2010-08-30

Former Counterterrorism Czar Richard Clarke Calls for New National Cyber Defense Policy to Prevent a Cyber 9/11

Naval Postgraduate School Public Affairs Office

Naval Postgraduate School

Former Counterterrorism Czar Richard Clarke Calls for New National Cyber Defense Policy to Prevent a Cyber 9/11

Article By: Barbara Honegger

The Honorable Richard Clarke – former National Coordinator and Special Assistant for Counterterrorism, Security, Global Affairs and Cyber Warfare to three presidents – called for a new national cyber defense policy to reduce the likelihood of a Cyber 9/11, during a special lecture at the Naval Postgraduate School, Aug. 17.

The internationally renowned national and homeland security expert was at NPS to give two fast-faced back-to-back lectures on the subject of his latest book, Cyber War: The Next Threat to National Security and What to Do About It. The first venue was the Secretary of the Navy Guest Lecture to the assembled student body in King Hall, followed by the NPS Foundation Fall Quarterly Event on the Quarterdeck in Herrmann Hall.

“When historians look back at this period, what are they going to say were the really important changes that were going on?” he asked rhetorically in opening. “I think they’re going to say that this was a time when a new form of warfare – cyber warfare – came into its own. Though the U.S. leads in cyber warfare -- we invented it in terms of offense – we’re also the nation with the highest dependence on cyberspace in the world and only ten percent of our chips are from trusted fabricators. Because our critical infrastructure so heavily depends on computer networks and because of the open nature of our society, we’re highly vulnerable to cyber attack while also being relatively weak in cyber defense.”

“Would you go into a football game with just an offense and no defense?” he asked. “Of course not. But today in this country, that’s the situation we find ourselves in. The mission of the new U.S. Cyber Command is to defend the .mil environment, and [the] Homeland Security [Department] defends the .gov domain. But all the civilian-corporate private sector .com’s that run our critical infrastructure – the Internet, the stock market, the oil and gas pipelines, our food supply – are told, ‘You’re on your own.’ It’s in our clear national security interest to defend all of our critical infrastructure, but it’s our current policy not to do so. [Cyber] Offense has been given to the military, but defense is diffused.”

Clarke painted how much there is to defend against in stark terms, and took pains to distinguish cyber warfare from cyber crime and cyber espionage.

“Cyber espionage is essentially new – it didn’t happen 15 years ago,” he noted. “Today, cyber spies and cyber thieves don’t just read or steal few pages or documents a week like Aldrich Ames or Robert Hansen. They take out terabytes – measured in entire ‘Libraries of Congress’ of information – all remotely at a distance, like cyber predators. Every major government department including the military and every major private enterprise in this country and the world has been hacked, and can hack each other, and they’re sophisticated attacks. As just one example, Johns Hopkins University’s Applied Physics Laboratory is really good at cyber security, but nothing they could do could stop it. So their solution was to unplug the entire campus from the Internet. So, if there’s any value to the information you have in your systems, you can bet that it’s gone. The head of MI5 did. He wrote the CEOs of the top 300 U.K. companies telling them to assume that their computers had been hacked by the Government of China and that all their intellectual property had been exfiltrated. And our own cyberwar units have done successful red team attacks on the Pentagon’s SIPRNET and other supposedly secure closed-loop networks.”

But Clarke’s greatest warning was for “the arm that can come out of the computer” and wreak damage, disruption and destruction by breaching the firewalls designed to separate the cyber and real worlds.

“In a society where computer programs automate so many of the command and control functions of our critical infrastructure systems like gas pipelines, railroads, the stock market and mass communications, the difference between cyber espionage and cyber warfare is only a few keystrokes,” he stressed. “Once you’re there [inside an enemy system], you can issue electronic commands to open or close valves causing pipeline explosions and refinery fires; change the RPMs on huge generators causing them to fly apart; cause more power to go down high tension lines than they can safely carry; order trains to derail; and trigger chaos in the stock market, 70 to 80 percent of whose trades are now done by computerized buy-sell

programs, like the afternoon recently when it went crazy and one company’s market cap suddenly went to a trillion dollars. The Internet itself has physical aspects. It has servers and fiber optic cables, all of which reside in some real-world location that can be hacked and attacked in the same way. The U.S. government has done experiments proving that you can hack your way from the public Internet into the command and control system of our power grids, so this is very real.”

The paradigm shift is so all encompassing that, Clarke recalled, “a train company executive recently said, ‘I’m not a train company. I’m a network company that has trains.’ The Navy’s reconstituted Tenth Fleet, the World War II anti-submarine warfare fleet in the Atlantic, has no ships – it’s a cyber command; and the Air Force’s reconstituted 24th Air Wing has no planes – it’s also a cyber command, both components under the new four-star U.S. Cyber Command stood up last Oct. 1 [2009] at Fort Mead. Whether we realize it or not, we live in cyberspace – all the networks on the Internet and everything connected to it. It runs everything we do. ”

“So what needs to be done?” Clarke once again asked rhetorically. “First, decision makers and the public need to know and face these realities, admit that we’re vulnerable, and have a serious, open public debate on what this country’s cyber defense policy should be. And places like the Naval Postgraduate School are great places to start that national dialogue. NPS is well situated to discuss and develop strategy and to bring it to Washington and the White House, so in the future we can look back at the time when we had this great [new cyber defense] capability and we didn’t have to use it.”

“However it’s implemented, that big picture policy decision needs to be that the U.S. government will defend cyberspace, not just the .mil and .gov domains. We need to be ready so that, if there is an attack, like Captain Kirk on the Enterprise, the president can issue the ‘Shields up!’ command. To be able to do this, we need to decide – as a nation – who’s going to defend cyberspace, and I don’t think the military should be the lead agency. It should be run by the private sector in partnership with Homeland Security, with expertise and advice from NSA and Cyber Command.

“We also need to think seriously about an arms control treaty for cyberspace,” he stressed, “because two, and more, can play this game. Between 20 and 30 countries now have cyber warfare commands, many of which could hack into the command and control functions of Iran’s nuclear facilities, for instance. If we or an ally did that, do you think they’d just retaliate against our ships in the [Persian] Gulf and our military personnel in the region – in real space? They’d also attack us in the homeland, at a distance, through their cyber warfare unit. But we don’t have to speculate about possible cyberwar attacks in the future – they’ve already happened. Before the Russians physically attacked Georgia, they initiated a cyber attack on its critical infrastructure, remotely coordinated from a server in Brooklyn.”

“It [cyber arms control] won’t be easy – attribution [determining who is behind an attack] is immensely difficult, so the cyber world doesn’t lend itself to deterrence strategies like mutually assured destruction with nuclear weapons – but we have to try, just as we did with conventional weapons and bio weapons. We succeeded with those, and the only way to get there is by

starting. We need cyberwar 'hotlines', like the red phone to the Soviet Union during the Cold War, and most countries would agree to sign a treaty not to attack each other's international financial and banking system networks. They don't want to cross that Rubicon, or the entire international banking system could go down. We have an international regime for cyber crime, and we need one for cyber war – to rule out some things globally. But we have to take this seriously and move quickly. If we're not careful – if we don't take cyber defense and cyber arms control seriously – we may find ourselves in a shooting war and wake up to find that the enemy has pulled the plug on all our shiny, trillion dollar weapons, that our chips and supply chains have already been compromised, that our pipelines have been shut down and our trains derailed, all while our computer screens are telling us that nothing is happening."

As for cyber terrorism by non-state actors, the President's top counterterrorism advisor on Sept. 11 noted, "Don't use the two words in the same sentence. We haven't seen evidence of cyber terrorism connected with any terrorist organization, including Al Qaeda – probably because they're so dependent on electronic media and information technology to carry out their operations. The only exception to what I've seen is, prior to the 2006 Bali bombing, the Australian government said that the terrorist organization behind it raised funds, in part, through cyber crime, but even that's not using cyberspace to conduct actual terrorist acts."

Regarding Sept. 11 itself, Clarke noted that part of the little known history of that day was confusion by NORAD's North East Sector, which was about to conduct an exercise on a partial hijack scenario as the actual hijackings began, as to whether the unfolding events were "real world" or part of the exercise – a confusion whose cause bears an eerie similarity to the "arm reaching out of the computer" danger Cyber War warns about. "It's critical that exercises harden the firewalls between the computer and real worlds, but it happens more than you'd think. Yes, it happened on 9/11, and it happened with TWA Flight 800, when the Navy was doing a sea search exercise in the very area where the plane went down. And though the White House clears every major exercise, on Sept. 11th just last year, the Coast Guard ran an exercise on the Potomac River right near where the President was at the time. I'm a firm believer in exercises, and we have to make sure that firewalls in the future are tight. I wouldn't have been able to respond the way we did on 9/11 if we hadn't exercised it five times."

"This is such an important topic, and students here are such a key group – the future of the career military – to engage in this critical national policy debate on cyber defense," said National Security Affairs student and Foreign Area Officer Marine Corps Capt. Anna Noyne at the reception following the afternoon's second presentation. "So it's fantastic that Mr. Clarke is doing this here NPS. He can pick and choose where he goes, and it shows how important it is that the military be aware of this. He was right before [in warning of the danger of a terrorist attack before 9/11] when he said it could happen here, and we didn't pay attention. We have to pay attention now. This time, we have to take his warning seriously, and we have to act on it."

Despite decades of national responsibility resting on his shoulders, Clarke revealed a sense of humor commensurate with that weight. Taking the podium following a lengthy introduction citing his 11 consecutive years of White House service and 19 prior years in the Pentagon, intelligence community and State Department, he quipped, "I'm glad to see you left out my service in the Grant and Lincoln administrations."

Clarke's introduction included White House titles of Special Assistant to the President for Global Affairs, National Coordinator for Security and Counterterrorism and Special Advisor to the President for Cyber Security. During the Reagan Administration, he was Deputy Assistant Secretary of State for Intelligence, and in the Bush Sr. Administration served as Assistant Secretary of State for Political-Military Affairs.

Clarke's talks were sponsored by the Naval Postgraduate School Foundation, whose executive director, retired Rear Adm. Merrill Ruck, served with Clarke in 1990-91 when the latter was Assistant Secretary of State for Political-Military Affairs coordinating the diplomatic efforts to support the first Gulf War and subsequent security arrangements, and Ruck was Deputy Director of Political-Military Affairs for the Joint Staff in the Pentagon.

In addition to Cyber War, Clarke is the author of the New York Times No. 1 best seller Against All Enemies: Inside America's War on Terror, which details his pre-, day of and post-9/11 experiences in the Bush White House, and Your Government Failed You: Breaking the Cycle of National Security Disasters.

Clarke currently teaches at Harvard University's Kennedy School of Government, is an on-air consultant for ABC News, and is a partner in Good Harbor Consulting, LLC located in the Washington, D.C. area. Good Harbor advises clients on a wide range of issues including counterterrorism, corporate security risk management, information security technology, and dealing with the federal agencies on security and information technology issues.