Пише: Richard Clarke
четвртак, 24 децембар 2009 12:54

(The National Interest, 22.12. 2009)

ON OCTOBER 1, just beyond the Beltway inside Fort Meade, a four-star general became the first head of America's new Cyber Command. Subordinate to General Keith Alexander are the Tenth Fleet and the Twenty-Fourth Air Force. The fleet has no ships, and the air-force unit has neither aircraft nor missiles. Their weapons are ones and zeroes. Their battlefield is cyberspace.

The mission of Cyber Command is to protect the U.S. military's networks and to be ready to launch offensive cyber attacks on a potential enemy. Those offensive cyber attacks have the potential to reach out from cyberspace into the physical dimension, causing giant electrical generators to shred themselves, trains to derail, high-tension power-transmission lines to burn, gas pipelines to explode, aircraft to crash, weapons to malfunction, funds to disappear and enemy units to walk into ambushes. Welcome to warfare in the twenty-first century.

We have become accustomed to the pilots of Predator and Reaper drones driving a few miles to their homes in Virginia and dinner with their kids after having "flown" aircraft all day on the other side of the globe, firing deadly Hellfire missiles into houses of terrorists in Pakistan. That looks like war as PlayStation: death by joystick, no risk of being shot down, no chance of capture. Now, with cyber war, we have another means of launching attacks on the other side of the world, this time with only a keyboard. In Vietnam and Iraq, U.S. pilots were shot down while attempting to bomb enemy air-defense missiles. Now, a cyber warrior might simply shut off an air-defense network or cause missiles to explode on their launch rails, not by using a laser-guided missile, but by activating a logic bomb. Cyber war could well mean fewer casualties, less physical destruction. Surely then, it is a good idea.

PERHAPS NOT. Much like sixty years ago when we first began to deal with strategic nuclear weapons, we have neither outlined a clear strategy nor had an open debate about how best to deal with this new capability and this new threat. As former–Secretary of Defense Robert McNamara discovered, without a real strategy for the use of strategic nuclear weapons, we risked annihilation of both ourselves and our enemies. The Strategic Air Command (SAC) had a simple plan: the United States would perceive when the Soviet Union was getting ready to attack us and then SAC would go first, launching all of its weapons against all of its possible targets in the Soviet Union, China and the Warsaw Pact nations of Eastern Europe. Horrified by

that idea, McNamara commissioned work that developed a strategy of deterrence, including withholding attacks on cities, controlling escalation, minimizing crisis instability and initiating nuclear-arms control. Much of the development of that strategy was done in public, in speeches by then-President John F. Kennedy and McNamara, and in books by academics such as Herman Kahn, founder of the Hudson Institute, and MIT professor William Kaufmann. This is exactly the kind of discussion we need to have today. For it is not an overstatement to say that the body of work on atomic strategy initiated in the Kennedy administration probably prevented a nuclear war in which hundreds of millions may have died.

We sit at a similar historical moment. War fighting is forever changed. Though it will never produce the kind of death toll of nuclear weapons, we can see echoes of these same risks and challenges in today's newest cyber-war battlefield. We've developed a plethora of gee-whiz technological capabilities in the past few years, but cyber war is a wholly new form of combat, the implications of which we do not yet fully understand. Its inherent nature rewards countries that act swiftly and encourages escalation.

AS IN the 1960s, the speed of war is rapidly accelerating. Then, long-range missiles could launch from the prairie of Wyoming and hit Moscow in only thirty-five minutes. Strikes in cyber war move at a rate approaching the speed of light. And this speed favors a strategy of preemption, which means the chances that people can become trigger-happy are high. This, in turn, makes cyber war all the more likely. If a cyber-war commander does not attack quickly, his network may be destroyed first. If a commander does not preempt an enemy, he may find that the target nation has suddenly raised new defenses or even disconnected from the worldwide Internet. There seems to be a premium in cyber war to making the first move.

And much as in the nuclear era, there is a real risk of escalation with cyber war. Nuclear war was generally believed to be something that might quickly grow out of conventional combat, perhaps initiated with tanks firing at each other in a divided Berlin. The speed of new technologies created enormous risks for crisis instability and miscalculation. Today, the risks of miscalculation are even higher, enhancing the chances that what begins as a battle of computer programs ends in a shooting war. Cyber war, with its low risks to the cyber warriors, may be seen by a decision maker as a way of sending a signal, making a point without actually shooting. An attacker would likely think of a cyber offensive that knocked out an electric-power grid and even destroyed some of the grid's key components (keeping the system down for weeks), as a somewhat antiseptic move; a way to keep tensions as low as possible. But for the millions of people thrown into the dark and perhaps the cold, unable to get food, without access to cash and dealing with social disorder, it would be in many ways the same as if bombs had been dropped on their cities. Thus, the nation attacked might well respond with "kinetic activity."

Responding, however, assumes that you know who attacked you. And, one of the major differences between cyber war and conventional war—one that makes the battlefield more perilous—is what cyber warriors call “the attribution problem.” Put more simply, it is a matter of whodunit. In cyberspace, attackers can hide their identity, cover their tracks. Worse, they may be able to mislead, placing blame on others by spoofing the source.

In 2007, the Russian government denied that it had engaged in primitive cyber war against Estonia that took out such things as the financial-services sector, and in 2009 claimed it was not responsible for largely identical activity against Georgia; though Russia did concede that some of its citizens, outraged over the conflict in Abkhazia, might have launched the denial-of-service attacks.

In July of this year, cyber attacks were launched against commercial and government websites in the United States and South Korea. The targets included the White House and Washington Post homepages. South Korean intelligence officials blamed the North. The attacks, however, seemed to originate inside South Korea.

For years, masses of data have been stolen from sensitive U.S. government and defense-contractor computers in attacks that investigators have code-named “Moonlight Maze” and “Titan Rain.” Which nation—or nonstate actor—has repeatedly performed the brazen cyber espionage has never been clearly established. What is clear is that cyber warfare poses new risks that we have yet to fully grasp.

THE UNITED States thinks that its cyber warriors are the best at offense, with the capability of shutting down enemy air defenses, electric-power grids, rail systems and telephony. The United States has probably already penetrated many such networks and laced them with trap doors (ways to get back in easily) and logic bombs (software that would wipe out everything on a network).

Such offensive prowess does nothing to defend our own networks from similar attacks, however, and the current U.S. defense systems protect only parts of the federal government, and not civilian or private-sector infrastructure. No nation is as dependent on cyber systems and networks for the operation of its infrastructure, economy and military as the United States. Yet, few national governments have less control over what goes on in its cyberspace than Washington. And these major lapses in our defense present a threat we ignore at extremely high cost.

The possibility of an electric-power grid being hit by a cyber attack is less far-fetched than one might think. A CIA official has admitted that at least one blackout outside the United States was already caused by a cyber attack. An Energy Department laboratory determined that a cyber attack from the Internet could weave its way into the digital control system of a generator and cause the device to self-destruct. Officials have privately confirmed media accounts that logic bombs have already been placed in America's power-grid control systems, presumably by foreign cyber warriors.

And this problem goes deeper still. The "critical infrastructure" of the transportation, finance, energy and communications sectors are owned and operated by nongovernmental entities, corporations that have proven highly resistant to regulation. The Federal Energy Regulatory Commission (FERC) issued new cybersecurity guidelines to U.S. power companies in January 2008, requiring greater separation of the operations systems from the public Internet. But it took two years for these rules to go into effect (they start in January 2010), and many critics do not believe that the FERC has the ability to audit compliance. The leaders of those corporations, when asked about cybersecurity, almost uniformly believe that they should fund as much corporate cybersecurity as is necessary to maintain profitability and no more. They will defend themselves against cyber crime. Defending them against a cyber war, they all concur, is the job of the government.

Unfortunately, the government has no cyber-defense strategy. While the cyber warriors of Fort Meade may take comfort in America's reputation as having the most potent arsenal of cyber weapons, they may be members of the national cyber-war team with the lowest overall capability. Indeed, America's ability to defend its vital systems from cyber attack ranks among the world's worst. Some countries, like China, have implemented plans allowing them to shut the limited number of portals that connect their cyberspace to the outside world. Other nations, like North Korea, have such limited cyberspace and cyber dependence that there is almost nothing to defend. America's connectivity to the rest of the world is unlimited and controlled by no plan or agency. If, as a result of a cyber-war attack, our power grids failed, trains stopped and the financial sector froze, the government's response today would make former–FEMA Director Michael Brown's performance after Katrina truly look like one "hell of a job."

While we do have Cyber Command, it has a defensive mission largely limited to protecting the Defense Department. Cyber Command says someone else needs to defend civilian entities, specifically, the Department of Homeland Security (DHS). Unfortunately, DHS has neither a plan nor the capability to defend private-sector infrastructure from a cyber attack. Thus, electric power, gas pipelines, rail and air transport, banking, food-distribution networks and other key systems are defenseless against nation-state cyber attacks.

This asymmetry, in which we are developing offensive capability but doing little to prevent a devastating cyber attack, began in the Bush administration. In the last year of his eight-year presidency, George W. Bush signed a national-security decision called PDD-54. That directive, still classified, ordered steps be taken to improve the security of the Department of Defense and other federal-government computer networks. Critics say it did almost nothing to address the weaknesses of the national infrastructure. President Obama launched a sixty-day review of cyber policy in March, but it resulted in no new major initiatives. He did announce the creation of a cybersecurity position within the staff of the National Security Council (NSC). But it has yet to be filled permanently. The new staffer will report not only to bosses in the NSC staff, but also to Director of the National Economic Council Lawrence Summers—who has vehemently criticized government cybersecurity efforts in the past as imposing costly burdens on U.S. companies, whose leaders supposedly know best what level and type of cybersecurity they need.

When pressed about America's lack of cyber defenses, several officials privately suggested that there was no nation today that would want to hurt us like that. If that philosophy were applied more broadly to the defense budget, the nation could save hundreds of billions annually—and be left entirely defenseless.

THE FACT that legislators and policy makers do not understand the strategy issues surrounding cyber war may stem from the lack of public discussion, absence of academic contribution, minimal media coverage and insistence on unnecessary government secrecy. A multidepartment effort this year to develop a cyber-war-deterrence strategy produced a paper that is still labeled "secret." The last time someone thought a secret could deter an opponent was when 1960s movie character Dr. Strangelove yelled at the Soviet ambassador that a deterrent weapon only works "if you tell us you have it." America was not sufficiently deterred in that movie scenario (an air-force general launched an attack which resulted in escalation into global destruction).

In the absence of a public cyber-war strategy, we do not know today whether an air-force general could launch an effective cyber war. We have not had the basic discussion of whether the United States is better-off with the advent of cyber-war capabilities, or whether it is we who will be deterred in the future by the threat of cyber attack on our vulnerable infrastructure.

Although President Obama may not yet know it, his freedom to maneuver in the world is likely already restricted by those vulnerabilities. Perhaps in a crisis, someone will tell him. Or maybe he will learn it by looking out the window at a darkened city after he has ordered a bombing raid

on Iran, or sent a carrier battle group to protect Taiwan, or done something to irritate the Dear Leader of Pyongyang.

Maybe then he will ask policy questions such as: How does deterrence work in cyber war when our capabilities are secret and our weapons undemonstrated? Should we, because of our own vulnerabilities to cyber attack, initiate cyber-arms-limitation talks, instead of our current policy of opposing them? Can arms control work in cyberspace when verification is so difficult? Strategic defense was not possible in nuclear strategy, despite Ronald Reagan's best efforts, but does that also apply to cyber war? Can public discussion, international norms and established lines of communication result in some sort of risk-reduction process to address the issues of crisis instability that seem to be inherent in cyber war? Are the generals and admirals at Cyber Command more thoughtful than SAC's leaders were at the advent of the era of strategic nuclear war? We would like to think so, but in the absence of public-policy development, the American people cannot know the answer to that or to the many other questions that the possibility of cyber war raises. It is time for that public discussion.

Richard Clarke was special adviser to the president for cybersecurity in the George W. Bush administration. He is now chairman of Good Harbor Consulting. His book Cyber War*, coauthored with Robert Knake, will be published by HarperCollins in the spring.*