theoretically, the ability to harmonize norms across different cyber issues. It would probably also be extremely slow and have trouble keeping up with the dynamic cyber environment. Negotiations over the U.N.'s Law of the Sea Treaty might be an example of this kind of centralized norm promulgation process. It had broad participation and scope, but the process took years (or decades, depending on how you count) – something that makes no sense for cyber issues.[3] It would probably also be a largely intergovernmental endeavor, which may raise hackles in a policy domain with a tradition of minimal government interference.[4]

A more decentralized approach might involve different forums for different kinds of actors (e.g. states) or different forums to negotiate different kinds of cyber norms (e.g. commercial vs. military). Again, using existing institutions and structures might be useful in this regard. Already we can see groups of actors beginning to negotiate new cyber norms. For example, NATO has provided a forum for discussing these issues among its members. Getting cyber norms on the agendas of other regional and functional bodies might also be useful. These smaller bodies might move more quickly both because of smaller numbers but also because the members often share concerns and are more likely to reach some agreement. Of course, the risk is that decentralized promulgation might produce conflicting norms, which may cause trouble down the road.

The normative architecture of some existing forums may be especially attractive for promoting particular cyber norms. For example, Internet freedom advocates have put forth clever proposals to tie the free flow of, and access to, online information with international trade regimes (making Internet repression a non-tariff trade barrier), allowing democratic states to use the World Trade Organization's dispute arbitration mechanism to deter authoritarian governments from censoring online information.[5]

One thing to note: complete agreement or some flagship formal treaty may not be required for big multilateral negotiations to have an impact. Multilateral negotiations can influence norms even without unanimity. Simply publicizing preponderant agreement among important parties can create focal points around which other actors begin to organize. The negotiation process can also have benefits if it forces actors to improve clarity on at least some components of the norm where there is substantial, if not complete, agreement. The 1997 Ottawa Treaty, banning certain landmines, did not obtain signatures from key states (the United States, China and Russia) but clarified the norm, spelled out obligations, and disseminated it widely, shaping public opinion on the issue. Faced with a new, clear norm, U.S. procurement policies and behavior on this issue started to change, even if its signatory status has not. Similarly, the International Criminal Court has enjoyed cooperation from non-signatories like the United States, which found it a useful tool for handling atrocities in Sudan and Sierra Leone.[6] Big multilateral negotiations can also inspire productive track two efforts among non-governmental experts that can then facilitate broader agreement. An example of this kind of synergy may be the recent U.S.-Russian negotiations sponsored by the East-West Center that applied the Geneva and Hague conventions to cyber conflicts, prompted in part by Russia's efforts at cyber arms control at the U.N.[7] The norm negotiation process may thus have value in and of itself, regardless of the outcome.

Norm dissemination. Once promulgated, norm cultivators need to think about ways to spread the new cyber norms globally. The task at this stage would be to persuade (or coerce) more actors to adopt the norm. One can think of this task as having two dimensions – breadth and depth.

One goal of norm dissemination is usually to attract adherents and broaden the norm's reach. For cyberspace, this would seem to be particularly important. A constant worry is that networks are often only as robust as their weakest nodes. Getting all nodes in the network on board with new cyber norms would seem an obvious priority. If the norms apply to states, one would want to attract Nigeria, Ukraine, China and Russia – countries that may be skeptical of new cyber norms and may be sources of cyber problems – as well as the Organisation for Economic Co-operation and Development (OECD) countries. There may be a private sector analog to this. Big, well-heeled corporate actors with reputations to defend may be quicker to see benefits in adopting "good cyber citizen" norms (or may have more to lose from a crackdown and active enforcement). Smaller, fly-by-night enterprises may be harder to attract.

One persistent problem with norm dissemination is that the actors least in need of the norm are the first to adopt; actors who most need to adopt are often the recalcitrants. This is not surprising. Adopting a norm is easy if its requirements mostly line up with your preferences and current practices. Costs of adoption may be relatively low and desire to comply may be relatively high. The reverse would be true for actors whose current behavior most flagrantly violates the proposed norm. One advantage to the large group negotiation as a means of developing and promulgating a norm may be that the norm has wide adherence and dissemination at the time it is promulgated. (Indeed, it is being promulgated precisely because many actors have signed on.)

Another goal of cyber norm dissemination will almost certainly have to be expanding the depth of the norm's reach and its penetration into state and corporate actors. Getting national governments to adopt the norm may not be enough. State, provincial and municipal governments will also have a role to play if cyber norms are to be successful. So, too, will national companies, nongovernmental organizations and all other civil society actors. Similarly, getting corporate CEOs to agree with these norms may be easier than getting all the subsidiaries and suppliers to implement them.

Adherence from these smaller and more local actors may be less of a problem if national governments legislate norm compliance for all subsidiary governments in their jurisdiction. This happy outcome would require that national governments have both the power and the will to legislate. They may not. If they do legislate, however, the norm cultivation problem becomes a law enforcement problem, which lies more in the realm of implementation.

Norm institutionalization and implementation. Even after broad rhetorical and policy acceptance of new cyber norms at all levels, promoters of new norms will have to think about ways to ensure compliance. This is notoriously difficult and implementing major new norms is almost always an incomplete and continuous process. One should expect cyber norms to be no different.

One persistent problem with norm dissemination is that the actors least in need of the norm are the first to adopt; actors who most need to adopt are often the recalcitrants.

One source of potential lessons for cyber norm promotion might be efforts at "mainstreaming" new norms about gender, environment, corruption and other social goals at big international institutions. For gender concerns, the U.N. defines "gender mainstreaming" as: "Ensuring that gender perspectives and attention to the goal of gender equality are central to all activities…"[8] What we want in cyberspace is presumably something like cyber mainstreaming. We want awareness of cyber security issues and organizational rules mandating appropriate preventive measures (that presumably involve compliance with the new norms) to penetrate all levels of adhering organizations, be they states, corporations or civil society groups.

Big international organizations like the U.N. or U.S. government agencies often are given new jobs or are assigned new normative concerns. The common result of these dictates from the top tends to be superficial adherence. Organizations adopt the rhetoric or even the rules of compliance with the norm, but do not change the way they behave or actually implement the rules on the ground. Often this is not the result of active resistance or evil intent. Bureaucrats are busy. They have many other

things to do besides implement new directives, which may not come with clear guidance, additional funds or technical support, to say nothing of additional hours in the day. The result is not surprising: new norms often get lip service, sometimes extensive lip service, from organizations but little meaningful implementation.[9]

Strategies to avoid this problem, at least in part, might flow from an understanding of these problems facing bureaucrats. Funding and technical assistance will almost certainly have to be part of this effort for global cyber norms. This is true on both the breadth and depth dimensions, discussed earlier. Many of the countries the United States worries about as potential sources of cyber crime or cyber attack lack the laws but also lack the basic infrastructure – personnel, equipment and expertise – to ensure basic cyber hygiene. Figuring out the best way to help them help themselves (and the United States), both technically and financially, will be important. One obvious question is whether this assistance is best organized bilaterally, which would give the United States control over the funds it gives and the uses to which these are put, or multilaterally, which could spread out the costs and make assistance acceptable in more places.

Inside norm-adhering states, similar assistance may be needed. Apex actors, for example federal government bureaucracies centrally involved in cyberspace issues like the Department of Defense (DOD), may be able to implement new cyber norms on their own, but this is unlikely to be true at state and local levels, nor will it be true of the vast array of civil society and business actors using networks in the United States. Enforcement through well-formulated laws can help. Indeed, effective laws will be essential to a broad and deep norm implementation strategy. But even laws will be ignored if people do not know how to comply with them or do not have the funds to comply. Even when they have both knowledge and means, there will still be a non-trivial group of distracted, lazy or obstructionist citizens. Reducing the size of this group would improve norm success. Making it easier for people to "do the right thing" does not guarantee good outcomes. However, good outcomes seem almost impossible if compliance is difficult.

Relevant Features of Cyberspace

Every norm cultivation process is unique and the content of the norm being proposed matters to its success. So, too, do characteristics of the issue area that the norm is supposed to influence. Two issues are worth considering. Both flow from the ubiquitous nature of the Internet.

One distinctive feature of this policy arena is the diversity of stakeholders. Since the Internet touches almost everyone, almost everyone has an interest in, and views about, how cyberspace is governed, especially the military, businesses and civil society groups. Normative frames likely to be developed by these three sectors (which are not homogeneous) are very different and they are likely to champion very different kinds of cyber norms. The United States Cyber Command may think about cyber security norms as a "laws of war" issue. Economic actors are likely to think about cyber security norms as a crime issue. Civil society groups may be vocal about privacy and Internet freedom issues. These broad orientations will conflict at times and norm promoters will have to figure out how to handle this.

If norm development follows a decentralized path, these different actors may be able to promulgate their own norms inside different forums. But this, too, may create problems. Some of these stakeholders will find it easier to organize and promote their norms than others. DOD is out in front on this issue and is likely to develop, articulate and institutionalize its cyber norms internally long before civilians get organized.

This may matter because path dependence looms large in norm development; there are big "first mover" advantages. Once one set of norms is in

place, in this case military laws-of-war norms, they tend to color and in some ways perhaps constrain subsequent norm development by civilian actors. How, exactly, will DOD operationalize the details of discrimination, proportionality and non-combatant immunity in cyber conflicts? Will these be norms that the human rights community share or prefer? How might espionage be operationalized by the military in cyberspace? Would those be the norms preferred by business? Or by citizens' groups? These may not be a big problem, depending on one's goals and concerns, but it is worth some thought. The alternative – telling the military to hold off on cyber norm development until civilians get their acts together – seems politically unlikely and possibly dangerous given the rate at which civilians move on these things. External cyber attackers are not likely wait for our norm cultivation process to bear fruit.

The pervasiveness of the Internet and cyber issues, themselves, may shape the norm cultivation possibilities and prospects in other ways as well. Most norms govern domains that are more bounded. There is some discrete and usually limited population of stakeholders who care about the issue, whom the issue effects, and who are essential to change. These limits make the norm cultivation process more manageable. With cyberspace, by contrast, it may be hard to figure out who is not relevant to the process or essential to change.

This need for very broad involvement in solving cyber problems is challenging, but not unique. Other analysts have explored the policy effects of this pervasiveness of cyber concerns with a very good and helpful analogy to public health.[10] They point out that cyber attacks are like pandemics and can be averted by using similar methods. This is useful. It focuses our attention on crucial features of the problem – cyber's penetration deep into all aspects of society, the importance of prevention and good cyber hygiene, the deeply interconnected nature of the cyber world and dependence of each actor on good behavior by all others. This is a very happy analogy since no one is in favor of illness.[11] Yet a different analogy might give more caution.

Getting people to care about threats that seem abstract and distant to most of us (like climate change) is extraordinarily difficult.

Promoting cyber security and good cyber norms may also be like combating climate change. In important ways, cyberspace may be like carbon. Both are foundations for nearly all aspects of contemporary life. Modern militaries, business and social interactions depend on functioning networks and cheap carbon. You cannot fight a war, protect the nation from threats or run an economy without both. Yet both are associated with huge threats. Predictions about the potential damage from cyber attacks are catastrophic, as are predictions about the consequences of unabated carbon release.

Unfortunately, the fate of norms to prevent climate change is not encouraging. Formulating norms that command broad support by even a small numbers of apex actors (i.e., national governments) has been difficult. Achieving any kind of deep norm adoption or compliance inside societies is not faring much better. Getting people to care about threats that seem abstract and distant to most of us (like climate change) is extraordinarily difficult. Getting people to accept even modest short-term costs (higher gas prices, fuel efficient cars) to prevent long-term catastrophe is difficult. If those things are required for cyber norms, we should be worried.

Neither of these comparisons (cyberspace and health, cyberspace and climate change) are exact. It may be that the greater military concern with cyberspace will help put it on a different path from climate change. But the climate change analogy does suggest just how hard it may be to formulate and implement new norms that require cooperation of such a broad swathe of society.

Prospects for Norm Development: Two Examples

The foregoing analysis does not let us predict which norms will succeed or fail, but it does focus our attention on likely problems that norm promoters may encounter. Diverse stakeholders have proposed a variety of cyber norms. Each will face different challenges, as the following examples illustrate.

Civilian protection and minimization of collateral damage are widely accepted by all states as foundational norms of war. Following the grafting logic, outlined above, a number of analysts have explored ways to translate these norms into the cyber domain. The norms themselves are fairly clear – no harm to civilians, minimize collateral damage – and their rationale or utility would be the same as in kinetic, physical combat ("I don't kill your civilians, you don't kill mine.") Much of the debate here surrounds "do-ability" and technical obstacles to controlling effects of different cyber attacks (for example, cascading network failures). While attackers certainly have obligations to be concerned about these, the laws of war have always involved cooperation from potential victims to minimize damage as well. Hospitals and medical personnel must identify themselves if they want non-combatant immunity, for example. Promoters of cyber norms in this area might improve their prospects, then, with a multipronged approach: They could focus both on ensuring military targeting plans with an eye to ensuring civilian safety, but also on civilian planning to minimize entanglement with potential military targets. Protocols to share information about civilian systems and reduce opacity about them might also enhance compliance and, again, would very much conform to extant norms in physical space.[12]

Norms supporting Internet freedom will also present obstacles. At a basic level, efforts to secure the Internet are likely to involve some kind of regulations, limits and control. How national governments define "cyber security" and how they implement those understandings could thus place limits on online freedom of expression, and so create conflict over basic Internet norms. Opposing interpretations of cyber security by the United States and authoritarian governments such as Russia and China, mentioned earlier, are just one example. Disagreements will also surface between the American vision and that of our closest allies who exercise greater limits on free speech.[13] The United States, for example, did not sign the Additional Protocol to the European Convention on Cybercrime even though it ratified the convention. The Additional Protocol sought to harmonize domestic laws by making online racist and xenophobic acts a criminal offense, which the United States found to be contradictory to U.S. constitutional guarantees of free speech.[14] Such differences may make it difficult for norm promoters to achieve clarity about cyber security norms. Successful efforts to disseminate norms that comport with U.S. values must clearly distinguish efforts to secure basic infrastructure and networks from efforts to censor or control access to Internet content (to which the United States objects).

Attempts to align norms about Internet freedom with corporate business practices will be difficult as well, given the potential economic tradeoffs involved. Asking information technology companies to ignore foreign government requests for Internet user data could result in suspension or revocation of those companies' licenses, cutting off their access to those markets. "Do-ability" could thus be a big challenge for Internet freedom norms in an authoritarian state such as China,

which has eclipsed the United States as the world's largest Internet market with more Internet users than there are U.S. citizens. Some companies have already taken it upon themselves to articulate codes of conduct for responding to information requests and protecting their users, but these efforts need to be broadened and include more corporate stakeholders. Proactive steps from the private sector could also help give them some flexibility and leverage when negotiating with foreign governments. The fact that these companies are employing these practices on their own, for business reasons and not at the request of the U.S. government, could help insulate them from claims by authoritarian regimes that these companies are merely agents of U.S. statecraft. A private sector-led negotiation about business norms in cyberspace would therefore be a logical track to pursue.

ENDNOTES

1. Greg Rattray, Chris Evans, Jason Healey, "American Security in the Cyber Commons" in Abraham M. Denmark et al, eds., "Contested Commons: The Future of American Power in a Multipolar World, " Center for a New American Security (January 2010).

2. Definitions in social science often add a clause: Norms are collective expectations of proper behavior *for an actor with a given identity.* This amendment might be important if we want different cyber norms to apply to different types of actors. For example, the cyber norms one wants to cultivate for governments may differ from the norms one wants to cultivate for business or individuals. To the extent that what is normatively appropriate for one type of actor may not be appropriate for another, this extended definition could be useful.

3. The first U.N. Conference on the Law of the Sea (UNCLOS I) began in 1956. UNCLOS III produced a convention in 1982 that came into force in 1994.

4. Of course, creating a bigger role for government may be precisely the goal of some actors. For those suspicious of U.S. dominance in cyberspace, intergovernmental negotiations in a one-state, one-vote system like the U.N. might be very attractive. This kind of "forum-shopping" is common in norm promulgation processes.

5. "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information," Google, Inc. (15 November 2010): 8, http://googlepublicpolicy.blogspot.com/2010/11/promoting-free-trade-for-internet.html.

6. Vijay Padmanabhan, *From Kampala to Rome: The U.S. Approach to the 2010 International Criminal Court Review Conference*, Council on Foreign Relations Special Report No. 55 (April 2010).

7. Karl Frederick Rauscher and Andrey Korotkov, *Working Toward Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace,* East-West Institute (January 2011), http://www.ewi.info/working-towards-rules-governing-cyber-conflict.

8. U.N. Women, "Gender Mainstreaming," http://www.un.org/womenwatch/osagi/gendermainstreaming.htm.

9. For an excellent analysis of this kind of "organizational hypocrisy," see Catherine Weaver's study of the World Bank's efforts to implement reforms. Note that one of the ironic but often validated predictions of the theoretical work on organizational hypocrisy is that rhetoric about norm compliance may be inversely related to actually implementation. Talk becomes a substitute for action and a strategy (often a successful one) for obfuscating non-compliance. Catherine Weaver, *Hypocrisy Trap: The World Bank and the Poverty of Reform* (Princeton, N.J.: Princeton University Press, 2008); Nils Brunsson, *The Organization of Hypocrisy*: *Talk, Decisions, and Action in Organizations* (New York: Wiley, 1989).

10. Greg Rattray, Chris Evans, Jason Healey, "American Security in the Cyber Commons" in Abraham M. Denmark et al, eds., "Contested Commons: The Future of American Power in a Multipolar World, " Center for a New American Security (January 2010).

11. Biowarfare is, of course, a concern, but most pandemics to date have not been purposefully instigated by humans as a tool of either statecraft or terror, or as a criminal effort for financial gain.

12. Martin Libicki, "Pulling Punches in Cyberspace," in Committee on Deterring Cyberattacks, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: The National Academies Press, 2010): 123-147.

13. While the United States has some limits on free speech (speech involving child pornography, slander, perjury and "fighting words" is illegal online or off) its free speech laws are generally stronger than those of other major countries. Germany, for instance, prohibits Holocaust denial online and France does not allow the sale of Nazi paraphernalia online. The United States does not exercise these kinds of restrictions. For a more detailed discussion of this issue, see Richard Fontaine and Will Rogers, "Internet Freedom and It's Discontents: Navigating the Tensions with Cyber Security" in this volume.

14. See "Council of Europe Convention on Cyber Crime: Frequently Asked Questions and Answers," U.S. Department of Justice, http://www.justice.gov/criminal/cybercrime/COEFAQs.htm#QA8.