Statement for the Record

House Permanent Select Committee on Intelligence

The Cyber Threat

4 October 2011

Mister Chairman, Senior Member Ruppersberger, thank you very much for including me in today's testimony. It's good to be back among some old friends.

I have been asked to say a few things about the cyber threat. Earlier this year I received the same request from Air University, the Air Force's institution of higher learning, and in response I published an article in their Strategic Studies Quarterly entitled, "The Future of Things Cyber."

I have updated the article and submit that update as my statement for the record.

I began in January recounting that years ago, when I was an ROTC instructor, the first unit of instruction for rising juniors dealt with communication skills. Near the beginning of the unit, I would quote Confucius to my new students: "The rectification of names is the most important business of government. If names are not correct, language will not be in accordance with the truth of things." The point had less to do with communicating than it did with thinking—thinking clearly. Clear communication begins with clear thinking. You have to be precise in your language and have the big ideas right if you are going to accomplish anything.

I am reminded of that lesson as I witness and participate in discussions about the future of things "cyber." Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon. Do not get me wrong. There are genuine experts, and most of us know about patches, insider threats, worms, Trojans, WikiLeaks, and Stuxnet. But few of us (myself included) have created the broad structural framework within which to comfortably and confidently place these varied phenomena. And that matters. I have sat in *very* small group meetings here in Washington, been briefed on an operational need and an operational solution, and been unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of *any* decision we might make.

US Cyber Command has been in existence for almost two years now, and no one familiar with the command or its mission believes our current policy, law, or doctrine is adequate to our needs *or* our capabilities. Most disappointingly—the doctrinal, policy, and legal dilemmas we currently face remain unresolved even though they have been around for the better part of a decade. Now ~~it is~~ is the time to think about and force some issues that have been delayed too long. This committee hearing could not be more timely as it surfaces questions, fosters debate, and builds understanding around a host of cyber questions. The issues are nearly limitless, and many others will emerge today's testimony, but let me suggest a few that frequently come to the top of my own list.

How do we deal with the unprecedented? Part of our cyber policy problem is its newness and our familiar experience in physical space does not easily transfer to cyberspace. Casually applying well-known concepts from physical space like deterrence, where attribution is assumed, to cyberspace where attribution is frequently *the* problem, is a recipe for failure. And cyber education is difficult. In those small group policy meetings, the solitary cyber expert often sounded like "Rain Man" to the policy wonks in the room after his third or fourth sentence. As a result, no two policy makers seemed to ~~have left~~leave the room with the same understanding of what it was they had discussed, approved, or disapproved. So how do we create senior leaders—military and civilian who are "cyber smart enough"?

Is cyber really a domain? Like everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, *cyber*. It trips off the tongue, and frankly I have found the concept liberating when I think about operationalizing this domain. But the other domains are natural, created by God, and this one is the creation of man. Man can actually change t~~his ~~this geography and *anything* that happens there actually creates a change in someone's *physical* space. Are these differences important enough for us to rethink our doctrine? There are those in the US government who think treating cyber as an independent domain is just a device to cleverly mask serious unanswered questions of sovereignty when conducting cyber operations. They want to be heard and satisfied before they support the full range of our cyber potential.

Privacy? When we plan for operations in a domain where adversary and friendly data coexist, we should be asking: what constitutes a twenty-first-century definition of a reasonable expectation of privacy? Google and Facebook know a lot more about most of us than we are comfortable sharing with the government. In a private-sector web culture that seems to elevate transparency to unprecedented levels, what is the appropriate role of government and the DoD? If we agree to limit government access to the web out of concerns over privacy, what degree of risk to our own security and that of the network are we prepared to accept? How do we articulate that level of risk to a skeptical public and who should do it?

Do we really know the threat? Former Director of National Intelligence Mike McConnell frequently says we are already "at war" in cyberspace. Richard Clarke even titled his most recent cautionary book, *Cyber War*. Although I generally avoid the "at war" terminology, I often talk about the inherent insecurity of the web. How bad is it? And if it is really bad, with the cost of admission so low and networks so vulnerable, why have we not had a true cyber Pearl Harbor? Is this harder to do than we think? Or are we just awaiting the inevitable? When speaking of the threat, citizens of a series of first-world nations were recently asked whom they feared most in cyberspace, and the most popular answer was not China or India or France or Israel. It was the United States. Why is that and is it a good thing? People with money on the line in both the commercial and government sectors want clear demonstrable answers.

What should we expect from the private sector? We all realize that most of the web things we hold dear personally and as a nation reside or travel on commercial rather than government networks. So what motivates the private sector to optimize the defense of these networks? Some have observed that the free market has failed to provide an adequate level of security for the net since the true costs of insecurity are hidden or not understood. I agree. Now what: liability statutes that create the incentives and disincentives the market seems to be lacking? Government intervention, including a broader DoD role to protect critical infrastructure beyond .mil to .gov to .com? The statutory responsibility for the latter falls to the Department of Homeland Security, but does it have the 'horses' to accomplish this? Do we await catastrophe before calling for DoD intervention or do we move preemptively?

What is classified? Let me be clear: This stuff is overprotected. It is far easier to learn about physical threats to the U.S. from US government agencies than it is to learn about cyber threats. In the popular culture, the availability of 200,000 applications for my smart phone is viewed as an unalloyed good. It is not—since each represents a potential vulnerability. But if we want to shift the popular culture, we need a broader flow of information to corporations and individuals to educate them on the threat. To do that we need to recalibrate what is truly secret. ~~Beyond this tactical concern, o~~Our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a *common* body of knowledge. With no common knowledge, no meaningful discussion, and no consensus . . . the policy vacuum continues. This will not be easy, and in the wake of WikiLeaks it will require courage, but it is essential and should itself be the subject of intense discussion. Who will step up to lead?

What constitutes the right of self-defense? How much do we want to allow private entities to defend themselves outside of their own perimeter? Indeed, what should Google appropriately do *within* its own network when under attack from the Chinese state? I have compared our entry into cyberspace to mankind's last great era of discovery—European colonization of the Western Hemisphere. During that period large private corporations like the Hudson Bay Company and the East India Tea Company acted with many of the attributes of sovereignty. What of that experience is instructive today for contemplating the appropriate roles of giants like Google and Facebook? We probably do not want to outfit twenty-first-century cyber privateers with letters of marque and reprisal, but what should be the relationship between large corporations and the government when private networks on which the government depends are under sustained attack?

Is there a role for international law? It took a decade last century for states to arrive at a new Law of the Seas Convention, and that was a domain where our species had had literally millennia of experience. Then, as a powerful seafaring nation, we tilted toward maritime freedom rather than restraints. Regulating cyberspace entails even greater challenges. Indeed, as a powerful cyber faring nation, how comfortable are we with regulation at all? After all, this domain launched by the DoD has largely been nurtured free of government regulation. Its strengths are its spontaneity, its creativity, its boundlessness. The best speech given by an American official on macro net policy was given late last year by Secretary of State Clinton when she emphasized Internet freedom, not security or control or regulation. But there are moves afoot in international bodies like the International Telecommunications Union to regulate the Internet, to give states more control over their domains, to Balkanize what up until now has been a relatively seamless global enterprise. How and when do we play?

Is cyber arms control possible? As a nation, we tend toward more freedom and less control but—given their destructiveness, their relative ease of use, and the precedent their use sets—are distributed denial-of-service attacks *ever* justified? Should we work to create a global attitude toward them comparable to the existing view toward chemical or biological weapons? Should we hold states responsible if an attack is mounted from their physical space even if there is no evidence of complicity? And, are there *any* legitimate uses for *botnets*? If not, under what authority would anyone preemptively take them down? These are questions for which no precedent in law or policy (domestic or international) currently exists. If we want to establish precedent, as opposed to likely unenforceable treaty obligations, do we emphasize dialogue with like-minded nations, international institutions . . . or multinational IT companies?

Is defense possible? At a recent conference I was struck by a surprising question: "Would it be more effective to deal with recovery than with prevention?" In other words, is the web so skewed toward advantage for the attacker that we are reaching the point of diminishing returns for defending a network at the perimeter (or even beyond) and should now concentrate on how we respond to and recover from inevitable penetrations? This could mean more looking at *our own* network for anomalous behavior than attempting to detect every incoming zero day assault. It could mean concentrating more on what is going out rather than what is coming in. It could mean more focus on mitigating effects and operating while under attack rather than preventing attack. Mike McConnell and I met with a group of investors late last year, and we were full-throated in our warnings about the cyber threat. One participant asked the question that was clearly on everyone's mind, "How much is this going to cost me?" At the time I chalked it up to not really understanding the threat, but in retrospect our questioner may have been on to something. At what point do we shift from additional investment in defense to more investment in response and recovery?

Where should we work in the risk equation? For those who attempt to measure risk, the routine formula is that risk is equal to the level of threat times our own vulnerability times the consequences of a successful attack. If any of these factors are pushed close to zero—there is not a threat, I am nearly invulnerable, I am indifferent to the consequences—risk approaches zero as well. To date we have put an overwhelming majority of our energy into reducing vulnerabilities, making our attack surface smaller with good cyber defenses. Although this will (and must) continue, we may be reaching diminishing marginal returns on these efforts so we are now seeing more energy being put into managing the consequences of a successful penetration of a network. Words like resilience and operating while under attack are becoming more common. And there is now even speculation about how to reduce the threat itself through international norms and the like. Where should we put our weight of effort?

There are more questions that could be asked, many of them as fundamental as these. Most we have not yet answered or at least have not yet *agreed* on answers and none of them are easy. How much do we really want to empower private enterprises to defend themselves? Do we want necessarily secretive organizations like ~~the~~ NSA or CyberCom going to the mats publicly over privacy issues? At what point does arguing for Internet security begin to legitimate China's attempts at control over Internet speech? Do we really want to get into a public debate that attempts to distinguish cyber espionage (which all countries pursue) from cyber war (something more rare and *sometimes* more destructive)? Are there any cyber capabilities, real or potential we are willing to give up in return for similar commitments from others?

Tough questions but until these and other questions like them are answered, we could be forced to live in the worst of all possible cyber worlds—routinely vulnerable to attack and self-restrained from bringing our own power to bear.