Center for International and Security Studies at Maryland
School of Public Policy, University of Maryland

The Cybersecurity Situation

By John Steinbruner

CISSM Working Paper

September 2011

This paper was prepared as part of the Advanced Methods of Cooperative Security Program, with generous support from the John D. and Catherine T. MacArthur Foundation.

Center for International and Security Studies at Maryland
4113 Van Munching Hall, School of Public Policy
University of Maryland
College Park, MD 20742
(301) 405-7601

UNIVERSITY OF MARYLAND

THE CYBERSECURITY SITUATION

John Steinbruner

The Obama administration has recently issued two documents outlining its intended efforts to protect the country against the many real and imagined forms of cyber attack.[1] Both documents are clearly works in progress featuring basic principles and generally worded aspirations with very little specification of plausibly effective operational policy. At the level of computer code, there is, of course, a world of intricate operational detail to which the documents refer, and that level of detail is validly considered to be too abstruse and too sensitive for public discussion. But in declaring that policy actions are required to deal with significant vulnerabilities that cannot be decisively removed, the issued documents implicitly reveal a prevailing judgment that robust protection cannot be achieved by mastery of computer code or by any other technical means. The beginning of wisdom on the subject is realization that the issues in question are essentially unprecedented and for that reason very imperfectly understood. We are in for a lengthy discussion on the topic and have to hope that enlightenment can outrun unfortunate experience, which so far it largely has.

The Basic Problem

As is well recognized, the basics of the situation arise from the spontaneous emergence of the Internet, which surely counts as one of history's more remarkable events. The Internet itself is simply a set of protocols for transferring files between addresses assigned to individual computers. The transfer occurs without examining the content of the files and without identifying the persons involved. At the time that arrangement was formulated, the network to be created was expected to involve on the order of 100,000 computers worldwide, all of them mainframes. It was not imagined that the network would grow to encompass billions of individual computers most of them substantially more capable that main frames of the early 1970s. It was not foreseen that it would become in effect a global public utility vital to the operation of most institutions and to the daily lives of a substantial portion of the human population.

The consequences of that development have been enormously beneficial but not entirely benign. The transfer protocols have enabled anonymous predators to operate with global reach and have created a constantly evolving problem of protecting legitimate services from exploitative or destructive intrusion. Up to this point the spontaneous process of defending against predators has been sufficiently effective to support progressively extensive use of the Internet. There have been occasional instances of malicious software propagating to the extent of inducing global consciousness and similarly occasional episodes of prominent denial of service attacks. There is, moreover, a constant daily barrage of limited but troublesome intrusions. Nearly everyone has experienced some irritating episode. Nonetheless, many imaginable disasters have not occurred. Power grids have not collapsed, aircraft have not been diverted, nuclear reactors have not exploded and the amount of fraud the financial system has suffered has not been sufficient to preclude the daily flow of money, stocks and commodity trade running in the trillion dollar

[1] Department of Defense Strategy for Operating in Cyberspace, July 2011: Cyberspace Policy Review,

range. It is conceivable that experience reflects inherent limits on the level of Internet predation but also possible that some catastrophe is incubating.

The fact that the possibility of catastrophe cannot be precluded with confidence gives compelling reason to consider how the underlying risks might be minimized even if they cannot be entirely eliminated. But that has to be a judiciously limited aspiration. Not every conceivable disaster can be actively prevented. If there is to be a standard of protection more reliable than what individuals, organizations and nations can provide for themselves, it would have to be based on globally accepted priorities and would not include all concerns.

It is extremely unlikely, for example, that organized global protection would extend to espionage in all its many forms. The Internet has been a bonanza for intelligence agencies, marketing organizations and all manner of busybodies. The practice of exploitation, as unauthorized access to information is commonly termed, is too widespread and too deeply entrenched to be included in any categorical restriction. Whoever exposes information to the Internet has to rely on whatever degree of protection they personally can devise or what the natural process can provide. Similarly military operations that selectively serve their own societies and threaten others would not qualify. Military organizations will have to protect their use of the Internet as best they separately can. But globally organized protection might be extended to critical functions widely acknowledged to be vital to the legitimate operations any society. Power grids, air traffic control systems, financial transaction clearing houses, emergency response teams, ship navigation and hospitals are all plausible candidates frequently mentioned.

The Case of Power Grids

Among those candidates power grids loom as the most significant test case. They are yet more vital to the functions of society than the Internet itself, which depends on power to operate, and they are in principle vulnerable to Internet predation. Power grid operations depend on computer codes which could be penetrated and maliciously altered. Doing so would require extraordinary sophistication and sustained effort subject itself to exposure, but it is technically conceivable. If one admits that it could happen, then one has to admit the possibility of lengthy power outages extending over large areas. Informed opinion at the moment does not consider absolute protection to be feasible and concedes that significant tradeoffs between exposure and operating efficiency keep the realized level of protection below its technical potential.

The consequences are necessarily speculative. It is evident that societies can adapt to intermittent power service and continue to function, even if simultaneously burdened with ongoing civil conflict. Iraq would be a prime current example. No advanced society has encountered the complete termination of power grid service lasting weeks or months, however, and there are intuitive reasons to worry about social coherence in urban industrial areas under such a circumstance. Power grid disruption offers an apparent means of inflicting massive damage, and it is prudent to assume that the opportunity to do so anonymously might be attractive to a strategic terrorist organization or to a dissident state facing an inherently superior military establishment.

The most essential feature of any arrangement for organized global protection that aspires to be effective is a legally binding, categorical prohibition of destructive cyber attacks directed against power grids. That principle would have to be accompanied by monitoring and enforcement measures, but the viability of those measures would primarily depend on the degree to which the basic principle had been established. If a categorical prohibition were to be universally accepted, monitoring and enforcement measures could be devised that would provide a much higher standard of protection than currently prevails, but the defection of any major state would critically weaken the arrangement. As practical matter that means that China, Russia and the United States would all have to be committed and assertive participants, and that unavoidable fact significantly complicates the problem.

In order to accept a categorical prohibition, the United States would have to overcome its recent aversion to any legal rule that would restrict its freedom of action and in doing so would have to absorb the implication that attacks on power grids are generally illegitimate. That implication would be resisted by advocates of coercive air power. Assaults on Iraq during the gulf war in 1991 and on Serbia during the crisis over Kosovo in 1999 featured attacks on power grids with conventional munitions. Prohibition of power grid attacks by cyber methods would not directly extend to attacks by kinetic means but would implicitly undermine their legitimacy and would therefore force judgments of the relative balance of interest. Similarly, Russia and China would have to make relative balance of interest judgments regarding their reliance on cyber attack methods to compensate for inherent disadvantages in conventional force capability as well as their concerns about exposure through the Internet to external political influence and internal dissent. Common sense suggests that the real interest in mutual protection is in principle strong enough to override those marginal implications, but political systems of all varieties have difficulty with judgments of relative interest and will predictably attempt to construct any inconvenience as a categorical objection. As a practical matter organized protection for power grids especially but for other infrastructure assets as well cannot be detached from the basic issues that determine fundamental security relationships. That is both an impediment and an opportunity.

Visualizing Opportunity

The impediments to any significant policy innovation are, of course, substantial, and in the absence of an action forcing incident too destructive to be ignored there has been as yet no serious effort to organize global protection of vulnerable infrastructure. The major protagonists – China, Russia and the United States – have suspected each other of clandestine intrusion, largely in unofficial and indirect comment, and have alluded to the preparation of retaliatory measures but have made no attempt to negotiate mutual restraint. That is a familiar story but not an excuse for general resignation. If national governments are too mired in traditional attitudes to organize constructive initiative, then the societies they are supposed to serve have reason to explore the possibilities. And to their credit the recently issued United States policy documents do encourage active public discussion, implicitly acknowledging that current and foreseeable operational practices do not assure adequate protection.

The fundamental question is the concept of interest to be applied. Legacy security policies are based on a presumption of conflicting national interest, and they at least attempt to assure that national military forces can either deter or repulse any assault on sovereign territory derived from fundamental conflicts of interest. National governments are reluctant to admit to any meaningful reliance on global legal rules for protecting their sovereign territory, but most of them are in fact compelled to do so. Very few countries are capable of repulsing the attacks that could in principle occur. The United States is the primary exception, but that exception has limited scope. Of all the countries in the world the United States is the least vulnerable to a combined arms invasion, but it shares with all others vulnerability to remote destruction by nuclear bombardment and to terrorist intrusion. Moreover, all governments are being subjected to a common threat of major proportions emerging from the process of global warming. However reluctant they may be at the moment to acknowledge that threat, it will almost certainly prove to be relentless and will predictably impose an imperative for coordinated action. The underlying reality is that traditionally separate and mutually contentious national interests are being transcended and harmonized by a globalization process, embodied in the Internet, that has created a worldwide economy which must be collectively managed if it is to be managed at all. Under that circumstance, common interests can be expected to dominate, and equity rules can be expected to become far more important than national military power. It may well take a generation or more for political attitudes to adjust, but gracefully or otherwise that will have to happen.

The immediate implication is not only that common interest in critical infrastructure protection is strong enough to justify serious efforts to develop the idea but also that there is some potential for such an effort to play a catalytic role in the ultimate reformulation of security policy generally. At the moment the United States political system does not appear capable of undertaking any meaningful initiative on any subject, but presumably or at any rate hopefully its current paralysis will not be permanent. Even if it does eventually require some specific misfortune to enable a serious initiative on critical infrastructure protection, it is important to work out a basic design based on the principle that effective protection must be global in scope and therefore equitable in order to be effective.

The ingredients of such a design are reasonably apparent. A categorical prohibition of cyber attacks on critical infrastructure assets would have to be imposed by a universally ratified treaty if it is to be strong enough to be enforced. In addition there would have to be institutionalized arrangements with global reach actively developing protocols for protection, actively monitoring illicit intrusion efforts and actively prosecuting any party who attempts to violate the prohibition. Protocols for protection would involve mandatory standards for those who operate infrastructure assets. They might be required, for example, to register their operational codes and periodically to compare the current versions of those codes to the authenticated registry. The authenticated standards would have to be guarded with rigor comparable, say, to the protection of gold reserves or nuclear explosives, but high standards of protection are feasible if they are universally imposed. The problem arises when the costs of protection are pitted against operating efficiency in an unregulated market. In addition the operations of at least some infrastructure assets, most notably power grids, would probably have to be disconnected from the general Internet to assure robust barriers to intrusion – a requirement that is feasible in principle but would require constant monitoring to accomplish in practice. Those provisions would not assure

absolute protection, but they would establish a much higher standard than currently prevails or is currently projected.

As with many things in life, however, visualizing a rational outcome is much easier than getting it accomplished, and in this case that is especially true. The three principal protagonists whose active sponsorship of a global protection arrangement is essential have not been able to establish the presumptions on which meaningful security collaboration is necessarily based. As the enduring result of legacy policies, they remain locked into deterrent confrontation that defines the basic character of their security relationships even though they are usually polite enough not to mention it. The governments cannot or at any rate will not discuss the Internet without entangling themselves in the disposition of nuclear weapons, the deployment of ballistic missile defenses, the balance of conventional forces, the regulation of space activities, the status of Taiwan and many other neuralgic issues. But their respective societies are less constrained, and as a practical matter they will have to carry the initial burden of initiative. If there is to be organized global protection of Internet functions critical to daily life, those involved in the provision of services and those engaged in the social interactions the Internet has enabled will have to respond in a serious and sustained way to the call for public discussion.

For the arms control community in particular it is important to recognize the situation as an opportunity to preempt the perverse interaction that looms as an imminent danger. The policy document issued by the United States Department of Defense emphasized the development of defensive measures, but at the press conference releasing the public version of the document the Vice Chairman of the Joint Chiefs of Staff, General James Cartwright, made it clear that he believed offensive measures will have to be prepared.[2] To the extent that China and Russia perceive the United States is actually doing that, they are virtually certain to emulate, and all three will predictably justify their effort by citing the others. That is a formula for a very destructive arms race driven by mutual suspicion as distinct from real national interest.

The situation is meaningfully reminiscent of the moment immediately after World War II when it was in principle possible to establish international control over nuclear technology. The Acheson-Lillienthal report issued in the spring of 1946 recommended the formation of an international authority to regulate the entire cycle of uranium production and use in order to prevent application to nuclear explosives and to promote nuclear power generation.[3] The idea was transformed into what came to be known as the Baruch plan featuring a veto free voting rule that was categorically unacceptable to the Soviet Union. After the initial presentation of the plan and statement of objection, neither the United States nor the Soviet Union made any effort to negotiate acceptable terms, and over the course of the ensuing two decades massive deployments of nuclear weapons occurred. We are still living with the consequence and still struggling to impose reliable restraint.

We cannot know whether a more judicious and more sustained effort to establish international control might have succeeded in preventing or at least mitigating the Cold War confrontation. We can reasonably judge in retrospect, however, that the failure to make a sustained effort was an egregious error of statesmanship. We should also acknowledge that ever since that moment

[2] Wall Street Journal July 15, 2011.
[3] http://www.learnworld.com/ZNW/LWText.Acheson-Lilienthal.html

failures of statesmanship have been far more damaging to national and international security than any deficit in the deployment of destructive firepower.

The destructive potential of cyber attack methods certainly does not appear to be comparable to that of nuclear weapons unless there is some intrusion into the command procedures for controlling nuclear weapons. Nonetheless, even if we assume that possibility can be and has been reliably excluded, the potential for social disruption by cyber attack is massive, and the practice of deterrence that we believe has so far prevented the actual use of nuclear weapons is dramatically less reliable. Since those responsible for a cyber attack cannot be reliably identified, the threat of retaliation cannot be credibly wielded. It does not appear possible to control the capacity for cyber attack in the manner that capacity for nuclear explosives could in principle have been controlled had the Acheson-Lillienthal recommendation been implemented. But meaningful global protection can be provided if the principle is established, and it is important to at least attempt to establish the principle before it is vitiated by the development of antagonistic offensive programs.

By now we should have learned that heading off a destructive process off before it occurs is vastly more effective than trying to contain it after it has occurred. Response to the call for public discussion of cyber security is an urgent matter.