ONLINE
DOKUMENTATION

Konrad-Adenauer-Stiftung e.V.

MICHAL MACHNOSWSKI

Juni 2010

www.kas.de
www.kasusa.org

Cyber War – The Next Threat to National Security And What to Do About It

In „Cyber War“ Richard Clarke (and co-author Robert Knake) describe in chilling detail how the U.S. is currently far more vulnerable to cyber war than Russia or China, and that the U.S. is more at risk from a cyber attack than are minor states, like North Korea. The U.S. may even be at risk some day from nations or non-state actors lacking cyber war capabilities, but who can hire teams of highly capable hackers.

Like the days preceding 9/11, there is currently a lack of coordination between the various arms of the military and various committees in Congress over how to handle a potential attack, and government agencies and private companies in charge of civilian infrastructure are ill prepared to handle a possible disaster.

The biggest secret in the world about cyber war may be that at the very same time the U.S. prepares for offensive cyber war, it is continuing policies that make it impossible to defend the nation effectively from a cyber attack. It will be the public, the civilian population of the U.S. and the publicly owned corporations that run the key national systems that are likely to suffer in a cyber war.

What is a Cyber War?

First, cyber war is real. What has been seen so far is far from indicative of what can be done. Most of the well-known skirmishes in cyberspace used only primitive weapons. It is reasonable to guess that the attackers did not want to reveal their sophisticated capabilities, yet. What the U.S. and other nations are capable of doing in a cyber war could devastate a modern nation.

Second, cyber war happens at the speed of light. As the photons of the attack packets stream down fiber optic cables, the time between the launch of an attack and its effect is barely measurable, thus creating risks for crisis decision makers.

Third, cyber war is global. In any conflict, cyber attacks rapidly go global, as covertly acquired or hacked computers and servers throughout the world are kicked into service, and many nations are drawn in the attack or war.

Fourth, cyber war skips the battlefield. Systems that people rely on, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country’s traditional defenses.

Finally, cyber war has already begun. In anticipation of hostilities, nations are already preparing the battlefield. They are hacking into each other's networks and infrastructures, laying in trapdoor and logic bombs—now, during peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability.

Based on these five key assumptions, there is every reason to believe that most future conventional wars will be accompanied by cyber war, and that other cyber wars will be conducted as "stand-alone" activities, without explosions, infantry, airpower, and navies. There has not been, yet, a full-scale cyber war in which the leading nations in this kind of combat employ their most sophisticated weapons against each other. Thus, there is no concrete data on who would win, nor what the results of such a cyber war would be.

U.S. Cyber Command

In June of 2009, the new U.S. Cyber Command was announced and proposed to be fully operational by October, 2010. The U.S. Cyber Command is a military organization with the mission to coordinate computer-network defense and direct U.S. cyber-attack operations. This came in response to repeated reports of attacks on U.S. Defense networks, including a breach of the U.S. electrical grid and of the F-35 fighter jet program.

Three star Lt. Gen. Keith Alexander, the nominated commander of U.S. Cyber Command, outlined his views in a report for the United States House Committee on Armed Services subcommittee in May: "My own view is that the only way to counteract both criminal and espionage activity online is to be proactive. If the U.S. is taking a formal approach to this, then that has to be a good thing. The Chinese are viewed as the source of a great many attacks on western infrastructure and just recently, the U.S. electrical grid. If that is determined to be an organized attack, I would want to go and take down the source of those attacks. The only problem is that the Internet, by its very nature, has no borders and if the U.S. takes on the mantle of the world's police; that might not go down well."

Cyber Command's mission is to defend Department of Defense (DoD) and several other government agencies, but there are no plans or capabilities for it to defend the civilian infrastructure. Both former National Security Agency Directors (John McConnell and Kenneth Minihan) believe that mission should be handled by the Department of Homeland Security (DHS), as in the existing plans; but both men contend that Homeland has no current ability to defend the corporate cyberspace that makes most of the country function. Neither does the Pentagon. In fact, there is no federal agency that has the mission of to defend the banking system, the transportation networks, or the power grid from cyber attack. Cyber Command and DHS state that by defending their government customers they may coincidentally help the private sector. The government's policy is that it is the responsibility of individual corporations to defend themselves from cyber war. However, CEOs agree that it is up to the company to spend enough on computer security to protect against the day-to-day threat of cyber crime, with many stating that "defending against other nations' militaries is the government's job, it's what we pay taxes for."

Preparing the Battlefield

These military and intelligence organizations are preparing the cyber battlefield with weapons called "trapdoors" and "logic bombs," placing virtual explosive within other countries in peacetime.

Trapdoors are unauthorized software maliciously added to a program to allow unauthorized entry into a network or into the software program. Often after an initial entry into a program or computer system, a cyber criminal or cyber warrior leaves behind a trapdoor to permit future access to be faster and easier. It is believed that North Korea is behind the cyber attacks of July 2009 that took down the Web servers of the Treasury, Secret Service, Federal Trade Commission and the Transportation Department, and is thought to have placed trapdoors on computer networks on at least two continents (surprisingly, these attacks are thought to have originated in China, as North Korea does not have the Internet connectivity to launch sophisticated cyber attacks from its own territory).

A logic bomb, on the other hand, is a software application or a series of instructions that cause a system or network to shut down and/or to erase all data or software on the network. According to Defense Secretary Robert Gates, cyber attacks "could threaten the United States' primary means to projects its power and help its allies in the Pacific." Mr. Clarke wonders if this would be enough to deter the U.S. from a confrontation with China, if the possibility of China crippling U.S. force projection capability is not enough to deter the U.S., maybe the realization of the U.S. domestic vulnerabilities to cyber attack would be. The alleged emplacement of logic bombs in the U.S. electrical grid may have been done in such a way that the U.S. government would notice. One former government official told Mr. Clarke that he suspects the Chinese wanted the U.S. to know that if the U.S. intervened in a Chinese conflict with Taiwan (under the security guarantee that the U.S. has with Taiwan), the U.S. power grid would likely collapse. "They (China) want to deter the U.S. from getting involved militarily within their sphere of influence. The problem is that deterrence only works if the other side is listening. U.S. leaders may not have heard or fully understood what Beijing was trying to say. The U.S. has done little or nothing to fix vulnerabilities in its power grid or in other civilian networks."

According to Mr. Clarke, there are two main uses of cyber war. One use of cyber war is to make a conventional (kinetic) attack easier by disabling the enemy's defenses. Another use of cyber war is to send propaganda out to demoralize the enemy, distributing emails and other Internet media in place of the former practice of dropping pamphlets.

There have been several cyber war clashes recently by the Russians on Estonia and Georgia, by the Israelis on Syria, and by the North Koreans on South Korea.

Consensus

At a 2009 Las Vegas conference attended by former government officials, current bureaucrats, chief security officers in major corporations, academics, and senior IT company officials, the conference organizer, Jeff Moss put a question in the air: What do we want the new Obama Administration to do to secure cyberspace? Since Moss was placed on the Homeland Security Advisory Board, there was some chance that his reporting of the group's consensus views would be heard.

The group reached a general accord on a few points. The first was that the group advocated for the federal government to ramp up spending on cyber security research and development. The Defense Advanced Research Projects Agency, in charge of funding, had essentially abandoned the Internet security field during the presidency of George W. Bush, instead focusing attention on "netcentric warfare," apparently oblivious, wrote Mr. Clarke, that such combat depended upon cyberspace being secure.

The next point was that there was a need for “smart regulation” of some aspects of cyber security, like proposing federal guidelines for Internet backbone carriers. Backbone carriers are the large, national network of fiber-optic cables on which Internet and other cyberspace traffic runs to the major cities, operated by the five major Internet service providers (known as Tier 1’s) in the U.S. (AT&T, Verizon, Level 3, Qwest and Sprint).

Another consensus observation was that there really should be no connectivity between utility networks and the Internet. The idea of separating “critical infrastructure” from the open-to-anyone Internet seems as a no-brainer. But the Obama Administration seems to be heading in the opposite direction concerning Smart Grid, with the 2009 stimulus bill allocating $4.5 billion for the high-tech program. Smart Grid refers to the transition from the current, outdated power-grid infrastructure to a more technologically advanced structure that allows expanded real-time monitoring and energy delivery that’s more efficient and cost effective for utilities and consumers. The technology promises to solve a number of problems, but it also could introduce new problems, such as increasing the vulnerability to cyber attack as power grid resources become increasingly linked to the internet. China, on the other hand, has the ability to disconnect all Chinese networks from the rest of the global Internet, something that would be an asset if it believed that the U.S was going to launch a cyber attack on, let’s say, their power grid. In essence, China can go “manual”.

While the U.S. very likely possesses the most sophisticated offensive cyber war capabilities, that offensive prowess cannot make up for the weakness in our defensive position. As former Admiral McConnell has noted, “Because we are the most developed technologically, we have the most bandwidth running through our society and are more dependent on that bandwidth, we are the most vulnerable. We have connected more of our infrastructure and economy to the Internet than any other nation.”

However, Mr. Clarke acknowledges that protecting every computer in the U.S. from some form of cyber attack is hopeless, but it still may be possible to sufficiently harden the important networks that a nation-state attacker would target, enough that no attack could disable the U.S. military or undermine the economy. Even if the defense is not perfect, these hardened networks may be able to survive sufficiently, so that the damage done by an attack would not be crippling. Therefore, there are three major components to U.S. cyberspace that must be defended.

The Defensive Triad Strategy

Mr. Clarke’s proposed Defensive Triad Strategy would be a departure from what President Clinton, Bush and Obama have done. President Clinton and Bush both sought to have every critical infrastructure defend itself from cyber attack. There were eventually eighteen industries identified as critical infrastructures, ranging from electric power and banking to food and retail. All three presidents eschewed regulation as a means of reducing cyber vulnerabilities, with little or no outcome. President Bush approved an approach to cyber war that largely ignored the privately owned and operated infrastructures. It focused on defending government systems and on creating a military Cyber Command. President Obama is implementing the Bush plan, including the military command, with little or no modification to date.

Mr. Clarke’s proposed Defensive Triad Strategy would use federal regulation as a major tool to create cyber security requirements, and it would, at least initially, focus defensive efforts on only three sectors.

The first sector would be the backbone and the protection of the Tier 1's. Over 90 percent of Internet traffic in the U.S. moves on these Tier 1's, and it is usually impossible to get to anyplace on the U.S. without traversing one of these backbone providers. The idea is that if you protect the Tier 1's, you are protecting most of the Internet infrastructure in the U.S. and also other parts of cyberspace. To attack most private-sector and government networks, you generally have to connect to them over the Internet and specifically, at some point, over the backbone. If you could catch the attack entering the backbone, you could stop it before it got to the network it was going to attack. In other words, if you knew that someone was going to drive a truck bomb from New Jersey into a building in Manhattan, you could defend every important building in Manhattan, or you could inspect all trucks before they went on one of the fourteen bridges or four tunnels that go to Manhattan.

The second prong of a Defense Triad is a secure power grid. The easiest thing a nation-state cyber attacker could do today to have a major economic impact on the U.S. would be to shut down sections of the Eastern and Western Interconnects, the two big grids that cover the U.S. and Canada. These two power-sharing systems could be secured, but not without additional federal regulation. That regulation would be focused on disconnecting the control network for the power generation and distribution companies from the Internet and then making access to those networks require authentication. But the power companies have a different view. When asked what assets of theirs were critical and should be covered by cyber security regulations, the industry replied that 95 percent of their assets should be left unregulated with regard to cyber security. A security expert who works with the major cyber security firms had asked each audit firm that had worked with power companies if they had been able in their audits to get to the power grid controls from the Internet. All six firms acknowledged getting access to the controls, and all got in under less than an hour. In response, the Federal Energy Regulatory Commission promised that 2010 will be the year that it will start penalizing power companies that do not have secure cyber systems.

In order to make the power grid more secure, the government would have to issue and enforce serious regulations to require electric companies to make it next to impossible to obtain unauthorized access to the control network for the grid. That would require no pathways at all from the Internet to the control systems. In 2009, the current head of U.S. Cyber Command, General Keith Alexander, said "So the power companies are going to have to go out and change the configuration of their networks…to upgrade their networks to make sure they are secure is a jump in cost for them…and you're going to have to work through their regulatory committees to get the rate increases so that they can actually secure their networks. How does government, because we're interested in perhaps having reliable power, how do we ensure that that happens as a critical infrastructure?" In other words, General Alexander was stating that power companies need to reconfigure so that the U.S. can have secure, reliable electricity, that this may require extra spending, and that the regulatory organizations will have to help make that happen.

The third prong of the Defense Triad is Defense itself, as in the Department of Defense (DoD). If an opponent were going to hit the U.S. with a large cyber attack, they would have to assume that we might respond kinetically. Therefore, a cyber attack on the U.S. military would likely concentrate on DoD's networks. While nation-state actors might try to cripple the private-sector systems like the power grid, pipelines, transportation, or banking, it's hard to imagine such actions coming as a bolt from the blue. However, even if DoD secures all of its networks, there is still the risk that the DoD software and hardware it uses to run its weapons systems may be compromised.

Joel Brenner, head of the U.S. Office of the National Counterintelligence Executive, said that officials have seen counterfeit hardware (computer chips) make their way into U.S. military fighter aircraft. “You don’t sneak counterfeit chips into another nation’s aircraft to steal data (referring to a report that plans for the F-35 Joint Strike Fighter where infiltrated by hackers). When it’s done intentionally, it’s done to degrade systems, or to have the ability to do so at a time of one’s choosing.”

The computer chips U.S. weapons use as well as some of the computers or their components are made in other countries. DoD’s most ubiquitous operating system is Microsoft Windows, which is developed around the world on development networks that have proven vulnerable to hackers in the past. This supply-chain concern is not easily or quickly solved. It is one of the areas that the 2008 Bush plan focused on. New chip factories are being built in the U.S. Some private sector companies are developing software to check other software for bugs. In addition to adding quickly to the security of its networks, one of the most important things the Pentagon could do would be to develop a rigorous standards, inspection and research program to ensure that the software and hardware being used in key weapons systems, in command control, and in logistics are not laced with trapdoors or logic bombs.

In summary, Mr. Clarke’s Defensive Triad rests on the need to harden the Internet backbone, separate and secure the controls to the power grid, and vigorously pursue security upgrades for Defense IT systems. Only then, according to Mr. Clarke, can the U.S. cast doubt in the minds of potential nation-state attackers about how well they would do in launching a large-scale attack against the U.S. Even, if an attack did occur, Mr. Clarke believes that the Defense Triad would mitigate the effects.

Use and Limitations

Coupled with a defense strategy, in order to reduce the risk of initiating a cyber attack, there should be a treaty in place limiting the use and scope of a cyber attack, similar to the Strategic Arms Limitation Treaty for nuclear weapons. A proposed Cyber War Limitations Treaty would seek to limit cyber war, not seek a ban on intelligence gathering. The treaty should establish a Cyber Risk Reduction Center to exchange information and provide nations with assistance; create as international-law concepts the obligation to assist and national cyber accountability (a country hosting a cyber attack is just as guilty as the country that is doing the attacking); impose a ban on first-use cyber attacks against civilian infrastructure, a ban that would be lifted when (a) the two nations were in a shooting war, or (b) the defending nation had been attacked by the other nation with cyber weapons; prohibit the preparation of the electronic battlefield in peacetime by the emplacement of trapdoors or logic bombs on civilian infrastructure, including electric power grids, railroads, and so on; and to prohibit altering data or damaging networks of financial institutions at any time, including the preparation to do so by the emplacement of logic bombs.

Role of the President

In his conclusion, Mr. Clarke points out that the President must be required to approve personally the emplacement of logic bombs in other nations’ networks, as well as approve the creation of trapdoors on a class of politically sensitive targets. Because logic bombs are a demonstration of hostile intent, the President alone should be the one who decides that he or she wants to run the destabilizing risks associated with their placement. The President should be the one to judge the likelihood of the U.S. being in armed conflict with another nation in the foreseeable future, and only if that possibility is high should he or she authorize

logic bombs. Key congressional leaders should be informed of such presidential decisions, just as they are for other covert actions.

On an annual basis, the President should review the status of all major cyber espionage, cyber war preparation of the battlefield, and cyber defense programs. An annual cyber defense report to the President should spell out the progress made on defending the backbone, securing the DoD networks, and securing the electric power grid.

Part of the annual check-up should be a review of the progress of U.S. Cyber Command; what networks have been penetrated; what operation would be available to the President in a crisis, and whether there are any modifications needed to the President's earlier guidance. This review would be similar to the annual covert-action review and the periodic description of the nuclear war plan with the President.

Finally, the President should put reducing Chinese cyber espionage at the top of the diplomatic agenda, and make clear that such behavior amounts to a form of economic warfare. Within this context, the President should state that a cyber attack on the U.S. will be treated as the same as if it were a kinetic attack and that the U.S. will respond in the manner it thinks best, based upon the nature and extent of the provocation. By proposing a global system of National cyber Accountability, the President would seek to impose on nations the responsibility of dealing with cyber criminals and allegedly spontaneous civilian hacktavists, and an Obligation to Assist in stopping and investigating cyber attacks.

Cyber Weapons are not simply the next stage in the evolution of making war less lethal. If they are not properly controlled, they may result in small disagreements spiraling out of control and leading to wider war, or to the orchestrated collapse of world's fundamental economic and governmental systems. The end-game for Mr. Clarke is when the world can take a step back from the edge of what could be a new battlespace, and take steps not to fight in cyberspace, but to fight against cyber war.

Richard A. Clarke and Robert K. Knake: Cyber War - The Next Threat to National Security And What to Do About It, New York 2010.