The "Korean" Cyber Attacks and Their Implications for Cyber Conflict

James A. Lewis
Center for Strategic and International Studies
October 2009

It has been several months since the basic "denial of service" attacks against networks in the United States and South Korea in early July. No one has yet taken credit, nor have others been able to determine the attackers' identity. As with many other cyber incidents, there is no conclusive evidence as to who was responsible.

Cyberspace enables anonymous attacks. Identities are easily concealed or fabricated in cyberspace, and an astute opponent will of course make it look as if another was responsible for an attack. The use of botnets complicates attribution - the source of an attack, at the first iteration, will be innocent and unknowing third parties. Forensic work may eventually reveal the source of an attack, but a sophisticated opponent will be able to operate clandestinely and with a high degree of deniability. The "Confickr" worm is a good example of this difficulty. Confickr was a global malware that infected millions of computers.[1] Many companies and governments made a coordinated effort to fend it off, but we still have no idea who launched Confickr, what their intent was, or even whether it has been removed from all infected systems.

This failure of attribution leads to several conclusions on state of cyber conflict. Cyber conflict is a new and complicated strategic problem. There is neither an adequate policy framework to manage conflict in cyberspace nor a satisfactory lexicon to describe it. Uncertainty is the most prominent aspect of cyber conflict – in attribution of the attackers identity, the scope of collateral damage, and the potential effect on the intended target from cyber attack. Many concepts – deterrence, preemption, proportional response – must be adjusted or replaced for the uncertain cyber environment.

This uncertainty has significant political implications for both attackers and defenders and creates constraints and thresholds for the use of cyber "weapons." Cyber attacks use software as a weapon launched over interconnected networks, to coerce an opponent or damage its ability to provide essential government, economic or military services. Advanced cyber weapons cause disruption or damage to data and critical infrastructure. A serious cyber attack would be an incident that disrupted critical services for an extended period, perhaps damaging military command or information systems, shutting off electrical power or fuel pipelines, or interrupting financial services. Cyber conflict will be part of warfare in the future and advanced militaries now have the capability to launch cyber attacks not only against data and networks, but also against the critical infrastructure that depend on these networks.

The July event was not a serious attack. It was more like a noisy demonstration. The attackers used basic technologies and did no real damage. To date, we have not seen a serious cyber attack. That is only because the political circumstances that would justify such attacks by other

[1] Computer networks for the French Navy, the Bundeswehr and the UK's Ministry of Defense were infected and in some cases disrupted.

militaries have not yet occurred and because most non-state actors have not yet acquired the necessary capabilities. As an aside, this last point undermines the notion of cyber terrorism. The alternative to the conclusion that terrorist groups currently lack the capabilities to launch a cyber attack is that they have these capabilities but have chosen not to use them. This alternative is nonsensical.

The environment for cyber conflict is produced by technologies that were designed for commercial transactions, providing easy and fast connectivity among multiple poorly identified parties. While the leading actors are nation-states, the activities of non-state actors, including commercial entities, cybercriminals and terrorists groups complicate the terrain for cyber conflict. Conflict in cyberspace blends crime, espionage and military action in ways that often render these elements indistinguishable. The use of cybercriminals by states has become an element of cyber conflict – some countries use cyber criminals as agents or mercenaries against other states.

Cyber-warfare will not be a "clean" conflict where only combatants are present in the area of operations. Instead, cyber conflict takes place in a crowded environment where combatants are connected to noncombatants, including allies, friends and neutral third parties. Combatants and noncombatants may even be intertwined and interdependent in cyberspace, so that an attack on a legitimate target may unavoidably damage a neutral party.[2] The mixture of interdependency, anonymity, and multiple state and non-state actors makes managing cyber conflict a complex task.

There are some parallels for cyber conflict with the task of assembling strategic concepts for the use of nuclear weapons, an immense technological innovation that required years of work to reshape American thinking on national security. We are in our thinking about the relationship of cyber conflict to security where we were in the early 1950s concerning strategic thinking on nuclear weapons, and some early writings on nuclear weapons and arms control by scholars like Brodie, Kahn and others are instructive in considering how to approach cyber conflict. There is some merit to this analogy, but it overstates the destructive capacity of cyber weapons and it understates the political uncertainties that complicate operations in cyberspace.

When Does Cyber Attack Become an Act of War?

The "Korean" cyber incidents of early July did not rise to the level of an act of war. They were annoying and for some agencies, embarrassing, but there was no violence or destruction. In this, they were like most incidents in cyber conflict as it is currently waged. Cybercrime does not rise to the level of an act of war, even when there is state complicity, nor does espionage – and crime and espionage are the activities that currently dominate cyber conflict. The individuals and nations that engage in these activities do not think of themselves as engaging in warfare, at least as our current rules define it, and the lack of international norms for cyberspace only reinforces this sense of impunity. If a nation catches a spy, there is an increase in bilateral tensions, it may expel an attaché or demarche the guilty party, but it does not respond with military force.

[2] The operational implication is that a successful cyber attack will require a deep knowledge of target networks and their connections to other networks to increase the probability that only intended targets are damaged.

Cyber incidents in Estonia and Georgia also did not rise to the level of an act of war. These countries came under limited cyber attack as part of larger conflicts with Russia, but in neither case were there casualties, loss of territory, destruction, or serious disruption of critical services. The 'denial of service' attacks used against these countries sought to create political pressure and coerce the target governments, but how to respond to such coercion remains an open question, particularly in light of the uncertain attribution and deniability.[3]

We could begin to identify a threshold for when actions in cyberspace could be considered an act of war if we accepted that an action in cyberspace that produces the equivalent effect as physical sabotage begins to rise to that level. It would be an exceptionally serious matter if a nation sent agents or soldiers across our border to blow up a pipeline or power station and a similar action in cyberspace, unlike crime or espionage, could justify a military response.

Violation of sovereignty is not a useful threshold under current laws and norms for deciding when an event in cyberspace is an act of war or justifies the use of military force. A more forceful assertion of sovereignty in cyberspace could increase security. Cyberspace is best seen as a "pseudo commons," a space where owners have granted the right of way to any and all traffic as long as it does not impose costs or damage upon them.[4] There are a host of "interconnect" agreements[5] that give the illusion of a commons. Under current interconnect rules, traffic is allowed to pass from nation to nation without inspection or confirmation of identity. This passive approach to sovereignty results from political decisions to defer to commercial agreements on interconnection among networks (and the reasons for this are a combination of ideology and commercial concerns).[6] Essentially these agreements allow for the free passage of traffic regardless of payload. The airspace equivalent would be agreement among countries to let any aircraft, military or civilian, overfly their nations as long as they were en route to another destination

Cyberspace is not the high seas. Sovereign control exists for all of the networks that a cyber weapon may use to reach its target – even though this control may last only a few milliseconds. National sovereignty applies completely to cyberspace, even if nations have not always chosen to assert it. There is no moment when a collection of bits moving from one computer to another is not actually on a network that someone owns and that is physically located in a sovereign state. The exceptions might be undersea cables or satellite transmissions, but transmissions over these systems still takes place on a facility where the owner is subject to a nation and its laws.

The legal and governance framework of cyberspace was designed to accommodate commerce, but it also enables covertness and reinforces deniability. Western nations, as the most frequent

[3] During the Estonian incident, a senior German official stated that while denial of service did not trigger NATO's Article 5 (which commits members to come to the assistance of a member under attack), that could change if the sophistication of the attacks increased. We do not know if this statement helped to deter an expansion of the attacks but its effect was probably beneficial.

[4] This idea comes from Christopher Painter

[5] Interconnect agreements are the contracts between telecommunications companies that determine how they exchange traffic

[6] How American ideology and culture shaped cyberspace, is how this is now undergoing subtle changes, as manufacturing spreads to Asia, and as Americans no longer make up the largest number of internet users, deserves its own discussion.

target of cyber attack and those most constrained by law, might gain if they were to decide collectively how to improve governance and what penalties should apply when a sovereign fails to exercise responsibility for actions taken in cyberspace under its jurisdiction.

Ultimately, the decision as to whether something is an act of war rests with a country's political leaders. For example, would it be an act of war if instead of cyber attacks, the North Koreans had hijacked a U.S. Navy vessel off the high seas, killed a few sailors, towed it into port, pillaged the ship and imprisoned the surviving crew? The answer is it depends – in this case (the 1968 attack on the USS Pueblo) the United States chose not to retaliate with military action, just as we chose not to retaliate for the Beirut Bombings or Khobar Towers. Political leaders will want precise information on attribution and on collateral damage before authorizing a cyber counterstrike, and even if this information is available, they may decide that in the larger strategic context, the risks of military action outweigh the benefits, or that there are alternative courses of action that are more beneficial.

This suggests that there can be no reflexive rules of engagement for cyber conflict. Some militaries have rules of engagement for self-defense that give a commander the discretion to fire back when fired upon, without prior approval from higher authorities. This sort of rule could be rarely exercised in cyberspace, if ever, since a counterstrike in cyberspace is likely to lack clear attribution and clear scoping of the side effects on neutral parties.

Deterrence

Weak attribution and unpredictable collateral damage make deterrence ineffective in cyberspace. Deterrence is a threat of retaliation, but it is hard to credibly threaten unknown parties and counterproductive to threaten or damage the wrong party. The United States is widely recognized to have pre-eminent offensive cyber capabilities, but it obtains little deterrent effect from this.

In the absence of attribution, the response options for the United States to the July 4 events were extremely limited. We could not retaliate against an unknown attacker. Deterrence is the threat of violent retaliation. This threat changes the opponent's calculus of the benefits and costs of an attack. But it is hard to convincingly threaten an unknown attacker, and weak attribution makes traditional deterrent concepts – those based on the threat of reprisal for an attack (either counterforce or countervalue) – largely irrelevant in cyberspace.

The interconnectivity of cyberspace makes predicting collateral damage difficult. Uncertainty about the scope of collateral damage involves both unintended effects on the target and also possible damage to third party networks connected to or dependent upon the target network. Disabling or disrupting one network may affect third parties; for example, an attack on an opponent's network might accidently degrade a neutral nation's satellite or telecommunications services. Anecdotal reports suggest that Israeli cyber attacks on Syrian air defense networks also damaged domestic Israeli networks.

Classic deterrence accepted (in theory) a measure of collateral damage. Strikes on invading Soviet forces in Germany would have harmed civilian populations in both allied and enemy

countries. But these strikes were reserved for extreme situations when sovereignty had been clearly violated by military force. The extent of collateral damage for nuclear weapons was in some ways easier to predict than is the case in cyber conflict – the blast and radiation effect of nuclear weapons is limited to an area around impact; in cyberspace, collateral damage may not be contiguous with the target. Uncertainty about collateral damage may hobble deterrence in cyberspace, by reducing the willingness of political leaders to incur the risk of a retaliatory response that goes awry, widening a conflict or creating unfavorable political consequences.

The threat of counterstrike was the basis of deterrence in the Cold War. However, the rationale for this kind of deterrence is not applicable to cyber conflict. In the Cold War, there was symmetry in vulnerabilities – each side had cities and populations that the other could hold hostage. That symmetry no longer exists. The United States is far more dependent on digital networks than its opponents and this asymmetric vulnerability means that the United States would come out worse in any cyber exchange. There was clear attribution in the Cold War that allowed for both credible threats and for "signaling" and tacit understandings between opponents on "redlines" and thresholds. We lack that clarity in cyber conflict. The combination of asymmetric vulnerability, weak attribution and unpredictable collateral damage limit our ability to make a credible threat against an opponent in cyberspace.

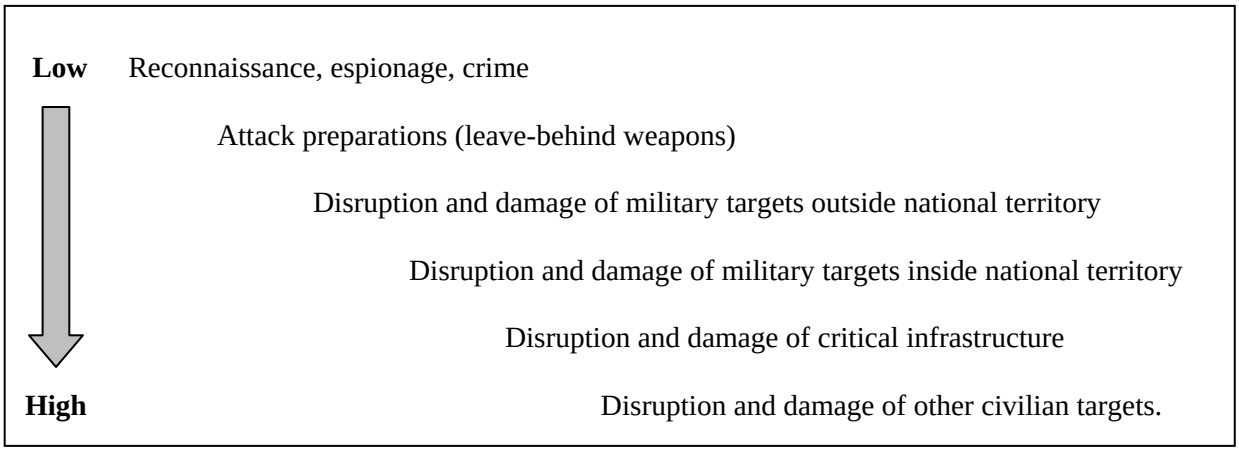
Deterrence relies on more than the implied threat of the use of force in response to an attack. It requires statements about intentions and understanding among potential opponents that define and limit the environment for conflict. Deterrence in cyberspace is limited because we have not adequately assessed what combination of cyber capabilities, defensive measures, and international agreements will make the United States and its allies most secure. It would be useful to undertake a larger strategic calculation, preferably in a public dialogue, to determine the weighting and balance among offensive, defense and multilateral efforts in cyberspace that best reduces the risk of cyber attack.

Norms and Thresholds

The lack of explicit generally accepted international norms for cyber conflict reduces the political risk of cyber attack. Norms can limit the scope of conflict and shape behavior. An opponent's calculus of the benefits of an attack is determined, to varying degrees, by the concern over the reaction of other states. There are implicit norms now for conflict in cyberspace, thresholds that a nation-state attacker is unlikely to exceed. Attackers do not wish to see the current level of cyber conflict lead to an escalation of violence or to some overt disruption of relations. They will strive to remain below these implicit thresholds to avoid this.

The threshold is the line between reconnaissance or exploitation (espionage and crime) and disruption and damage. Crossing this line would escalate any cyber conflict. A secondary threshold could be the move from disrupting or damaging military targets to damaging critical infrastructure or other civilian targets. Norms or thresholds like these would accept a certain level of conflict in cyberspace, but would attempt to increase the risk and consequences for states if they (or actors in their countries) move beyond espionage and crime.

Cyber Conflict Thresholds



A starting point for a discussion of norms and threshold would be to accept that if it is legitimate to attack a target physically, it is also legitimate to attack it using cyber weapons. At a minimum, degradation of an opponent's military networks and information, or the networks that support critical infrastructure, can be defended as legitimate military objectives, but the degree of interconnection with third parties blurs the line between intended and unintended and legitimate and illegitimate targets. A norm that ranked targets by minimizing damage to noncombatants – military networks, then critical infrastructure, then other civilian networks – could provide thresholds and a rationale for retaliatory escalation.

However, there is no agreement or explicit understanding on what is a legitimate target in cyberspace. One approach would be to declare that if it is legitimate to attack a target physically, it is also legitimate to attack it using cyber weapons. Discussion of making some set of networks "sanctuaries" – hospitals, for example – that participants agree not to attack ignores the degree of interconnection that blurs the line between legitimate and illegitimate target. A decision to disrupt power supplies will affect both military targets and hospitals. Cyber attacks against critical infrastructure do not allow for the possibility of sanctuary.

Inadvertent and unpredictable damage to third party networks carries real political risk. The high degree of interconnection in cyberspace means that an attack aimed at an opponent could produce collateral damage not only in third parties but potentially also in the attacker. An attack that damaged the protocols or infrastructure that supports global connectivity is somewhat "suicidal" in that it shuts of the global internet for the target, attacker and neutral parties.[7] There may be instances where a nation may choose this option, but they would be extreme. Non-state actors face fewer constraints, but an attack by them would compromise their own ability to exploit the global internet for operational purposes.

One question to consider is whether we have been too quick to strip cyber conflict from its political context. Given the limitations of deterrence, a nation like the United States, which is uniquely vulnerable, would gain more by creating international norms. These actions would

[7] There is anecdotal evidence that unknown parties have explored the possibility of disrupting the global network.

change the deterrent calculus (by reducing the likelihood of success for an opponent in launching a cyber attack and by increasing the cost of being caught) in ways that that are not achievable by threatening reprisal or retaliation.

Political Constraints on Cyber Attack

These implicit norms politically constrain the actions that the leaders of an attacking state may choose because of risk and uncertainty. Cyber conflict creates political risk. Discovery entails risk, of course, but more importantly, a decision to broaden the scope of an attack from a perpetrators' network or computers to other networks not directly involved, or to move from purely military targets to civilian targets, such as critical infrastructure, brings significant risk of escalation. Inadvertent damage to third party networks, including neutral and allies, also carries significant political risk. A decision to expand the intensity or scope of cyber attack risks the escalation of conflict. The political consequences of cyber attack, should it move from espionage and exploitation to disruption and damage, need to be brought into the open and discussed.

Only a few nations –Russia, China, Israel, France, the United States, and the United Kingdom, and perhaps a small number of the most sophisticated cyber criminals – have the advanced capabilities needed to launch a cyber attack that could do serious and long-term damage equivalent to sabotage or bombing and thus rise to the level of an act of war. A sophisticated attack against infrastructure requires planning, reconnaissance, resources and skills that are currently available only to these advanced cyber attackers. As part of their larger military planning, these nations have likely planned to launch such attacks in the event of a crisis.[8] Such attacks are not yet within the scope of capabilities possessed by most non-state hackers.

Serious cyber attack independent of some larger conflict is unlikely. To transpose cyber to the physical world, there are remarkably few instances of a nation engaging in covert sabotage attacks against another nation (particularly larger powers) unless they were seeking to provoke or if conflict was imminent. The political threshold for serious cyber attack (as opposed to espionage) by a nation-state is very high, likely as high as the threshold for conventional military action. At a minimum, this suggests that a serious cyber attack is a precursor, a warning, that some more serious conflict is about to begin.

Absent such larger conflict, however, a nation-state is no more likely to launch a serious cyber attack than they are to shoot a random missile at an opponent.[9] The risk is too great and the benefits of a cyber attack by itself too small for political leaders to authorize the use of this capability in anything short of a situation where they had already decided on military action. Cyber weapons are not decisive; cyber attack by itself will not win a conflict, particularly against a large and powerful opponent. It is striking that to date; no cyber "attack" that rises above the level of espionage or crime has been launched outside of a military conflict.

Even in a conflict, a decision to strike civilian targets in an opponent's homeland using cyber

[8] There is anecdotal evidence that the intelligence services or militaries of several nations have 'mapped' digital infrastructure in the United States to provide the capability for cyber attack in the event of a conflict.
[9] This raises the question of command and control of cyber capabilities and the possibility of an inadvertent attack.

weapons is a major step that brings the risk of serious escalation. Engaging American military forces overseas is not the same as attacking critical infrastructure in the United States. Nations may reserve these serious cyber attacks against targets in the opponent's homeland for either retaliation for attacks against their own homeland or for when they are in extremis.

Nuclear doctrine very quickly settled into a pattern where the use of nuclear attack was reserved, to be used only in extremis.[10] Careful calculation is needed to see if the same should be true for cyber attacks against civilian targets in an opponent's sovereign territory. We and our opponents are unlikely to renounce the use of some forms of cyber action involving espionage or low level disruption, but a more serious attack may likely be reserved for the most serious situations. The deterrent value of a cyber response might be increased if our public doctrine reserved the most serious attacks (those that led to major disruption of critical infrastructure) for retaliation.

Non-State Actors in Cyberspace

Non-state actors do not face the same political constraints that apply to state actions in cyberspace. They are much less likely than states to be deterred by the threat of military force. In theory, a non-state actor could hire cybercriminals to launch an attack that was beyond its own capabilities, and there is one media report that Israel suspects the Hamas or Hezbollah may have hired Russian cybercriminals for an attack against its networks.

But cybercriminals operate in a political context. The most skilful non-state actors live in "sanctuaries," where they are tolerated by the government. An informal arrangement between government and cybercriminal, where a cybercriminal limits criminal activity to targets outside the host nation, perhaps pays the occasional bribe to local law enforcement, and agrees to be responsive to requests for assistance in attacking targets designated by the government, would please everyone. The cybercriminal can live well, the local economy benefits, and the government gains a powerful weapon with a strong case for "plausible deniability" when it is used for political purposes, as appears to be the case in Estonia or Georgia.

We should not forget that many of the countries that are havens for cybercrime have invested billions in domestic communications monitoring to supplement an already extensive set of police tools for political control. The notion that a cybercriminal in one of these countries operates without the knowledge and thus tacit consent of the government is difficult to accept. A hacker who turned his sights from Tallinn to the Kremlin would have only hours before his service were cut off, his door was smashed down and his computer confiscated.

There is a benefit from this dependence of advanced and persistent cybercrime on state tolerance, however. It provides a degree of constraint on support for cyber terrorism. Most sophisticated cybercriminals operate with tolerance of the country they live in, acting according to a set of informal rules on what they can target. Financial crimes, the theft of intellectual property, political activism and extortion are tolerated. Actions against the host state or actions that approach the act of war threshold and threaten to escalate cyber conflict are not. The political environment in which the most advanced cybercriminals exist militates against them becoming mercenaries for many terrorist groups without the consent of their host.

[10]This idea comes from Arnold Kantor

A nation that has advanced cyber attack capabilities or which harbor sophisticated cyber criminals could decide to supply an advanced cyber capability to a terrorist group, either through direct support or by tacit permission to cybercriminals, but this would be a major political decision fraught with extreme risk of conflict if it were discovered. More importantly, it would likely go against the country's own interests. The nations with the most advanced cyber capabilities - Israel, France, Russia, the United States, the United Kingdom, or China – are unlikely to support cyber jihad.

For cybercriminals to act as mercenaries in launching serious attacks for terrorist groups, they would likely need the tacit approval of their host government. The countries that tolerate cybercrime have their own concerns with jihad and, absent some change in the political equation that makes the risk of conflict seem acceptable or that redefines support for jihad as acceptable (or at least support for jihadi attacks against other nations), these nations are unlikely to tolerate their sophisticated cybercriminals becoming mercenaries for jihadi groups. This suggests that for now, it will be difficult for terrorists, particularly Islamic terrorists, to gain access at this time to advanced capabilities.

Even if we accept this political constraint on mercenary support for cyber terror, other trends suggests that terrorist use of advanced cyber weapons (if current trends remain unchanged) is inevitable. A thriving black market in software attack tools, personal information, botnets and other criminal devices support cybercrime. These can be purchased or rented, or a criminal can be hired to carry out an attack. At this time, what is available on the black market is not sufficient for an advanced cyber attack. This will change, however, in a matter of years.

A very rough estimate would say that there is a lag of three and eight years between the capabilities developed by advanced intelligence agencies and the capabilities available for purchase or rental in the cybercrime black market.[11] The evidence for this is partial and anecdotal, but the trend has been consistent for more two decades. This suggests that in less than a decade, perhaps much less, a terrorist group could enter the cybercrime black market and acquire the capabilities needed for a serious cyber attack.

Faith is not a Defence

Currently, only a few nations with advanced capabilities can unleash a serious cyber attack. But they are unlikely to do so outside the context of a larger crisis (although we should expect to see continued covert reconnaissance and perhaps testing of cyber attack capabilities). Serious cyber attacks by non-state actors is now only likely if a nation with advanced capabilities decided to support them by providing advanced capabilities (including the option which provides a greater degree of deniability, of allowing sophisticated cybercriminals among their citizenry to support such attacks).

At this time, no nation with advanced cyber capabilities is likely to provide such support. None of the six or so nations with these capabilities has any affinity for jihad, all are at risk of

[11] This estimate is based on a small and informal sample of advanced technologies that were first only available to government entities but which then appeared in the cybercrime black market.

terrorism, and they are no more likely to help non-state actors in cyber conflict than they are to provide any other kind of weapon or support. However, as cyber technologies continues to diffuse, as the tools available on the black market become sufficient for a serious cyber attack, and as the sophistication of non-state opponents continues to grow, we must recognize that the degree to which political constraints on state actors limit the possibility of serious cyber attack by non-state actors will decline.

The implications for the United States are troubling. We have, at best, a few years to get our defenses in order, to build robustness and resiliency into networks and critical infrastructure, and to modernize our laws to allow for adequate security. Our current defenses are inadequate to repel the attacks of a sophisticated opponent. The United States will need to define doctrine for the use of the cyber attack as a tool of national power. It would benefit from an effort to reshape the international environment for cyber conflict in ways that could reduce risk, to win consensus (as we did with proliferation) on a set of norms and constraints for cyber conflict and on the relations of states with criminals and terrorists. Frankly, many colleagues do not believe we as a nation will be able to do this and only a successful major attack will spur the United States to make the needed changes.