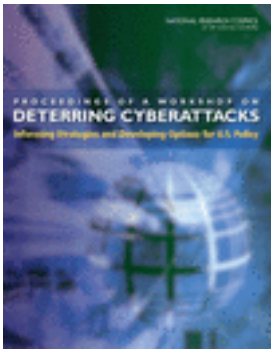

Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council

ISBN: 0-309-16086-3, 400 pages, 8 1/2 x 11, (2010)

Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm

Patrick M. Morgan
University of California, Irvine

Deterrence is a common practice in the history of international politics and in many other social relationships, and was largely taken for granted until after World War II. Early in the Cold War analysts and policy makers began to seize on it as the ultimate recourse for preventing another great war, which led to developing the first extensive theoretical analysis of deterrence in international politics plus construction of a number of national deterrence strategies, postures, and policies. The topic here is what the U.S. might make use of or learn from Cold War deterrence, including what is not relevant and why, in seeking cybersecurity. The format is to select important highlights of, mainly American, deterrence thinking and practice and then indicate how they are relevant or not for the problem of cyberattacks.

BASIC ELEMENTS OF DETERRENCE

In international politics "deterrence" refers to efforts to avoid being deliberately attacked by using threats to inflict unacceptable harm on the attacker in response.[1] The threatened harm can be inflicted by a stout *defense*, frustrating the attack or making it too costly to continue, or by turning its success into a pyrrhic victory. Or it can be inflicted through *retaliation*. (And through a combination of the two.) The emphasis in international politics is on providing that defense or retaliation *militarily* but nonmilitary actions can also be used.

Normally, the most gratifying is a defense that discourages attacks by looking too tough and too costly to overcome. This is preferable to deterrence by retaliation because the defender largely determines the results if deterrence fails and an attack occurs. A potent defense is also simpler to understand and apply. But defending can be expensive and painful so getting effective *deterrence* from a defense is very welcome—security is achieved at less cost and no loss. In contrast, deterrence by retaliatory threats can be cheaper than deterrence by defense but offers slim comfort if it fails. A tough defense often had to compensate for failures in seeking deterrence by threats of retaliation. The distinctive reliance on deterrence by retaliatory threats in the second half of the 20th century resulted, beginning in the 1930s, from new weapons systems that could make known and prospective defenses much too porous. In

[1]Typically any attack is unacceptable, but an actor will have specific kinds of attacks it wants to prevent, in terms of the target(s), means used, size, and damage inflicted.

turn, the use of deterrence by threats of retaliation could readily exploit weaknesses in defenses. With nuclear weapons it became possible to deter by threatening terrible retaliation without maintaining any serious military defenses, but having to face devastating levels of harm, if deterrence failed, from a similarly armed opponent.

Modern states have had to decide how to try to deter. While relying at least somewhat on defense, using threats of retaliation is sometimes chosen even if a suitable defense is conceivable, for various reasons:

- A suitable defense is not yet ready;
- A suitable defense may not be achievable;
- The defense will be painful and/or expensive—it is better to avoid defending if possible;
- A suitable defense will not work for long—it will give way under sustained attacks or will soon be outmoded;
- Relative military capabilities shift rapidly and a suitable defense will eventually be outmoded.

Deterrence is a psychological relationship; the goal is to shape an opponent's perceptions, expectations, and ultimately its decisions about launching an attack. Thus deterrence requires an "opponent" who is thinking, or might readily think of attacking. Ideally deterrence short-circuits that thinking, convincing the opponent to reject undertaking even a seriously considered and prepared attack,[2] making it a deliberately contrived relationship with an *opponent*. (The U.S. is not deterring Canada). The Strategic Command's bombers and missiles are not deterrence, just capabilities useful for deterring. Deterrence requires threatening an opponent who has an attack in mind.

In mounting deterrence the policy maker works with three spectra. One consists of actions which can probably inflict what the opponent will consider unacceptable damage. Next is the set of actual actions available within the national defensive and retaliatory capabilities and their expected impact. Finally, there is a set of "acceptable" retaliatory responses—acceptable to oneself, one's allies, "world opinion" or the international community, future enemies, or whoever is deemed relevant. Conducting deterrence requires finding things to threaten to do that fall where the three spectra overlap. The boundaries of this area can readily change, not only over time but also during a confrontation, even just after an attack.[3]

It is important to note that deterrence is not only used to prevent attacks and war via threats of harm. It is often used *via* attacks and war, that is, deterrence by doing harm. China's ultimate effort to deter UN forces from completely occupying North Korea in 1950 was to launch several attacks on those forces to indicate it was prepared to fight if they approached the border. Often disputes are conducted by the repeated use of force, a kind of *serial deterrence*, in which the parties periodically punish each other to contain each other's behavior—as in Israeli interactions with the Palestinians during several periods. Cold War analysts talked about deterrence not only for preventing an East-West war but for using it to prevent escalation of one if it ever started. Of course, there is also the use of force against one

[2]In the usual usage an attack is a military action, but deterrence is used to discourage other unwanted acts as well.

[3]General works on deterrence in the Cold War era include: Freedman, L. 1981. *The Evolution of Nuclear Strategy*. New York: St. Martin's Press; Jervis, R. 1979. Deterrence Theory Reconsidered. *World Politics* 39: 289-324; Jervis, R. 1989. *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca, NY: Cornell University Press; Morgan, P. M. 1983. *Deterrence: A Conceptual Analysis*. 2nd ed. Beverly Hills: SAGE; Powell, R. 1990. *Nuclear Deterrence Theory: The Search for Credibility*. Cambridge: Cambridge University Press; Wohlstetter, A. 1959. The Delicate Balance of Terror. *Foreign Affairs* 37: 211-234; Brodie, B. 1959. *Strategy in the Missile Age*. Princeton: Princeton University Press; Kahn, H. *On Thermonuclear War*. Princeton: Princeton University Press; Kahn, H. *On Escalation: Metaphors and Scenarios*. New York: Praeger; Schelling, T. C. 1960. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press; Schelling, T. C. 1960. *Arms and Influence*. New Haven: Yale University Press; Mearsheimer, J. J. 1983. *Conventional Deterrence*. Ithaca: Cornell University Press; Jervis, R., R. N. Lebow and J. G. Stein, eds. 1985. *Psychology and Deterrence* Baltimore: Johns Hopkins University Press; Lebow, R. N. and J. G. Stein. Rational Deterrence Theory: I Think, Therefore I Deter. *World Politics* 41: 208-224; Lebow, R. N. and J. G. Stein. 1994. *We All Lost the Cold War*. Princeton: Princeton University Press; Snyder, G. 1961. *Deterrence and Defense: Toward a Theory of National Security*. Princeton: Princeton University Press.

opponent in order to deter other opponents in the future, a standard justification offered by the U.S. for its wars during the Cold War.

Relevance for Cyberattacks

The current explosion of concern about cyberattacks in the U.S. and elsewhere is the culmination of fears building for some time.[4] Many thousands of attacks on American cybersystems occur daily, with the damage often estimated in billions, even trillions.[5] It is said that important sectors, particularly in national defense, will be targeted in the future, resulting in very extensive damage, including paralysis of critical activities, if attacks are carried out.[6]

For a deterrence analyst this is puzzling. The threat is seemingly dire yet thus far the U.S. has done little to deter cyberattacks. Elaborate defensive arrangements exist or are being mounted, yet everyone agrees we are very vulnerable—the defenses are porous, and when they work they typically impose no serious cost on the attacker so the attacks continue to rise. No national strategy exists for deterring cyberattacks by retaliation either, with little indication available as to what sorts of retaliation are planned or under development. It is as if, having to choose deterrence by defense, retaliation or a combination of the two, the U.S. chose "none of the above." If the harm being done is severe and the prospective harm incalculable, including serious damage to national security, why isn't this a national crisis, with things being done intensively to deter attacks? This suggests that the harm is only now becoming enough to attract serious attention, and that scenarios depicting more devastating attacks are gaining in plausibility. Perhaps we have been grossly neglecting the threat, but given the highly developed threat-perception elements in our political system it is more likely that the cyberattack problem is still modest.[7]

This is reinforced by weak U.S. retaliation to date. Literature on deterrence of cyberattacks describes the many problems involved in retaliation, and there is little information about steps the U.S. is taking to retaliate.[8] Again, this strongly suggests the attacks are not terribly costly or bothersome—at least not yet. While retaliation may be practiced covertly, that seems unlikely—significant retaliation should be hard to hide unless the U.S. is using the difficulty of detecting sources of attacks to hide its actions. And deterrence normally benefits from retaliation and its effects being publicized.

---

[4]For an impressive, detailed analysis see Clark, R. A and R. Knake, 2010, *Cyber War*: *the Next Threat to National Security and What to do About It,* New York: HarperCollins.

[5]For examples of estimates see Blair, Dennis. February 2009. Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence. Washington, DC, 38-40, available at http://intelligence.senate.gov/090212/blair.pdf. Levett, C. February 15, 2010. U.S. Seeking Allies for Warfare in Cyberspace. Available at http://www.smh.com.au/technology/us-seeking-allies-for-warfare-in cyberspace-20100214-nzg2.html; Clark, W. K. and P. L. Levin. 2009. Securing the Information Highway: How to Enhance the United States' Electronic Defenses. *Foreign Affairs* 88, 6: 2-10; Moore, T. 2010. Introducing the Economics of Cybersecurity, this volume.

[6]Possible threats are explored in Kramer, F. D., S. H. Starr, and L. K. Wentz, eds. 2009. *Cyberpower and National Security*. Washington, DC: National Defense University Press.

[7]Kugler, R. L. 2009. Deterrence of Cyber Attacks. In F. D. Kramer, S. H. Starr, and L. K. Wentz, eds. *Cyberpower and National Security*. Washington, DC: National Defense University Press 309-340. The U.S. has a National Strategy to Secure Cyberspace dating back to 2003 which is vague. A description of the "cyber hawks" view of the threats to national security as quite serious, and a suggestion that the threat is not very serious for now, are offered in Libicki, M. C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND 35-37.

[8]The Obama Administration has adopted, and recently released information about, a Comprehensive National Cybersecurity Initiative which includes steps toward a deterrence posture. See Nakashima, E. 2010. White House Declassifies Outline of Cybersecurity Program. *Washington Post* March 3. This was a follow on to the Bush Administration's Comprehensive National Cybersecurity Initiative. The administration also has created a new high level coordinator on cyber affairs, and there is now a U.S. Cyber Command under the U.S. Strategic Command, while the Department of Homeland Security coordinates nonmilitary departments on cybersecurity matters. Theohary, C. A, and J. Rollins. 2009. Cybersecurity: Current Legislation, Executive Branch initiatives, and Options for Congress. Congressional Research Service Report for Congress, September 30. The new Cyber Command commander was confirmed in May 2010. The administration has also proposed development of a "voluntary trusted identity" system to restrict internet access to people with a special authenticated identification, which some analysts claim is too little too late. Markoff, J. 2010. Taking the Mystery Out of Web Anonymity. *New York Times,* July 4.

In fact, the United States is not practicing much deterrence at all. In place of grave warnings of the harm attackers will suffer are assertions we are getting serious about this and instituting new bureaucratic arrangements for doing so. Few cases are cited of attackers suffering significant consequences. How serious can the problem be? Even if the threat is still relatively limited, it is disturbing that the attackers are numerous and the vulnerable targets are so plentiful. Much that is at risk has little to do with national security but is still important—computers damaged by viruses, hackers stealing identities and funds, damaging traffic control systems, disrupting operations at locks and dams. And so on. And sometimes national security is involved. So why the relatively limited reactions to date? The answer, in part, is that the problem is serious but not yet in terms of *national security*, which is where deterrence is most salient. And in most cases the attacks are not from enemies or opponents in the classic sense, making deterrence of the usual sort in international politics difficult to apply.

Another straightforward reaction from a deterrence analyst would therefore be that in cyberattacks the nature of the opponents is certainly very different. Usually this is said about the many nonstate actors who launch attacks, but that isn't the heart of the problem. In the Cold War the enemies were "out there," beyond the nation's boundaries. However, rising interactions and interdependence among states and societies have shrunk the relevance of out there. Cyberspace is transnational. Thus the enemy is "in here," participating like the rest of us in, as a component of, the interactive and interdependent networks that constitute cyberspace. Unless and until we want to completely reorder, reorganize, and redesign cyberspace, to participate in it is to be vulnerable to attack. Attack capabilities are variants of the basic resources required for operating, and operating in, cyberspace.

The motivations of the attackers are different too. Many attacks apparently reflect a desire to defy authority, or assert oneself and one's daring and thereby gain prestige among peers, or make life more exciting. None of these fit the usual model of a deterrable actor. Many other attacks are criminal, mounted by deliberately risk-taking individuals/groups behaving with a selected subculture's norms and rejecting more generally accepted ones, making them poor targets for deterrence of the usual sort. As for the espionage attacks, even in regular international politics spying by *states* is not considered a crime—punishment is reserved for the individuals involved (and often skipped even then)—and thus rarely evokes severe retaliation, just stiffer defenses or spying efforts in return.

This means deterrence efforts must, for now, involve steps, disconnected from specifically designated enemies, that cannot readily be "tailored" to a single target within an established national strategy, or a few variants of it, for a few high priority opponents who clearly threaten national security. At least not now. Without clearly defined enemies, ranked in priority and capabilities to do harm, the general dimensions of the threats to be faced cannot be known and their nature cannot be reasonably specified. During the Cold War the ultimate threats could be depicted in terms of things like when and how well known enemies, familiar conflicts with them, and their clear capabilities for doing harm could suddenly coalesce into brutal violence. With cyberattacks, the fundamental *nature of the threat* to national security remains largely hypothetical. This is strange territory for the designing and application of deterrence.

We want deterrence for containing serious enemies who would use cyberattacks to do significant damage. This includes states that could readily be or are already enemies, nonstate actors our enemies support and assist, and people willing to facilitate such harm on their own or on behalf of those states and nonstate actors. Lesser kinds of attacks, up to and even including cyber espionage, call for versions of deterrence of far less relevance in international politics. Without specified real enemies with capacities to do major harm via cyberattacks, including harm roughly equivalent to that from *military* attacks or inflicted via aiding and abetting military attacks, it is much harder to draw on Cold War deterrence thinking and experience.

As for the U.S. having to choose how to deter, for cyberattacks it will have to rely on both defense and retaliation. Defense will be especially necessary because of the flood of attacks the U.S. already experiences; some capacity to block or mitigate them is vital and hopefully it will eventually be good enough to discourage them. Retaliation and retaliatory threats will not work well enough—they are not appropriate for the great majority of attacks, and the necessary preconditions for using them are

unevenly present. Reversing the U.S. situation during the Cold War, for cyberattacks the deterrence supplied by defense must now compensate for the limits of deterrence based on retaliation.

Deterrence by defense, if much improved, will be very important as well for curbing the attribution problem which complicates deterrence by threat of retaliation. The more effective the U.S. defenses, the easier it will be to detail the nature of the severest, most threatening attacks. They will be the ones requiring the most resources, the most sophistication, the most elaborate planning, and the most penetrating advance intelligence work to pull off. That combination of capabilities will sharply limit the problem of figuring out "who done it" and provide a clearer focus for retaliation.

Finally, cyberattacks are very likely to turn out to be manageable primarily through applications of serial deterrence, repeated harmful responses over an extended period, to induce either temporary or eventually permanent suspensions of the most bothersome attacks or of attacks by the most obnoxious opponents. The attacks are already so common and come from so many sources that expecting to one day install a vigorous deterrence posture and virtually bring them to a halt is unrealistic. Successfully deterring one attacker will not discourage all the others.

DETERRENCE AND THE COLD WAR

The Cold War provided Americans with clear enemies, and the expectation that they were poised to strike at the U.S., its friends, allies and others important to American interests. In response the U.S. either had to defend those interests wherever they were attacked or, hopefully, avoid the attacks through deterrence. Interest in deterrence had begun to rise before World War II when vulnerability to being attacked, plus the harm that attacks might inflict, began to increase sharply for even the most powerful states. The more destructive a future war could be, even if one was victorious, the less attractive even "winning" became. When the 1930s international political situation, particularly great-power relations, made other ways of avoiding war unpromising, states' interest in deterrence climbed, but it did not prevent World War II nor do much to contain it. Not long after the war, nuclear weapons and the Cold War made *preventing* attacks vital, and interest in deterrence soon became intense.

The American armed forces' initial planning for another major war integrated nuclear weapons into standard strategic conceptions. Almost immediately some observers and analysts saw this as a mistake and grasped the central importance of deterrence and eventually led efforts to bring deterrence to the fore. But the initial American approach to deterrence in the 1950s, which envisioned winning a future major war by initial massive attacks and deterring by the threat of such attacks, was soon outmoded by events and the refining of deterrence theory. By the time new approaches were developed, it was difficult to add them to, or have them displace, what had already been set up.

The resulting nature, tone, and extent of Cold War deterrence strongly reflected the historical context from which it sprang, including the American experience of World War II and the behavior of its totalitarian opponents. The Cold War was seen as a conflict paralleling what World War II had been about, but with the nuclear age generating new conflict, and deterrence, capacities. The U.S. was again a status quo state facing a fierce aggressive challenge that must be deterred to prevent World War III. It took a while to appreciate:

- what was unique about the nuclear age in warfare, and strategy;
- what could and could not be done with nuclear deterrence;
- what could and could not be done with deterrence based on conventional forces; and
- whether and when nuclear weapons could be used.

It turned out that deterrence and related coercive efforts, with or without nuclear threats, worked unevenly. Nasty confrontations and serious crises occurred for years in the Cold War, alongside wars and other unhappy developments the U.S. had hoped to prevent. It also proved difficult to determine just when deterrence (nuclear and nonnuclear) worked and how well, or when it had failed and why.

Relevance for Cybersecurity

The U.S. has been slow to construct a substantial cyberdeterrence posture but that may turn out to be a good thing. It makes it possible to avoid going overboard on this. We are in the early stages of the cyber era and the cyberattack problem. On deterrence for cyberattacks we can presume that the context is in transition, with exciting improvements or nasty shocks to come in the technologies, international political situation, and our strategic thinking. We don't know enough about the future nature and sources of cyberthreats, all the things that could be done about them, plus the roles deterrence can play.

A similar situation existed early in the Cold War. Nevertheless, U.S. deterrence efforts rushed ahead with weapons, delivery vehicles, theory, strategy, policies—in a frenzied atmosphere. Deterrence seemed the crucial recourse for national security and the result was a quickly developed strategy, theory, and deterrence posture. It is not surprising that the posture soon fit badly with the theory and the strategy did not fit either of them. The deterrence capabilities and posture helped exacerbate the Cold War and make Soviet threats more fearsome,[9] while deterrence efforts tended to crowd out alternative approaches to dealing with the Cold War. Once the deterrence posture was firmly established it proved difficult to change—the basic elements were still in place when the Cold War ended and are still around today.

There is no frantic necessity today to risk making similar mistakes by claiming to know how deterrence will relate to cyberattacks and cybersecurity and making elaborate preparations accordingly. There is no intense political conflict among the major states to generate overwhelming fears of major cyberattacks, and virtually no U.S. conflicts with lesser states where a major cyberattack is likely. We do not see ourselves perched on the brink of a devastating attack. Thus there is no central security concern driving grand and military strategies, dictating priorities, shaping responses and forces, etc. when it comes to deterrence. While we worry about attacks on our friends, they seem mostly able to take care of themselves and, on the whole, act like being cyberattacked is not a grave concern.

There is an important political divide in the international system generating significant frictions but it differs greatly from the Cold War. The divide is between the developed, liberal, and democratic states and a number that are not like them. The former dominate the international system and are often seen by the others as expansionist and aggressive—they often depict themselves as having to deter "the West." Cyberspace, particularly the Internet, is a vehicle for Western "attacks" in their view, but less for inflicting crippling physical blows than as a purveyor of unacceptable ideas, norms, practices, and behavior. While we worry about and want to deter the misuse of cyberspace, an invaluable global resource, others worry that the basic nature of cyberspace as designed in the West is the real threat. This makes characterizing the relationship between deterrence and cybersecurity much more complicated than developing deterrence theory and strategy was in the Cold War.

It is, for instance, not clear what highly security-focused cyberattacks and a cyberwar would be about. They could be new ways of harassing or competing (such as in cyber-espionage) that substitute for warfare. They could improve the weapons in standard international conflicts and wars—a particular American concern since U.S. forces are exceedingly dependent on cyberspace for operations, and cyberattacks disrupting those operations could have impressive military effects. They could therefore someday constitute the essence of national strength and national standing in the world, making a cyberwar the ultimate expression of international conflict. Or they could be key instruments in struggles over the nature of cyberspace and who will dominate it. Each version would call for a different emphasis and policy orientation. Should we envision the emergence of MAD-like[10] cyberwar postures if international enmity deepens again? Extensive cyberwar–fighting capabilities for a new version of flexible response?

[9]Examples of this: megatonnage far beyond anything useful, highly vulnerable weapons, conventional forces on an unsustainable scale, many developments treated as affecting deterrence effectiveness far more than they turned out to do; repeated overestimates of opponent capabilities. (All of this eventually turned up in the Soviet Union too.)

[10]MAD—Mutual Assured Destruction—referred to the situation in which the U.S. and Soviet Union could readily completely destroy each other either by attacking or in retaliation for being attacked.

An extended conflict confined to cyberspace itself? Or would such plans be the latest examples of preparing to fight (or deter) the last war?

Will cyberwar be so technologically advanced that little physical harm and destruction results? Or put the survival of modern society at risk? Threats of the former would make retaliation less attractive than defense, necessitating a war-fighting, defense-dominant security posture. The latter would incite fears of defense inadequacy, putting the emphasis on deterrence by retaliation and making Cold War perspectives more relevant.

We cannot answer such questions, so we need to seize the opportunity to avoid the types of mistakes that characterized the early U.S. Cold War deterrence effort and the harmful long term consequences that resulted. Until we accumulate more evidence about the threats, problems, conflicts, and possibilities so our responses can rest on a sturdier foundation, we should treasure the chance to proceed cautiously in measured yet flexible "initial" responses.

The context is different from the Cold War in other ways as well. One example is how the U.S. is experiencing myriads of cyberattacks without wars or grave conflicts and few designated enemies. The world's most powerful nation suffers the most attacks! Many are crime-related, some resemble adolescent male joy-riding, others seem like probes or practicing—possibly by other states. Some are espionage. Obviously *deterrence cannot be asked to prevent all this*. But, as happened during the Cold War, it will continue to be difficult to determine when deterrence has failed, has worked, or is working, and why. Like in struggling to ward off disease, we will have so-so confidence in what we are doing, uncertainty about knowing when we are successful or not, and why. Like dealing with crime, the attacks will vary greatly and remain ubiquitous despite efforts to deter them; it will be difficult to know how deterrence is doing, whether and when it is successful. As with the drop in major crime in the past two decades, we will not be certain why a "success" has occurred or whether deterrence had much to do with it.[11]

An additional and important facet of cyberattacks is that the weapons are integral to the version of cyberspace in which we are immersed. The effects of attacks at one point can spread unpredictably, far beyond the target and even back to the attacker, given *the highly interdependent nature of cyberspace*. A cyberattack launched in retaliation might damage cyberspace in ways that harm the defender, not unlike earlier fears about the uncertain consequences of using ABC (atomic, biological, and chemical) weapons. But in contrast to those weapons, the point of developing cyberspace has been to promote rising interactions and interdependence through information availability and exchange. Its essence is what leads to vulnerability to attacks; to participate in it effectively is to also acquire capacities to damage cyberspace and harm others, deliberately or—just by leaving a computer inadequately protected—inadvertently.

This is responsible for still another difference from the Cold War. At that time national security concerns led to efforts to contain the spread of harmful weapons. Nothing like this applies to cybersecurity because, as noted, the relevant capabilities are integral to cybersystems.

BASIC CAPABILITIES NECESSARY FOR DETERRING

According to deterrence theory, in the abstract (and sometimes in reality) all that is necessary to deter is that the opponent *believe* you can and will harm him unacceptably if he attacks, whether or not this is true. Deterrence takes effect in the mind of the opponent—he ultimately determines whether he is deterred. What matters is his concluding that the harm will be "unacceptable." In theory, that is why he does not attack. Deterrence is therefore best pursued by having capabilities to impose such harm. Early in the Cold War analysts worked out what those capabilities should look like:

- Means (defensive and/or retaliatory) capable of inflicting unacceptable harm—typically military—on an attacker and able to sufficiently reach him (effective delivery systems);

[11] In terms of our major explanations for crime, the recession should have stimulated a resurgence in it but it hasn't.

- Effective capabilities for ordering and directing the necessary harmful steps—durable C2 (command and control); and
- The means and C2 being sufficiently survivable and effective to do that unacceptable harm after the opponent has launched his best attack and then puts up his best defense.

During the Cold War vast attention was paid to these things in designing and conducting deterrence.

Relevance for Cyberattacks

Applying this perspective, the first thing to note is the absence of substantial evidence about actors' attack capabilities in cyberspace. We are too early in the cyber age to know with any precision how much damage states or other actors can do or how much in the future they might reasonably be expected to do by cyberattacks, on their own or linked to other, probably military, attacks. We don't know how good attackers' abilities to ward off retaliation are either. For practicing deterrence we lack relevant information about how much damage an attacker would consider unacceptable, i.e. how much would be enough.

As noted above, rushing ahead almost blindly early in the Cold War was a mistake. While important conceptual and analytical progress was made when little was known about what nuclear war would be like, what military capabilities the opponent(s) possessed—how destructive, how reliable under stress, how survivable, how accurate—and how best to manage confrontations, much American thinking about these things did not survive serious encounters with reality. For instance, debates raged about whether a new age had emerged, outmoding much of the past, or much that seemed new was actually not and various lessons and thinking from the past still applied. Analysts and policy makers often got this wrong; determining what was really new was difficult.[12]

There is considerable secrecy now about American cyberattack capabilities and their survivability for purposes of retaliation. The U.S. is widely believed to have the best capabilities in the world, but little is available about how robust they would be after a major attack. There is more uneasiness than hard evidence about how damaging attacks by opponents or prospective opponents could be. Like early in the Cold War, discussion about how a conflict would go and what it will take to deter it is largely hypothetical.

It seems more important today, than it did early in the Cold War, to focus on the vulnerability of command and control of cyberattack defense and retaliatory capabilities. One Cold War concern was about how crippling attacks on national command centers and communications could affect negative control over unauthorized actions, particularly with nuclear weapons. Another was how antagonists' fears of attack could lead to nearly automatic retaliation upon receiving any serious warning signal of a possible attack. There seems to be little discussion about negative control over cyberwar and cyberattacks—concern about escalation seems mainly focused on how damage from initial attacks could generate a deliberately escalating conflict spiral rather than on a loss of control over national cyber capabilities that has them wreaking havoc on their own. This despite how negative control is now flimsy or nonexistent over so-called "patriotic" hackers in various countries.

Even more important is how C2 for many noncyber military capabilities is so heavily reliant on cyberspace. A failure of deterrence could be triggered by the temptation to seek a crippling first-strike capability not against defenses or retaliatory capabilities but the command and communication links for operating them. What kinds of responses to this problem might be employed?

During the Cold War, U.S. efforts to offset the effects of being attacked started with elaborately redundant attack capabilities, and eventually included redundant C2 arrangements as well: multiple

[12]Jervis, R. 1984. *The Illogic of American Nuclear Strategy*. Ithaca: Cornell University Press. Soviet thinking also remained deeply rooted in World War II, displaying an important conceptual lag. A recent illustration of this phenomenon is how the Gulf War came as a great shock to Chinese security perceptions.

and varied communications channels, information storage capabilities, repair resources, sites for storage of replacement equipment, command centers, and a strategic nuclear triad for retaliation. Much less effort now seems to be going into redundant cyberspace capabilities, particularly in the private sector. Since the public and private sectors are intertwined, the latter's deficiencies may be very harmful but cannot readily be corrected unless the government is willing to pay. Forcing the private sector to bear the costs seems unlikely since failure to comply cannot readily be detected. Meanwhile, redundancy in the public sector is always a convenient target, apt to be eventually regarded by some as waste and marked for elimination.

An alternative is simple and durable, or easily and cheaply repaired, components. This is a common preparation for military attacks in various countries. The emphasis is on systems with the ability to take hits and keep on going. The U.S., on the other hand, has normally gone for complex, hard to repair, advanced systems—much more potent but not necessarily very durable. Today, with respect to cyberspace the U.S. has the novel additional concern, steadily rising, about extreme dependence on foreign supplies of, and necessary backups for, many critical components of cyberspace and military systems.

Another alternative, seriously considered during the Cold War, was bolstering deterrence threats by arranging that decisions on responding to attacks, particularly with nuclear weapons, were decentralized in advance to regional and local military commanders—the response to an attack would be virtually instantaneous. However, this kind of arrangement soon looked too difficult to keep safe (worry about negative control) and too likely to generate escalation. Instead, control over American conventional forces and particularly American nuclear weapons was eventually extremely centralized. It is hard to know where we are on this with cyberattacks. On defenses, the initial responses have to be virtually automatic, with little central control. While immediate steps to counterattack are possible there seems to be uneasiness about making this automatic and also about officials ordering it through channels, particularly since the attacks might well have been routed through many locations and computers surreptitiously and thus the counterattacks would harm innocent parties. But punitive responses could be far more common, and essentially uncontrolled, from the private sector, and would be uncoordinated and possibly counterproductive, particularly for limiting escalation. The uneven cooperation now between the government and the private sector will make dealing with this problem serious and sensitive.

Decisions to more thoroughly retaliate can be centrally made but it is unclear how much central control there would be of the implementation. The crucial question is whether American cyberattack capabilities can inflict unacceptable harm. It is unclear how good others' defenses are and also how durable American resources will be under a sustained onslaught. One U.S. advantage is being the world's foremost bull's eye for cyberattacks: it has more experience spotting and coping with attacks than anyone, has been able to test more defenses, and presumably has more people used to dealing with attacks. However, the experience is apparently almost exclusively with *defenses*, and cyberspace defenses inflict little harm on attackers—at best they produce frustration and the costs of unsuccessful effort, not the extensive damage defenses often inflict in military combat. There is plenty of evidence about what cyberattacks can and cannot do against the cybersystems Americans are familiar with, but little about how effective American preemptive or retaliatory attacks might be. Lack of a potent American image and record of imposing unacceptable harm on attackers, by either defense or retaliation, makes effective deterrence next to impossible.

There are several possible reasons for this situation. The U.S., at least for now, may be unwilling to retaliate in noncyber ways. Perhaps it has potent defensive or retaliatory cyber capabilities in reserve but is unwilling to use them for fear of degrading their future effectiveness—to use them might be to lose them. Thus the U.S. prefers to rely on its (very uneven) reputation rather than to show what it can do. Another possibility is that using them would be too informative to others about profitable lines of research and development, or heighten foreign efforts to reproduce what the U.S. has.[13]

[13]The same applies to using noncyber responses to attacks—there could be reluctance because that might help opponents strengthen their defenses or better imitate U.S. capabilities.

If these are actually important considerations in the government, it is better for now to stress deterrence by *defense*, because those restraints on attacking others add significantly to its appeal. But defense is clearly far more expensive for the U.S. than attacking it is. This can be a serious problem and is often cited as a major deficiency of BMD—it costs more to build than ways around it do. There must be significant costs for an attacker in being thwarted by defenses—without compensating benefits—to get an effective rather than just annoying deterrence effect, and this is rarely the case for U.S. defenses now.

ADDITIONAL COMPONENTS OF EFFECTIVE DETERRENCE

In addition to the *image* of being able to seriously harm an attacker, it is important to effectively convey the *threat* to do so. Deterrence theorists quickly noted the difference between the two. Threats are not necessarily inherent in a military posture. A threat must reach the opponent and be understood, and may not work if it is garbled, is in the wrong "language," is aimed at the wrong party, or conveys an incorrect message by being, say, ambiguous, misleading, insincere, or too indeterminate.

While harmful capabilities sometimes convey a potent intrinsic threat and achieve a deterrence effect from this alone, this is rarely reliable enough. It is important that the deterrer specifically project the threat it feels is needed. But this can be hampered by vague diplomatic and other communications: alliances have escape clauses, threats are phrased so as to leave some avenues for retreat, they are interwoven with inducements and concessions, etc. There are various concerns as a result. The opponent may ignore or underestimate the threat; preoccupied with his own plans, he may neglect to carefully ascertain the other side's intent. Or he may be determined to attack no matter what. Or he may misinterpret the threat, seeing it as a sign he is about to be attacked (and must hurry to attack first) or dismissing it as empty posturing. Or he can treat threats as attempts to bully or humiliate, strengthening his desire to attack (leading to suggestions as to when and how threats are better conveyed privately). With such possibilities in mind, deterrence analysts stress the importance of offering not just threats of harm but reassurances that compliance will cancel that harm, but without indicating how to convincingly do this. Studies show that combining threats with incentives increases chances of success, but the opponent may instead treat the incentives as evidence the deterrer's commitment is weak.

Relevance for Cyberdeterrence

From a deterrence perspective it is therefore important to detect an emerging threat of attack well in advance, gaining time to assess it, design and implement appropriate deterrence threats, see how they are working, and make adjustments if needed, etc. Cold War era deterrence analysts often worked with an image of deterrence even in a crisis as conducted in the following fashion: rising conflict intensity and military preparations that threaten a possible attack lead to deterrence steps, which stimulate serious efforts by each side to ascertain the other's goals, intentions, plans, and determination—a learning process.

However, cyberattack preparations are likely to offer much less (maybe no) palpable evidence of an impending attack, and thus provide little inducement to mount a specifically targeted deterrence. And the necessary preparations to either defend vigorously or retaliate will also be much less visible. Evidence may have to come primarily from shifts in the intensity of the political conflict along with detectable increases in probing by each actor. Thus far, however, cyberattacks do not amount to such costly and deadly steps that they are *necessarily* preceded by a marked deterioration in relations. They are planned and prepared with virtually no signs, unlike most military attacks. Strategic nuclear attacks during the Cold War could eventually be launched on a few moments notice but there were some signs of going to a high level alert a deterrer might detect. Probes or shifts in behavior prior to military attacks were normally more costly to undertake and thus less likely to be exercises or a bluff. In contrast, there is a steady rain of cyberattacks today so even an opponent's probing may not necessarily or decisively stand out. Intelligence analysts fear that extensive but irrelevant information will drown out vital information; in the world of cyberattacks, such static is huge.

Thus deterrence of cyberattacks must rest on the necessary threat being *prominently displayed* virtually all the time. Not that it must always be carried out, but that readily detectable expressions of it are at least regularly displayed and periodically implemented. Much is made in the deterrence literature about harm from threats not being carried out, but this is because threats involving major military steps are reserved for a very serious crisis which rivets the attention of policy makers and onlookers. Under these circumstances backing down (in effect) from the threat can readily damage one's credibility. This is less true of general (noncrisis) deterrence, where threats are broader; not carrying them out might damage one's credibility but typically they offer more loopholes for the deterrer and are harder to interpret as backing down.

Cyberattacks on the U.S. occur constantly, and are not (yet) linked to deep political conflicts with other states, so they do not pose a crisis and a failure to fully defend or retaliate need not demean U.S. deterrence. The problem is to strongly establish the *principle* of a strong U.S. interest in deterring and in making preparations to punish attackers when, in fact, only a few attacks will evoke a truly harmful response. Deterrence has to be achieved not by making a response highly likely but via the *possibility* of one. This is hardly unique; international political threats often operate in this fashion, as statements not of certainties but about the risks of suitably harmful possibilities.[14] In deterrence such threats can be effective not in preventing all attacks but in reducing the highly provocative ones.

This is getting some virtue out of a necessity; ideally, a harmful response would be very common. Studies indicate that deterrence works best, with criminals for example, when coupled with a high probability of some harm being inflicted for attacks even if only on a low level, something which is not evident and not possible now for cyberattacks. Intermittent implementation of deterrence threats invites potential attackers to misinterpret them or misestimate the risks they would be taking.

THE SPECIAL CONCERN ABOUT CREDIBILITY—THE CREDIBILITY PROBLEM

Of the possible reasons deterrence might fail, what received most American attention during the Cold War was the credibility problem, primarily because it is inherent in the nuclear age for nuclear-armed states, plus the impact of the Munich analogy (from the late 1930s) and the steps leading up to the Korean War.[15]

Concern started with the fact that since deterrence seeks to persuade an opponent who has a significant incentive to attack, the deterrence threat must be believed (the opponent expects it to be carried out) and must be persuasive (the opponent sees the consequences as too harmful). In addition to factors mentioned earlier, analysts focused on "will." A deterrer's capabilities mean little if the deterrer can't convey a strong will to use them. If it is hard to do that, deterrence is in trouble. However, if rational decision making is assumed the deterrer, like the attacker, does a cost-benefit calculation and will not retaliate or defend if it feels it would suffer unacceptable harm as a result, and under *mutual*, particularly nuclear, deterrence how could retaliation be rational when the defender would risk suffering great additional harm from a severe counterretaliation?[16] By extension, this particularly applied to a low level attack when escalation might turn it into a nuclear war: why would the deterrer rationally choose to risk that by retaliating? In particular, why would it take such costs and risks on behalf of an ally or some other third party?[17]

---

[14]North Korea, for example, is constantly threatening to treat various actions by others as creating a "state of war" to which it will appropriately respond, when the likelihood of such a response is quite low.

[15]The Munich settlement was seen as having destroyed British and French credibility for Hitler, leading him to continue his expansion policies right on into starting World War II. The Korean War was held to be due to the U.S. having done almost nothing to generate a credible commitment to South Korea's survival. See Khong, Y. F. 1992. *Analogies at War*. Princeton: Princeton University Press; and Stueck, W. 1995. *The Korean War: An International History*. Princeton: Princeton University Press.

[16]This also applies to stoutly defending. Fear that defending will make the attacker do a great deal more damage in order to win can undermine the will to fight, as Czechoslovakia demonstrated twice in the 20th century, in the 1938 attack and in 1968.

[17]The worry was not only that an opponent would figure this out and decide to attack, but also that U.S. allies would see this and lose confidence in U.S. promises to fight for them.

The problem disappears if the deterrent threat will be carried out automatically if an attack occurs and the opponent knows this—that cancels the defender's opportunity to rationally decide not to retaliate. But there were obvious problems with this suggestion so it was never implemented. A highly sensitive warning system might falsely trigger the automatic retaliation, or it could set off retaliation after a relatively small attack that was not worth it—turning an "incident" into a war. Or it might erroneously detect an attack, mechanically or due to human error. And so on.

Alternatives ranged from making the response to an attack "semi-automatic," to upholding almost any minor commitment so as to build a reputation for doing so (the most influential solution in the US), to trying to convey a degree of irrationality in confrontations. The ultimate recourse was to count on the fact that since no government could guarantee to be highly rational after being attacked and might resort to a vicious response, resulting in disaster for the attacker, there was an existential deterrence associated with nuclear weapons and other powerful forces that provided considerable credibility.[18]

None of these were fully satisfactory. There was no definitive answer to the credibility problem, and deterrence had to be pursued without one. More broadly, the credibility problem arises because of the need to make a *very difficult decision* and a decision maker might not make it effectively for any number of reasons, rational or irrational.[19]

It is important to emphasize that in the Cold War much of the emphasis was on crude threats that had little to do with things like precise attribution and carefully tailoring the response to the specific nature of the attack. Massive retaliation was the ultimate posture here, initiated by the U.S. and eventually imitated by all other nuclear powers as at least part of their deterrence postures. When the U.S. sought to limit military responses to an attack to the lowest level needed to defeat it, European members insisted on a NATO posture prepared to initially fight hard and then readily escalate to the nuclear level, steadily and perhaps massively—increasing the indiscriminate destruction. They felt that the threat of indiscriminate destruction was the most effective deterrent.

Ultimately the U.S. and Soviet Union developed huge nuclear weapon stockpiles capable of many kinds of attacks, not just huge and indiscriminate ones—many of their weapons were, in fact, aimed at each other. But even very limited, and/or very precise attacks to limit damage could have set off escalation to larger and more destructive nuclear warfare; many analysts and observers, and also policy makers, believed this was very likely. And even small or precise nuclear attacks could readily have inflicted substantial collateral damage. Nuclear deterrence continued to seem very crude and imprecise in the harm being threatened.

Actually, deterrence operated during the Cold War despite real doubts about its credibility under many circumstances. Not only was it difficult to make a nuclear threat credible vis-à-vis another nuclear power, but it also became very difficult to make one credible vis-à-vis a nonnuclear state because of the so-called "nuclear taboo";[20] nuclear threats sometime had little effect on opponents' behavior. Conversely, a *nonnuclear* retaliatory threat could be hard to make credible against even a weak nuclear power for fear of escalation. Deterrence by nonnuclear threats against nonnuclear weapons states had always been complicated and problematic, not reliably successful, and this was true of nuclear deterrence in the Cold War era. After World War II U.S. officials expecting to have leverage on the Soviets and others from the U.S. nuclear weapons monopoly were regularly dismayed by the results. Later there

[18]This was typically phrased in terms of a defender irrationally provoking a *nuclear* war but it could readily apply to other cases. For instance, the Chinese decision to intervene in the Korean War confronted the U.S. with the risk of a much wider war, nuclear or conventional, if it retaliated directly in China.

[19]Nonrational reasons could include being frozen in panic or fear; no consensus on fighting; no certainty a decision to fight would be carried out; being tossed out of office before making or communicating a decision to fight; relevant orders lost or not believed by underlings, garbled in transmission, or misinterpreted. Examples of rational reasons for a decision to fight not being made: seeing that a counterretaliation will add too much to the damage already done; the planned response looks excessive or escalatory; the attack looks like a probe—retaliating could give the opponent valuable information about the deterrer's capabilities and plans.

[20]This is a great reluctance to abandon the history of nuclear nonuse since 1945 lest that encourage future uses of nuclear weapons and arouse international condemnation for breeching such an important threshold.

were instances of nuclear powers being attacked by nonnuclear states, even losing the wars or suffering other outcomes short of victory.

Cold War era deterrence had an uncertain (hard to ascertain) impact even on preventing wars among the great powers. While most analysts believe it was an important factor in preventing World War III, many now hold that often the Cold War opponents were not particularly interested in attacking each other, making for times when deterrence was not particularly responsible for upholding peace and security. Part of the deterrence contribution was the *possibility* of a very harmful outcome; it was the risk of *possible disaster* that (unevenly) deterred. U.S. deterrence benefitted from the American ability to mount a nasty conventional response, not just a nuclear one, but even at that level deterrence was a crude recourse with an uneven record—the Vietnam War, for example, being a long history of deterrence failures (on both sides).

Relevance of the Credibility Problem for Deterrence of Cyberattacks

This leaves no intrinsic reason empirically for concluding that deterrence should now work well against cyberattacks. The available evidence on the credibility problem suggests, in part, that it cannot work well. The credibility problem:

1. increases as the scale of harm to be inflicted from an attack or anticipated attack declines—at low levels of conflict threats to do very serious harm are often not credible;
2. increases with the possibility of a catastrophic counterretaliation;
3. increases to the degree the deterrer's primary or vital interests are not threatened;
4. usually increases for deterrence by collective actors (like the UN Security Council);
5. increases when the attacker is difficult to detect, identify, single out;
6. is somewhat independent of the deterrer's past behavior; credibility is not guaranteed by having upheld past commitments;
7. increases when the deterrer's upholding of commitments is irregular and infrequent;
8. increases in extended deterrence; and
9. increases when deterrers are seen by opponents as cautious, risk-averse.

The first of these applies directly to cyberattacks. Thus far the harm they inflict is below the threshold for triggering very harmful U.S. reactions—U.S. deterrence credibility here is quite low. The third point also applies—the U.S. is only now getting close to behaving as if cyberattacks threaten *vital* American interests.

The fifth point on attackers being difficult to detect is the most cited in analyses of deterrence of cyberattacks. They come from myriads of sources, often virtually anonymously. They can come from people associating themselves with a government which has not authorized and does not approve of their actions. And so on. With no way to link retaliation to the actual attacker, the credibility of threats to do so is diminished.[21] This is a serious complication. It appears in various forms in deterrence thinking. A standard concern in alliances is the danger an ally will connive to induce a conflict that drags its allies in—inciting the "attack" they respond to. A concern early in the nuclear age was that with nuclear proliferation a third party could provoke a war between the superpowers via an attack that looked like it came from one of them, or by reacting to an attack in ways that generated rapid escalation to its allies. (The basic rationale for British and French nuclear weapons was the implied threat that they could escalate to the nuclear level after a conventional Soviet attack and draw the superpowers into direct nuclear exchanges.) One of President Kennedy's concerns during the Cuban Missile Crisis was that NATO forces put on high alert in Europe would automatically break out their nuclear weapons, possibly alarming the Warsaw Pact states. Another was that in operating the

[21]For various views on the attribution problem see Libicki, M. 2009 *Cyberdeterrence and Cyberwar*. Santa Monica: RAND.

blockade during the crisis the Navy worked to force a Soviet sub to surface—an action not ordered by the president but how was Moscow to know that? In short, Cold War deterrence was not about only acting when responsibility for an attack was obvious.

This is equally true in conventional and subconventional military clashes where nuclear escalation is not a consideration. The Tonkin Gulf incident involved retaliation ordered when the exact nature of the incident was unclear. Various countries in the Cold War downed civilian airliners, yet the question of attribution remained open as to who specifically was responsible. A standard justification for inserting peacekeeping forces in conflict situations then and now is that incidents readily occur even when whether an attack really occurred, who did it, and who ordered it are in doubt.

On the other points, it is hard to say much about the credibility of threats that promise very great harm in response to cyberattacks: we have no examples yet. We can speculate that familiar things will result—the threats will be difficult to make credible and thus will often not be issued or not be effective. But they will be possible to implement and thus will have at least some credibility, particularly after the U.S. suffers serious attacks and is intensely irate.

There is no example to date of a collective actor attempting to deter cyberattacks. Collective actor deterrence has a difficult credibility problem for numerous reasons.[22] However, such a threat can more readily represent—if well organized and mounted—a daunting level of opposition to the attacker, a factor that gives threats credibility. Perhaps in the future primarily collective actors will be used to defend, or particularly to order retaliation, to make deterrence more credible and spread responsibility for carrying out the threats.

Does the credibility problem pose insuperable difficulties? No, deterrence can have some impact if there is a reasonable possibility that the U.S. will periodically do unacceptable damage, and occasional demonstrations of this occur. Such an effort should, of course, especially be made when the U.S. has major interests threatened or harmed. Failing to respond when the stakes are low does not undermine the credibility of all one's commitments; opponents normally take the threat more seriously when the stakes are high. If they attack anyway, failing to respond in that situation is a mistake.

This is likely to be particularly true for cyberattacks. With so many attacks occurring, the best deterrence posture will be to respond strongly when something important is threatened or harmed and mount occasional responses to lesser attacks. This would maximize credibility over a wide range of attacks, not precluding them but somewhat containing their incidence.

Next, there is no inherent reason the threatened response has to be "in kind" to be credible. Nothing in deterrence theory or past experience requires this. Many deterrence threats and their implementation ignore it. Examples include the use of sanctions to prevent or end a state's misuse of force, or the use of threats and force to curb gross domestic violations in human rights. In some cases it may even be unacceptable or unwise to respond in kind.[23] Thus analysts who suggest that deterrence of cyberattacks may well draw on a wide variety of painful responses—economic, military, political/diplomatic, cyber—are correct.[24]

Responses in kind are attractive for reasons that go beyond deterrence, such as conforming to a sense of what is the "right" thing to do, or to better highlight the attacker's offense and indicate a willingness to avoid damaging other relationships between the parties. Reasons for in kind reactions a deterrence perspective can endorse include, first, to have the response—by its limited nature—indicate types of restraint the opponent should adhere to in order to limit escalation, and second, to avoid breeching thresholds of damage that might invite future enemies to do the same.

As for the problem of attribution, in deterrence theory and past practice it has not been considered

[22]Morgan, P. M. 2003. *Deterrence Now.* Cambridge: Cambridge University Press 172-202.

[23]Thus expecting that a nuclear attack *must* bring a nuclear response, something U.S. allies sometimes promote, is not correct. The U.S. may want to respond in a devastating nonnuclear fashion. In the Gulf War the U.S. decided before the war to respond with conventional means even to an Iraqi use of weapons of mass destruction.

[24]For example, Kugler, R. 2009. Deterrence of Cyber Attacks. In Krasner, F. D., S. H. Starr, and L. K. Wentz, eds., *Cyberpower and National Security*. Washington, DC: National Defense University Press 309-340.

necessary to retaliate specifically against those who ordered or carried out the attack. Deterrence has typically been crude in this respect, one reason being that it is often not possible to identify the actual culprits. It is common to hold a state responsible for harmful actions coming from its territory, especially when it has been repeatedly given evidence of this and told it will suffer if the attacks continue. A government with weak control (it claims) over hackers can be threatened and punished for not developing effective control, just like one can be harassed for being a haven for drug traffickers or terrorists. The U.S. can use sanctions on China for tolerating piracy of American entertainment items, and it could do the same for China's allowing and even encouraging hackers to flourish and attack the US. Unwillingness to retaliate in this fashion is a choice made on the basis of what is deemed ethically or politically attractive, or practical; it is not endorsed by deterrence theory or past practice.

In principle, therefore, it is possible to establish a deterrence policy for cyberattacks based on threats of serious harm by defense and retaliation and which would be upheld periodically, directing the harm at a state actor or leaders of a nonstate actor whether they are specifically responsible or not, and even harming people not parties to the attacks. None of this behavior is without precedent. None would be absolutely unacceptable now, *if the scale of the attack and the damage caused that evokes the response is great enough*.

Reluctance to behave this way based on ethical or political considerations is understandable, and reflects concerns to be taken seriously. Today, normative constraints on using force are given far greater consideration and this is certainly welcome. Deterrence is always conducted within a *normative context*, which contributes to shaping what are considered appropriate or legitimate reactions to attacks, and thus the appropriate and legitimate kinds of deterrence threats to deliver. Norms pertain to such things as the scale of harm (as with the concept of proportionality—punishment fitting the offense), the *type* of harm, the threshold that, when crossed, justifies seriously harming an attacker, etc. Deterrence theory basically does not deal with this. Perhaps that is good since norms can change readily, are far from universal, and are often ignored under extreme provocation.

It is also not necessarily required to be highly sensitive to collateral damage in both the threats mounted and the harm inflicted if necessary. Deterrence was initially pursued in the Cold War with exactly the opposite approach: the harm threatened often included maximizing collateral damage. The earliest American nuclear deterrence strategy called for preparations to rapidly escalate a war with the communist world via a massive nuclear attack, with plans to inflict many millions of casualties. There was no concern for collateral damage to people, cultural objects, hospitals, churches, or anything else.

How was that possible? One factor was that the strategy emerged in the wake of an intense war without limits in which the U.S., like other participants, often inflicted indiscriminate destruction. Another was that the enemies were characterized in virtually the same terms as the ones in World War II—monstrous totalitarian regimes. Conducting the Cold War with this enemy in mind gave it considerable potential for sliding into another total war. U.S. deterrence ultimately rested on promising exactly that. The threat had significant credibility because similar consequences had been delivered in recent memory.

We reject thinking in those terms now because we have no conflict so intense, or enemies deemed so despicable.[25] Cyberattacks involve nothing like that. The normative context is therefore much more confining. This could quickly change if international conflicts greatly deepen and intensify and cyberattacks are part of why this happens (such as by becoming much more destructive). It is therefore impossible to specify the future of deterrence in cyberspace conflict. Deterrence is not nice—it is nasty behavior and meant to be so, threatening enough harm to get the opponent to desist. If, as is often the case, this would mean behaving in normally unacceptable ways and doing so is rejected when the time comes, that occurs because of self- or community-imposed constraints. Choosing to accept the constraints is a political decision, not inherent in deterrence.

[25]We come closest to thinking that way with Islamic terrorists in Al Qaeda and the Taliban and our behavior toward them reflects as much when it includes, for example, assassination efforts that include harm to family members or other noncombatants.

THE SPECIAL CONCERN FOR DETERRENCE STABILITY—THE STABILITY PROBLEM

In developing deterrence theory, "stability" received much attention, first in the context of mutual nuclear deterrence and then with respect to the entire Cold War. Stability referred, in the first instance, to deterrence preventing a war, particularly a nuclear war, then to preventing unacceptable escalation in a war—keep major states' wars small and prevent others' wars from drawing the great powers in so they became major wars. Deterrence was also to sustain stability by preventing the use of increasingly destructive weapons and actions in a war. Deterrence was believed less likely to fail, and escalation more likely to be avoided, by preventing proliferation of highly destructive weapons, grievous environmental damage from weapons and warfare, ruinous arms competitions, intense crises, and other dangerous conditions. These and other situations could lead to deterrence failures—destabilizing deterrence. Preventing all this eventually came to be put under the heading of arms control. Arms control covers many other things but its modern version in the Cold War was driven primarily by concerns about deterrence stability.

While a lack of credibility could contribute to deterrence failure, having credibility might not be enough. Deterrence stability is partially linked to the *strength of the opponent's motivation to attack*. Deterrence is supposed to adjust that motivation so an attack does not occur, but it can readily override credible deterrence threats. Often the more intense the opponent's motivation appears, the greater the reliance on deterrence to keep safe—deterrence becomes the ultimate recourse; but the stronger that motivation the less likely deterrence is to work. Deterrence is not at its best when it is needed most.

In terms of stability, therefore, the best time for deterrence threats is relatively early in a conflict, hopefully inhibiting the opponent's desire to attack before it has hardened, attack planning is far along, preparations well underway, etc. Deterrence stability is on better ground in noncrisis than crisis situations. An earlier, broader (general) deterrence is needed to help convince the opponent to abandon thinking about and preparing to attack. When a war occurs, the failure of deterrence began with a breakdown in general deterrence.[26]

Attacker motivation is also related to deterrence stability via concerns about irrationality. It is commonly said that deterrence is undermined if the opponent is irrational. Often what is meant is a fear that the opponent's desire to attack, due to his being irrational, will override deterrence threats.[27] The problem lies not in irrationality, but in *anything* producing an excessive motivation to attack. Sometimes irrationality is the problem, sometimes it is other things, but Cold War governments worried about possible irrationality in their opponents. An important concern in deterrence must be that using threats might enrage an opponent—that deterrence can sometimes provoke an irrational reaction.

Other facets of the stability problem were seen as structural. One was how nuclear weapons reinforced a strong desire in modern war for capabilities to win quickly and relatively cheaply. Nuclear weapons seemed ideal for this, allowing a preemptive attack so devastating the war would be over without a response. In a serious crisis if one side had such a capability it would have an enormous incentive to attack first, to win quickly and cheaply; deterrence would readily fail. In a serious crisis involving two states with such capabilities, each would be desperate to make the initial attack, would race to do so, and deterrence would collapse. The structure of the deterrence postures would be responsible for the disintegration of deterrence! This was referred to as the "crisis stability" problem.

Another structural concern pertained to alliances and related arrangements to enhance deterrence against attacks on the members. Deterrence would presumably depend in part on how cohesive the alliances were and Cold War alliances sometimes had problems on this score. The most powerful members worried that concerns about sustaining their deterrence credibility with the allies, or the need to back up an ally that was behaving provocatively, might draw them into wars they could otherwise avoid. The allies worried that their powerful patrons might, should the occasion arise, choose not to defend them and the deterrence they counted on would dissipate. The alliances imposed conflicting interests

[26]See Morgan, P. M. 2003 *Deterrence Now*. Cambridge: Cambridge University Press 80-86.

[27]The target's irrationality, per se, is not harmful to the success of deterrence threats—it is the nature of the irrationality that is important. Many forms of irrationality can enhance, not undermine, deterrence.

that might cause a failure of deterrence. This was a stability problem within the cluster of difficulties involved in extended deterrence (providing deterrence for another actor, typically an ally).

A third structural concern was the incentive for proliferation. Depending on an ally has always been risky, and Cold War allies had the further risk of involvement in a deadly war not of their making. Thus having their own weapons of mass destruction (WMD) could be seen as a better deterrent. Similar concerns promoted interest in proliferation among nonaligned states. Some analysts and governments argued that this would make the international system safer, more stable.[28] Most thought multiplying nuclear powers would increase deterrence failures via more accidents or more conflicts that escalated, or more irrational leaders inciting crises or displaying extreme behavior.

The ultimate impact of the stability problem was the sense that Cold War antagonists' security had become highly interdependent. Intellectual exploration of how to stabilize and supplement deterrence came to highlight cooperative efforts to make it more stable and maintain a political context in which stable deterrence would more readily endure. The resulting efforts were sometimes unilateral: making one's nuclear weapons more secure, less vulnerable to unauthorized use, safer from theft or a fire. Many involved opponents cooperating to make deterrence more robust. Others involved multilateral agreements and related implementation.

All this prodded analysts to go beyond primitive conceptions of how to use cooperation toward viewing Cold War conflict relationships as something like communities needing a degree of management. Cooperative management might include forgoing defenses to keep opponents vulnerable to each other's forces; or unprecedented information-sharing among antagonists about their weapons; or agreeing to forego certain weapons as destabilizing; or cooperating against WMD proliferation.

Relevance for Cybersecurity

In cyberspace security, American deterrence has little credibility to bolster its stability.[29] The U.S. is obviously an attractive target, and the lack of any apparent decline in the strength of motivations to attack it is a bad sign. At lower levels there is no deterrence stability at all. The only comfort is that no major failure, no attack, has generated a serious national security crisis. Not yet.

The most recognizable version of the stability problem at work in cyberspace is how technological change constantly outruns defenses and the global hacking community readily surprises defenders. The attackers may well be doing better than is publically indicated.[30] This readily invites pessimism about the prospects for successful defenses. In the nuclear age pessimism about defenses led to preoccupation with deterrence by threats of retaliation, but it is not yet clear that defenses against cyberattacks will be that ineffective. Highly capable defenses would markedly diminish the problem of cyberattacks. In the meantime, improving detection of and resistance to attacks is vital, as is developing restrictions on connections to systems with so many vulnerabilities. Improving defenses is doubly important because, unlike in the Cold War era, the alternative—deterrence by threats of retaliation—is in even worse shape. If the U.S. is to change this it will have to link threats of retaliation to actions that are more likely and more harmful than appears to be the case now.

A classic recourse for a weak deterrence posture is redundant capabilities for replacing what attacks damage or destroy or to provide sufficient operating capacity while recovery is undertaken. This is especially appealing for nations with large resources. If U.S. defenses remain porous, and retaliatory threats irrelevant, it will be imperative to have more redundant cyber resources and the things dependent on them, capabilities that are constantly changed to match developments. This will be particularly necessary for attack and retaliatory cyber capabilities and their command systems, and should be accompanied by efforts at cleverly hiding or protecting them.

[28]See Kenneth Waltz on this in Sagan, S. D. and K. Waltz. 1995. *The Spread of Nuclear Weapons: A Debate.* New York: W. W. Norton.
[29]As far as I know, no one else's deterrence on cyberattacks has real credibility either.
[30]See Bowden, M. 2010. The Enemy Within. *The Atlantic,* June, 72-83.

The most important version of the stability problem in cyber security would be cyberattacks able to inflict a rapid, cheap defeat of an American military effort abroad or as a direct attack on the U.S. itself. There is no certainty that cyberwar capabilities will ever be this potent, but it is vital to consider the possibility. The losses need not be directly military but could exploit the rising dependence of the U.S. and its friends on cyberspace in many areas, inflicting grave damage not readily corrected. The motivation to have this kind of attack capability will only be enhanced if it turns out to be attainable by even small actors; cyberattacks will become a great leveler and very attractive for that reason.

If this capability comes into existence, it will probably emerge unevenly and unpredictably, in sharp contrast with the Cold War when the initial states to take up nuclear weapons were obvious, they did so gradually and visibly, and only two possibly achieved universally applicable first strike capabilities. The cyberattack equivalent would more likely resemble how the U.S. acquired an enormous advantage in conventional warfare almost unnoticed, which came as a major shock to others in 1991. It could be even more startling. Deterrence postures could be rapidly outmoded, perhaps repeatedly, by the appearance of dangerous new versions of cyberattack capabilities. Deterrence postures would need to be very nimble indeed.

The most glaring stability concern in the Cold War era was the problem of reciprocal fear of surprise attack. One aspect was that, if badly designed, a visible military buildup taken to deter could incite fear that led to an opponent attacking instead. Fortunately, the initially destabilizing effects of developing similar cyber capabilities seem much more avoidable. There is no sign that preparations alone to defend against or retaliate for a cyberattack are necessarily so *vulnerable to being attacked first*—and so evident—that they will incite an attack.[31] The preparations would be difficult to detect.

On the other hand, since they will likely not be readily visible, the emergence of capabilities for disarming or otherwise very crippling preemptive cyberattacks will be a real nightmare, and just the possibility of this is therefore very disturbing. Indications that this might be happening will cause alarm not just for the actors involved but also for broader stability in international politics. Both a potential attacker and the target would have to prepare for the worst. This could lead governments basing defensive and retaliatory preparations on the opponent's *hypothetical* attack capabilities, with each side operating from what it infers, on the basis of its own research, cybersystems, and espionage efforts, about what the opponent has.[32] With cyberattacks more feasible and more readily mounted (given the right secret preparations) with little transparency, this could sharply escalate the hair trigger nature of serious confrontations via the reciprocal fear of surprise attack. Mutual cyber first-strike capabilities would set up the severe structural instability once again (the crisis stability problem) of states racing to use them first before they could be lost in an enemy attack, the instability exacerbated if each opponent was uncertain how advanced the other side's capabilities were and turned to a worst-case analysis.

As for alliances and the complications they pose for deterrence stability, the incentives to develop potent cyberattack capabilities will apply much more broadly. Compared with nuclear weapons, the costs seem likely to be modest. Many states and other actors may soon have considerable ability to do serious harm—*proliferation of relevant capacities is already widespread*. This will pose quite a different problem from the nuclear proliferation threat which has taken years to involve only a limited number of actors.

During the Cold War the superpower alliances somewhat inhibited proliferation via extended deterrence. The U.S. is already seeking cooperative relationships with allies for dealing with cyberthreats,[33]

[31]Apparently some analysts fear that those kinds of preparations may turn out to be vulnerable enough to invite attacks.

[32]This would be a throwback to aspects of Cold War deterrence. There were frequent instances then in which deterrence strategy and practice were heavily influenced by hypothetical threats, some described in very dramatic terms, leading to considerable arms racing, a good deal of which later proved unfounded.

[33]See for example: C. Levitt. February 10, 2010. U.S. Seeking Allies for Warfare in Cyberspace. Available at http://www.smh.com.au/technology/us-seeking-allies-for-warfare-in-cyberspace-20100214-nzg2.html; and Kyodo News. May 4, 2010. Japan-US to Cooperate in Combatting Cyber Attacks. *NAPSNet Daily Report* May 5, 2010. Available at www.nautilus.org/mailinglists/napsnet under Mailing lists—Daily Report.

and this will presumably expand, especially since the U.S. and its allies are integrating many cybersystems for military cooperation purposes. However, the cyberattack cooperation involves exchanging expertise plus some relevant technology, and getting help from allies once a major attack occurs mainly in the form of visiting experts. It is not a matter of the U.S. specifically defending an ally, other than in the sense that when shared systems are under attack everyone will need to work together to beat it off. Pushing integration to where the U.S. would defend its allies systems would face strong objections that (a) this would expand American vulnerabilities via the integration of cybersystems, (b) an attack on an ally would automatically draw the U.S. into resisting it with no time to assess U.S. interests in doing so, and (c) many of the costs and burdens are much more affordable for the allies now than in the past.

It is difficult to assess the prospective stability problems associated with conflict escalation in cyberattacks. If U.S. alliances are adjusted to include *retaliating* for cyberattacks on allies, which seems quite possible, then escalation can take place through U.S. retaliation and the responses it provokes. A more interesting route is that damage by cyberattacks into systems can spread out of control. This is not a form of escalation deterrence can handle. Whether the attack was launched deliberately or inadvertently, deterrence cannot be expected to prevent its consequences from expanding thereafter.

Finally, we come to how arms control was the ultimate Cold War response to various versions of the stability problem. The starting point was that even serious opponents had strong incentives to cooperate to manage their security relationship and the security environment because they have overlapping national interests. That also led to broader multilateral efforts at security management on conflicts and arms, reflecting how security interdependence affected everyone's welfare. Eventually, the cooperation extended across a wide range of activities. How does this experience apply to the cyberattack problem?

Interdependence in cyberspace has yet to become an equivalent threat, so that particular incentive to cooperate is not yet fully in play. But in the everyday conduct of very important activities, societies' interdependence in the cyber age is profound, is much broader and deeper, is much more apparent, and will continue to rapidly expand. The cybersecurity problem is already virtually universal in character; abuse of cyberspace can affect almost anyone. As long as cyberattacks are more annoying than deadly, they are a cost of interdependence that is more than offset by the benefits. But if they begin to pose grave threats to national security, or it becomes vital to prevent that, the arms control perspective will be increasingly relevant.

However, arms control was aimed at making deterrence stable, i.e. very effective, with deterrence considered the key to managing national and international security. Arms control was not an alternative to deterrence; it was making reliance on deterrence more successful and less burdensome. This is directly relevant to cybersecurity because the capacity to do harm to and via cyberspace cannot be eliminated (for the foreseeable future). It is necessary to make living with that fact less burdensome. Cooperation can reduce vulnerabilities to being harmed, strengthen the effectiveness of deterrence by defense, and improve the possibilities for deterrence by significant retaliation in response to attacks. This is cooperation to make cyberspace itself more safely manageable, resembling what Cold War arms control sought to achieve.

However, the prior effort was containing *destabilizing* aspects of security relations between intense opponents, including destabilizing effects their armaments provoked, but not by seeking to eliminate those arms and resolving or diminishing the intense conflicts. The arms were considered an important component of the arms control effort in that they provided much of the stability it was vital to preserve. Thus arms control adjustments of the international status quo were needed, but little had to be fundamentally changed. After all, stability via deterrence rested on living with an enormous ever-present threat.

In cyberspace the means for inflicting harm and resulting attacks are not essential; they threaten key qualities of cyberspace and disrupt its proper operations. Unlike national and international security during the Cold War, cyberspace is not meant to be a threat-based system or a threat-managed system. Thus the intended function of deterrence and its arms control component must be much different.

Cyberspace security requires reducing attacks or their effects as much as possible, so eliminating the capabilities for attacks or reducing the effects achieved by attackers as much as possible is quite appropriate. Arms control is needed not to facilitate and sustain the utility of deterrence, but to reduce the necessity of deterrence and curb the capacities to override it while other important things are done to improve cyberspace security.

Needed is a much differently designed and regulated cyberspace, including improved cooperation and more transparency among governments, societies, and private actors on cyberspace matters. All of this will be needed on a much broader scale than now and certainly more than Cold War arms control arrangements required. It will include more intrusive regulation and verification arrangements. Elaborate cooperation on threat perceptions, attack detection, and identification/apprehension of those responsible for attacks will be needed. New international organization arrangements for these efforts will be necessary. Deterrence is needed to help promote cooperative activities that sharply diminish the importance of deterrence. And arms control is needed not to stabilize deterrence but to funnel overlapping societal interests in the interactions in cyberspace into management that reduces its security threats, including the actors' capacities to do harm. Thus even though the threat of attacks will not be eliminated, by not making threat capacities the key to sustaining security the arms control needed is somewhat closer to disarmament than the arms control devised and practiced during the Cold War.

Next, while Cold War arms control sometimes involved numerous actors, fundamentally it was the work of a small number—especially in the major negotiations. Those who had to cooperate extensively were relatively limited, and some important steps could be taken unilaterally. Sustaining and stabilizing security in cyberspace will likely involve a great many more actors. Widespread cooperation will be needed to make significant adjustments, such as shrinking flaws, in cyberspace systems that generate such extensive vulnerabilities and therefore such strong inducements for attackers to do their thing.[34] Fortunately, and in contrast to the Cold War, such arrangements can be undertaken before a full blown version of the threat that cyberattacks may someday pose emerges. This valuable opportunity should be exploited.

The result will be a sharp departure from the Cold War model of uneven cooperation to secure limited constraints on states so as to enhance security management. Needed for this new kind of security problem is development of collaborative operation of cyberspace as a collective resource, involving states and a variety of other actors. It will be the difference between keeping specific grievous Cold War threats and conflicts in check via independent deterrence posture and collectively lowering threats and conflicts in cyberspace matters to a much more tolerable level.

Pessimism that all this can be done is certainly understandable. Cold War arms control, limited as it was, required strenuous efforts to get a much more modest level of cooperation. The conflictual, political, and bureaucratic obstacles were daunting and many observers felt that the achievements fell well short of what Cold War national and international security required, right up to when the Cold War began to dissolve.

However, pessimism should be tempered today by the extensive experience at such things, when clearly necessary, already accumulated in the international effort to contain and curb the terrorism problem or the threats from potential new epidemics, and the initial steps toward management of Earth's climate, or the threats of global economic collapse. Perhaps the most distinctive element of today's international system is its burgeoning interdependence across many fields via endlessly proliferating interactions. The problems stemming from this, facilitated or actively stimulated by rising interactions, are multiplying rapidly, and they already involve participation much broader and deeper, transparency much greater, and transnational operations much more penetrating and fine-grained than the international security cooperation projects we were used to in the past. The progress made to date is rather

[34]Some very appealing features of the web may be sacrificed: autonomy, anonymity, decentralization, considerable tolerance for misbehavior. For example, the Obama administration has proposed new arrangements that would curb the anonymity of internet users. See Markoff, J. July 4, 2010. Taking the Mystery Out of Web Autonomy. *New York Times*.

astonishing in historical perspective, as major cooperative international endeavors go, in such a short time. The problems with cyberspace are just an extension of the same underlying conditions. We are embarked on expanding the management of the international system in almost every direction; we need to embed cooperative management of cyberspace more deeply in this broader effort.

Finally, Cold War arms control got under way only after the United States had already constructed an enormous nuclear and conventional deterrence posture and the Soviet Union was busy catching up. The benefits of it came only slowly thereafter, swimming against a strong-running tide. We are still early in the emergence of major cyberattack capabilities, and have a chance to short-circuit their growth and spread and perhaps even reverse it. Cooperative efforts to deal with the problem of cyberattacks should be sharply escalated as soon as possible.

The main difficulty will be that the incentives for much greater cooperation are less potent now than the initial incentives were for Cold War arms control. The costs of major weapons, the intensity of the political conflicts they reflected, the environmental consequences of just having those major weapons, and the opportunity costs of the huge emphasis on military forces were all much higher then. Cyberattack capabilities, on all these measures, are more like biological weapons than nuclear and huge conventional weapons and forces in this regard.

CONCLUSION: WHAT SHOULD A GOOD CYBERDETERRENCE POSTURE LOOK LIKE?

Deterrence during the Cold War was developed for helping regulate a type of international politics that has been set aside and which we have every reason to want to never see again. Many of the most salient characteristics of that deterrence therefore have little relevance today. At present the cyberattack problem is quite different in scale and character. Some of the most applicable lessons of Cold War deterrence are essentially negative—on why it does not apply or should be avoided. A few can be be helpful in devising a less dominant, less imposing use of deterrence. However, the most important lesson from that period is that cooperative security management should be taken to heart and applied even more elaborately today because the scale and interpenetration of the interdependence embodied in cyberspace are so much greater. Cyberattacks represent not the threat of everyday order being overwhelmed in a vastly destructive conflict, but a manifestation of a dark side to some central features of everyday order now—a much less esoteric, more intimate threat.

To deal with it will require a cyberdeterrence posture that eventually consists of:

- **Defenses for immediately responding to attacks.** With cyberattacks, even a short delay in detecting and responding to an attack can be catastrophic. Defenses are needed that immediately provide protection, to mitigate the damage done, and that capability requires detection first. This is vital because there are so many attacks, often not all that important and springing from motivations deterrence cannot normally daunt. What is disturbing is that attackers are so often better at detecting weaknesses in systems vulnerable to exploitation than the defenses are.
- **Backup defenses that are much more impressive.** These are needed to handle the real concern: more serious, more deeply penetrating, and more elaborately crafted attacks. Such defenses are, beyond offering crucial protection, vital for a serious deterrence by defense. Much of the problem now is that attackers can keep on probing not only because this may not be costly but also because there is often no major backup when a defense is breeched. This concern is familiar in shaping defenses of borders, with backup capabilities being the real heart of the defense. And some of the capabilities should be retaliatory, such as equipment that reaches out quickly to strike at, even destroy, machines used in attacks—equipment that should be used only when the harm from attacks is of very great concern.
- **Capacities for suitable retaliation when necessary in a more measured fashion.** These should encompass various forms of harm, cyber and otherwise, including military, economic, and political efforts and also steps to publicly provide evidence as to the identities of the attackers—seeking to embarrass the sources or generate greater pressure on them, in a fashion similar to the way this is done

on human rights violations. The retaliation should inflict more harm than the U.S. currently practices, and threats to use it must be given more credibility than is now the case.

- **Significantly greater redundancy in cyberspace resources.** Deterrence is a sometime thing—attacks cannot be completely avoided. With regard to attacks, things are changing so fast that the backup resources will need constant updating based on sensitivity to technical and environmental changes. And the necessity to better defend, via redundant capabilities, the valuable private sector resources is critical.
- **Active promotion of collective arms control and related management in cyberspace.** This will require long, hard work. The universality of the problem and its growing scale must be stressed. Success will require considerable reordering of cyberspace, with much more regulation, plus new organizations and networks to oversee required norms and practices. In a familiar pattern, enhancing security will require more controls, less freedom of action, and less tolerance for a cyberspace wide open for reckless individualism.