Rethinking Cybersecurity – A Comprehensive Approach
Sasakawa Peace Foundation
Tokyo, September 12, 2011

Cybersecurity has become a "hot topic" in the last year. We have all come to depend on the digital networks like internet, but we have discovered that they are very insecure. Spies and criminals have been quick to take advantage of this situation. Poor cybersecurity hurts consumers, companies, and countries. It is a factor in global competitiveness, and creates the real risk of military conflict. Better security is in almost everyone's interest.

But there are many obstacles on the path to better cybersecurity. Most of these obstacles are not technical. Even if we had better technology than we have now, there would still be risk and danger from sophisticated opponents. Some of the biggest obstacles we face come from outdated analyses of cybersecurity and the policies that are based on them. It is time to rethink our approach to cybersecurity.

Early analyses thought that the cyber threat would come from terrorist attacks against critical infrastructure. They assigned responsibility for security to the private sector, since it owned most critical infrastructure, and assumed that voluntary action would be sufficient for national defense. There was an optimistic belief that the problems of the internet would be solved by a self-governing global community where government needed to play only a minimal role. These ideas are still heard today, but they have proven to be wrong. The real issues for cybersecurity turned out to be state-sponsored espionage and crime and the growth of offensive military capabilities, issues best dealt with by governments.

Cyber terrorism is not a threat at this time. Terrorists have not launched a single cyber attack. This is probably because it currently takes a large, well–resourced and time-intensive effort to use cyber tools for disruption or attack. The most advanced attacks, like the "Stuxnet" attack on Iran's nuclear program, require resources and a level of technical sophistication that terrorist groups lack. Eventually they will acquire these skills, and will then launch cyber attacks. Some of the more provocative regional actors, such as Iran or North Korea will also acquire cyber attack capabilities in the future. Both nations are working to develop these capabilities. Eventually they will succeed. It will be a much more danger world when North Korea or Iran becomes cyber powers and one important goal for cybersecurity policy is to improve our defenses before that day arrives.

Our most dangerous opponents are military and intelligence services. Some countries also recruit proxy forces – hackers and criminals they use to carry out specific tasks. The use of these private actors should not obscure the central role of governments. The greatest danger from these state actors comes from economic espionage, where foreign governments, companies and citizens steal intellectual property and confidential business information. If a nation's cybersecurity is poor, it is subsidizing its competitors. The money you spend on research ends up as a gift to others, and the long-term effect is to reduce employment, exports and income in the target nation.

Espionage against political and military targets is also a danger. One senior intelligence official described this as the "Golden Age of signals intelligence," because of weak cybersecurity. Cyber espionage provides powerful intelligence capabilities to many countries that would otherwise lack the ability to do this sort of collection, in terms of both geographic scope and in the scale of information exfiltrated. Cyber espionage can include a new avenue for political action. Instead of hiring mobs or planting false stories in newspapers, an intelligence service could use simple denial of service attacks, leaks of material obtained through hacking, or more sophisticated exploits in an attempt to manipulate politics in the target country.

There is also a growing danger from cyber crime. Cybercrime's goal is to extract money from financial institutions rather than to steal intellectual property. Cyber criminals will not intentionally disrupt networks, as they are too busy harvesting money from them, but there is some risk that a cybercriminal could, while committing a crime, inadvertently damage the stability of financial markets. Cybercriminals fill an important role as proxy forces, providing countries that tolerate them a degree of deniability for espionage and political action.

Cyberwar is also a risk, but it is overstated. Advanced militaries have plans and capabilities to attack opposing military forces, critical infrastructure, and other civilian targets. We can regard cyber attack can be regarded as a new attack capability that has both tactical and strategic uses, similar to missiles or aircraft that can be launched from a distance and strike rapidly at a target. But a pure cyberwar, using only cyber attacks is unlikely. The initial analyses of cybersecurity exaggerated the effect of a cyber attack. It is possible to do physical damage by introducing malicious software into the computers or devices that control critical infrastructures, but this will not be the equivalent of a bomb. A cyber attack will not be a decisive weapon. This means that no nation will launch a cyber attack or engage in a pure cyber war, because a cyber attack by itself is more likely to annoy an opponent than to defeat it. We are likely to see cyber attack only in the context of some larger military conflict.

To date, there have been at best only three or four real cyber "attacks." Stuxnet was an attack, a short blackout in a Brazilian city was caused by a cyber attack –probably an extortion attempt that went wrong - and the Israelis may have used the cyber techniques in their raid on the alleged Syrian nuclear facility. Everything thing else is crime, espionage or a prank. The United Nations Charter, and The Hague and Geneva Conventions make clear that an attack involves physical destruction and casualties. The 2007 cyber incident in Estonia, although clearly intended to coerce the Estonian government was not an attack, although it did raise important questions about the future of conflict. If what happened to Estonia lasted longer and blocked key services for an extended period, might qualify as an "attack." Similarly, a massive erasure of data might be judged as equivalent to physical damage. These are areas of ambiguity that it would be useful to clarify, but calling everything an attack is only confuses the matter. Espionage and state-sponsored crime do not qualify as attacks and do not justify the use of military force in response. This means that while we can expect to successfully deter military attacks, we cannot expect our armed forces to prevent espionage or crime.

Misconceptions cloud our thinking and our policies. Cyberspace is not a commons. Cyberspace is an artificial construct, a term we use as an easy way to describe the collection of networks and devices that connect computers. Some owns all these networks and devices and all are subject to

the control of some national government. This is not a commons. A better way to think of the internet is as a condominium, where many owners share a common structure, but this condominium has few rules and a weak governing board.

One of the most significant changes in cybersecurity in recent years is the rejection of the "commons" notion and the extension of sovereign state control into cyberspace. The pioneers of the internet said it was borderless. This reflects a view commonly held in the 1990s that borders were disappearing and that sovereign states, which had been the main international actors since the treaty of Westphalia, were in decline. It turns out this was not true. Cyberspace has borders and nations are beginning to ask how they apply their laws within these borders. Governments want to extend their authorities into cyberspace and are building technologies that will let them do this. Some governments even argue that cyberspace is like their territorial seas, accessible from outside but subject to their control. The extension of sovereignty will affect the architecture of the internet, its rules and governance, and most importantly, the values that shape cyberspace.

You often hear that the private sector owns eighty or ninety percent of the critical infrastructure and that they should therefore lead in its defense. This is meaningless. The private sector owns most of the airplanes, but no one says it should be responsible for air defense. National security, law enforcement and public safety are government responsibilities. Cybersecurity is no different. The market will fail to adequately supply these public goods. A similar misconception is the claim that private sector is better at cyber defense than the government. Most people who say this are ignorant of the true capabilities of advanced militaries and intelligence agencies. It is like saying that a company softball team can regularly beat the Yomiuri Giants – in fact, it is no contest. There are five or six nations in the world with advanced cyber capabilities for penetration, espionage and attack, and other nations intend to acquire them. No private actor can match these capabilities.

We hear that technology changes too fast for governments to keep up. This is an exaggeration. There have been four major changes in the last fifty years of computing and networks; the development of huge, expensive "main frame" computers; the appearance of small mini-computers or personal computers; the networking of these small computers using the internet protocol; and now the transition to computing as a service, to what some call the "cloud," where mobile devices like the iPad or a smart phone will be the primary means for connecting to networks. A change every decade is not a blinding rate of speed that is impossible to manage.

Many say that attribution is a problem, that we cannot tell the source or identity of an attacker. This too is incorrect. It is better to ask for who is attribution a problem. Companies sometimes think that only forensic analysis, looking that the code an attacker leaves behind or at the path and attack took to gain entry is the only source of information. A senior American intelligence official recently told me that attribution is not a problem because he can use espionage techniques to identify the attacker. Attribution is hard, but is it not impossible and it is getting easier. We can also make judgments based on the aggregation of attacks. Blaming a country for a single attack when we have limited evidence is risky. When there are many incidents and when these incidents track with a country's larger economic strategy and intelligence activities, we do not need to hesitate.

We are sometimes told that cybersecurity is risky as greater security may damage the potential of the internet for innovation. This is just bad economics. Rules for air travel were introduced in 1948, but this did not stop airlines and aircraft manufacturers for innovation. The U.S. created safety rules for cars in the 1950s but we are not still driving big cars with fins. If the goal is to maintain innovation, it is more important to preserve equal access to networks and protection of intellectual property than to block cybersecurity. The appeals to protect innovation are rhetorical device, not a serious economic argument or a good guide for policy.

Perhaps this collection of ideas made sense in the early days of the internet, when it was a toy rather than a pillar of economic activity, but it is no longer adequate as a guide to policy. Replacing the clutter of the old ideas with three concepts drawn from our experience of the last ten years makes the tasks for cybersecurity become clearer: the immediate problems are crime, economic espionage, and the risk of offensive military action; the primary malicious actors in cyberspace are national governments, some of whom sponsor hackers and cybercriminals as a proxies, irregular forces they can use for intelligence or military advantage; cybersecurity is a national security and law enforcement problem where primary responsibility falls upon governments.

Redefining cybersecurity in these terms will help us identify a more effective strategy. This strategy has five key elements that address the most important cybersecurity problems: ISP responsibility for consumers, breach notification, regulation of critical infrastructure, active defense, and international cooperation. These can provide a strategic defense in depth that addresses the most pressing problems.

The first is to make internet service providers (ISPs) responsible for protecting consumers and small businesses, who will never be able to protect themselves. ISPs usually know when their customers are infected with malicious software (malware), but they take no action to remove it. This should change. When an ISP sees that a customer's computer is infected, it should notify the customer and offer to clean it. Alternatively, the ISP could notify customers of infection and then direct them to a website were they could get help. Partnerships between the ISPs and the government can increase the effectiveness if they can pool information on threats, malware and response techniques.

There is a fear that this approach will increase ISP costs, but it is more likely that ISPs will end up saving money. There is also a concern that the ISPs will incur additional liability. This concern is legitimate, and ISPs will need to either change the terms of service in their contracts with customers or get legislative protection against liability. As we move to cloud computing, where computing is a service, a utility and people connect to the internet with simple devices rather than through cumbersome desktop computers, making the ISPs bear the responsibility for security will become crucial.

Several countries have already tried variants of this approach with considerable success. Germany, Australia and Turkey have all, using different techniques, made the ISP's bear responsibility for customer security. The results have been a startling decrease in the number of

botnets – consumer computer captures by cyber criminals. This is a successful technique that provides a foundation for defense against low-end threat.

Making the ISP's responsible for customer security is a basic step that must be reinforced by additional measures. The first of these additional steps is to incentivize "enterprise" level defense by critical infrastructure companies. Critical infrastructure companies must bear responsibility for digital security, particular for securing industrial control systems that control crucial machinery. These control systems were the target of the Stuxnet worm, and the "Aurora" tests at the Idaho National Labs confirmed that hackers can use the internet to access controls systems and instruct these systems to destroy themselves. When you ask many critical infrastructure companies if their control systems are connected to the internet, most will tell you that they are not. If you then test their assertion, you will find connections that they do not know about. Hackers can find these connections and use them for attacks. Critical infrastructure is vulnerable to cyber attack and only the operator can ensure that control systems are secure. They and must be required to take the necessary steps for security.

Companies never have any desire for more regulation. This is understandable, but it is also unacceptable for national security and public safety. Companies will not provide adequate cybersecurity on a voluntary basis. There are several reasons for this. A company may not know of the vulnerability, it may underestimate the threat, and it may have no desire to spend more money on something that will not generate a return on investment. Government oversight is required. This oversight requires the development of standards for cybersecurity. Some people will tell you that it is impossible to develop such standards, that technology changes too fast or that we do not know enough. These arguments are inane. There are now standards and practices that, if they are but into practice, significantly reduce the risk of cyber attack. Government can base a regulatory approach to critical infrastructure on these standards and practices. There must be decisions about which infrastructure require regulation and how regulation should be implemented, but any nation that does not put this kind of safeguards in place will ultimately be vulnerable to cyber attack.

Protecting consumers and hardening critical infrastructure do not address all cybersecurity problems. The biggest single problem is the loss of intellectual property and business information due to cyber spying. It is hard to estimate the cost of the damage but it is likely to be in the billions of dollars. Industrial espionage of this kind is not new, but the internet has dramatically increased its scale and, by lowering the costs, made it easier for many more people do to illicitly access and acquire confidential business information. The Internet makes it possible to steal thousand of pages of blueprints, plans or manuals in a single night.

The problem is challenging, but one solution is to require companies to report when they have been hacked, as some nations now require notification when personal data of a company's customer is lost. When Google was hacked in 2010, another thirty-five companies also lost valuable information, but most did not report it. Sometimes, companies do not even know when they have been hacked. Most conceal it out of fear of reputational damage or losing investor confidence. Thresholds for notification would have to be developed (we don't need to know every incident, only those that cause damage) and "safe harbor" for liability would need to be created, but requiring publicly traded companies to report major cyber losses could create an

incentive in these companies to spend on better security. At a minimum, it would force companies and governments to confront the problem of economic espionage. The result would be beneficial for both national security and economic competitiveness.

These three measures could be reinforced by "active defense." Active defense offers a strategic, national-level approach to cybersecurity. It can be compared with air or missile defense. In air defense, the military monitors a nation's airspace and intercepts hostile aircraft before they can reach their target or do damage. In active defense, a government agency would work with the Tier One telecommunication service providers and the major ISPs to monitor the internet backbone – the high capacity fiber optic systems that are the physical foundation of the global network - to identify and intercept malicious incoming traffic. Most Tier One service providers already monitor the traffic that flows over their networks, but they do not always take action against malicious activity.

Almost internet traffic, and all international traffic, is passed among Tier One service providers. They connect at "peering points" on the internet backbone. The peering points that connect a country to the rest of the world, where traffic is aggregated, are the logical places to interdict malicious traffic. Defending these chokepoints requires placing "sensors" on the peering points. There are several ways to identify malicious activity. Behavioral analysis that looks for anomalous activity or unusual traffic patterns is a good indicator. Service providers and cybersecurity companies use signatures, essentially a pattern of binary code (machine readable code takes the form of ones and zeros) that has been identified as malicious. The information they already have can be improved by adding classified information from government intelligence sources. This combination of commercial and government information will provide a comprehensive view of the state of cybersecurity.

Once packets have been identified as malware, defensive actions can be taken. They can be removed from the stream of traffic and so never reach their intended target. Active defense systems can divert the packets to a holding area for isolation and further study. They can be opened and rewritten and then sent on their way, to make malware self-destruct, to identify infected machines, or take other actions aimed at the attacker. Active defense on the networks of the primary service providers offers the possibility of interception most incoming malicious traffic before it reaches its target.

Active defense raise major privacy concerns. Sensors on backbone networks will monitor huge volumes of traffic. While these sensors can be programmed only to look for malware, and not to intercept and read private messages, there is a fundamental question of trust as to whether governments will resist the temptation to go beyond cybersecurity and collect information as well. Any data collected and stored must be carefully controlled and its use limited to cybersecurity. There must be adequate oversight rules and mechanisms to ensure that privacy and legal requirements for communications monitoring are being respected. In the United States, there are also issues over which agency should be responsible for active defense that revolve around defining the role of the military in cybersecurity.

These measures – greater responsibility for ISPs, regulation of critical infrastructures, and active defense – are things that nations can do by themselves and they would significantly reduce risk.

But there would still be major challenges in cybersecurity. The most advanced opponents live in other countries. They are foreign military and intelligence agencies, or cybercriminals who act as their proxies. These people have the skills and the resources to mount campaigns that will challenge any defense. For this reason, the final element of a comprehensive approach to cybersecurity is building international cooperation to make cyberspace more stable and secure.

The pioneers of cyberspace hoped it could be self-governing with many stakeholders from civil society directing its course. This approach has worked well for engineering and technology, but it has produced chaos for public safety and security. Whether it is the Wild West or a Hobbesian society, cyberspace must become more secure if we are to reap the full benefit of digital networks. This will require extending into cyberspace the agreements, norms and rules we now have for international conduct in other areas, including trade agreements, the laws of armed conflict, and law enforcement cooperation, and identifying those areas were new agreements are needed. In this, governments must to play a leading role.

Cybersecurity is a difficult issue for negotiation, as it requires many nations with different values and interests to cooperate. The international processes we have now for cooperation in cybersecurity are very weak. A revitalized international discussion needs to focus on four issues. The first is the application of trade rules into cyberspace, particularly World Trade Organization commitments on the protection of intellectual property. Some trade analysts argue that the evidence of malfeasance is not precise enough to bring specific cases before the WTO. This is a fundamental misunderstanding of international relations, which are not confined to lawyerly processes and rules of evidence. Noncompliance with commitments to protect intellectual property creates extraordinary circumstances that provide the U.S. and other industrial nations the justification for strong action. Even the threat of strong action will affect and constrain malicious activity by other nations.

The second is to expand law enforcement cooperation. Currently most cybercrime is the result of action by hackers who live in sanctuary countries, countries that tolerate or even encourage cybercrime. We need international agreement on the norms of responsible behavior in cyberspace, including how the laws of armed conflict are applied and how states are responsible for the action of those resident on their territory – no more it was just a patriotic hacker excuse. Finally, we need consequence for bad behavior in cyberspace, whether this is trade penalties, WTO cases, expulsion of diplomats and other traditional responses to espionage, or special restrictions on internet traffic from countries of concern. If there are no consequences for bad behavior, there is no incentive for national to change their policies.

Changing our thinking about cybersecurity will not be easy. It will require taking a step back and looking at the internet as it really is, and not as it has been portrayed. But if we can make this change, the policies that will make us safer become clearer. Cybersecurity is a difficult task that will become more important as we grow more dependent on computer networks, but it is not an impossible task. A comprehensive approach to cybersecurity that combines greater responsibility for ISPs, breach notifications, regulation of critical infrastructure, active defense, and international cooperation can make us safer and let us take advantage of the new technologies in ways we have yet to imagine.