CyberPro

Volume 7, Edition 2
January 23, 2014

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: DR. RICHARD B. ANDRES, NATIONAL WAR COLLEGE

NSCI recently had the opportunity to interview Dr. Richard Andres, Professor of National Security Strategy at the National War College. He holds a research chair at the U.S. National Defense University and is a Senior Fellow at the Institute for National Strategic Studies. Previously he was Associate Professor of Security Studies at the School of Advanced Air and Space Studies. Dr. Andres has held a number of posts in government including Special Advisor to the Secretary of the Air Force and Special Advisor to the Commander of Air University (24 schools, colleges and think tanks). Dr. Andres specializes in developing national security strategy and has led teams developing strategy for the White House, Chief of Staff of the Air Force, Commandant of the Marine Corps, Office of the Secretary of Defense, several combatant commands, and other civilian and military institutions. Andres received his PhD in Political Science from the University of California, Davis and wrote his dissertation under Randolph Siverson, Miroslav Nincic, Scott Gartner, and Kenneth Waltz.

NSCI: We'll start with an easy one. Are there any cyber-related papers / studies by National War College students that our subscribers can access? What topics / areas could our readers expect them to cover?

Andres: This is a trickier question that it seems. Until a couple of years ago, virtually everything the United States did in cyberspace was classified; even trivial things that had no business being classified. The result is that there isn't a lot written by active duty members of the military on this topic. That's starting to change but for the moment there isn't much in the way of a literature to recommend.

NSCI: How have you seen the quality and quantity of cyber-related education change within the Department of Defense?

Andres: A group of us started pushing to add cyber strategy to war college curriculums a decade ago without much success. A few years back, though, when senior defense officials like Deputy Secretary of Defense William Lynn started publicly talking about the cyber threat, a dam seems to have broken. Over the last few years both the quality and quantity of cyber education in the department have increased prodigiously. I conducted a study on cyber education across the U.S. war colleges last year and was pleasantly surprised to see how well this topic is being integrated into curriculums.

NSCI: There are a lot of commercial cyber-related courses, certifications, etc. How does National War College cyber-related education differ from these?

Andres: The National War College curriculum focuses on national security strategy. For instance, the Containment Doctrine that guided the U.S. approach to the Cold War was developed at NWC. When we look at cyber we want to know how it will affect U.S. diplomacy, economics, and broad military strategy.

We are looking at how the United States can use cyberspace to increase international stability and prosperity and how we can prevent opponents from using it to threaten the United States and its allies.

NSCI: How do you think our overall National Security Strategy does at addressing / incorporating the cyber dimension?

Andres: Strategy isn't static. We've come up with a strategy but our opponents have done their best to develop strategies that outmaneuver ours. The U.S. and its allies are losing billions of dollars a year to cyber theft. A colleague calculated that if the cost of cyber theft is as high as many people think it is, it accounts for the current economic downturn. Similarly, private industry is reporting that China and Russia have placed malware on most critical infrastructure in the United States while taking precautions to protect their own. On the diplomatic front, our European allies are hostile to our approach. The truth is we need to reconsider our NSS as it applies to cyberspace.

NSCI: What recommendations do you have to improve our national and/or Department of Defense cyber strategy?

Andres: Our greatest vulnerability is private industry. Traditionally the U.S. military defends industry against attacks from other countries' militaries. If an opponent sent a cruise missile against Lockheed Martin, we would look to the Department of Defense. But when our opponents send malware that does far more damage than a cruise missile could do, we can't seem to wrap our heads around it. There is a story about European conquerors sending smallpox-infected blankets to their Native American opponents. How do you react to something bad wrapped in something good? Currently, the industry is spending millions lobbying Congress to block defense regulation and intrusion but it is losing billions to theft by foreign militaries. If we lose at home it doesn't matter how effective our troops are in the field. This problem is where we need to focus our attention as a military and a nation.

NSCI: How do you think we are doing in planning for / incorporating adequate cybersecurity as it relates to the smart grid?

Andres: According to the industry, our infrastructure is infested with malware. People are concerned but don't know what to do about it. Smart grid as it is currently envisioned is going to make the security threat much worse. It reminds me of the housing boom in Chicago preceding the great fire of 1871. It's not that people didn't know the cheap materials they were building with would burn; they just planned to make their money and get out before the whole thing went up in smoke.

NSCI: What do you see as the key cyber-related trends that ought to most concern us in the next few years?

Andres: The biggest problem is the "frog in the pot" dynamic. People look around and say "nothing bad happened last year" so they allow themselves, their companies, and their militaries to become a bit more vulnerable next year. I would guess that it would take a massive attack from a major power to do anything that looks like a Cyber Pearl Harbor right now but I'd bet that if we stay on our current

trajectory even mid-sized countries like Iran and North Korea will be able to cause enormous physical damage in two or three years.

NSCI: Any thoughts on the "right" balance between cyber deterrence, offense, and defense?

Andres: Our opponents appear to be trying to get as much from us as they can without crossing the threshold that would cause us to react. They've calibrated their moves fairly well so far. Both the government and industry are hamstrung from spending on cyber defense by short-term political and investment cycles. Government is unwilling to demarche opponents for fear of upsetting diplomatic and economic relations. This seems to leave a free-for-all offensive mindset for all countries concerned and has created a cybersecurity dilemma. The problem is that in a security dilemma, it does no good to unilaterally back down. What I would like to see is government and industry spending more on defense and attempting to deter future cyber offensives with credible threats of diplomatic and economic retaliation but I believe that reliance on cyber offenses will only increase over time.

NSCI: Finally, what are your thoughts on the reality / likelihood of a "Cyber Pearl Harbor"?

Andres: A well-coordinated nationwide cyber-attack by a major power would destroy a great deal of physical infrastructure and cause immense human suffering. Fortunately, the states most capable of executing a Cyber Pearl Harbor would have the least to gain by conducting one. Nevertheless, a state could attempt to use this capability to deter the United States from defending an ally or taking some other action, possibly using a combination of modulated escalation and plausible deniability. The bigger problem is that it will only become easier to execute cyber-physical attacks with time, and when mid- and small-sized opponents can execute this type of attack against the United States the risk will increase. Beyond this, I do worry about a catalytic attack in which a third party conducts an attack under a false flag to elicit a U.S. response, and about Sampson-outcomes in which an enemy regime that is about to go down executes an attack believing it has nothing to lose.

NSCI: Is there anything else you'd like to add?

Andres: Human beings have a talent for using good things for bad purposes. The printing press fueled the Thirty Years War, modern banking financed the rise of massive armies, and internal combustion led to tanks and bombers. Over the last few years we've seen cyberspace used for espionage and economic conflict. Today we are at the cusp of finding out how creative humankind is at turning cyber tools into cyber weapons.

NSCI: Thank you very much for taking the time to visit with us.

The opinions expressed here are those of Dr. Richard Andres and do not necessarily represent an official position of the Department of Defense, National War College, or any other government organization.