PREVENTING A DIGITAL PEARL HARBOR

By **COL Gregory Conti '89** and **LTC David Raymond '89**, USMA

It is 11 p.m. on a Saturday in April 2011, and Thayer Hall is dark except for a well-lit computer lab in a corner of the second floor. While most of their classmates are on pass, a handful of firsties toil into the night putting finishing touches on a computer network that, in a little over 48 hours, will be put to the test by some of the National Security Agency's (NSA) top computer network attack specialists.

For these cadets, a group of computer science, information technology, and electrical engineering majors, this is much more than an academic exercise or course grade. This is their "Army-Navy Game." Their branches already assigned and their first posts chosen, these cadets hope to carry on West Point's winning tradition in the annual Cyber Defense Exercise (CDX).

As our national infrastructure, economy, and military have become increasingly dependent on computers and networks, it is critical that the United States works to prevent what Defense Secretary Leon Panetta labeled a "Digital Pearl Harbor." To do this, the country needs leaders both with experience fighting on the cyber battlefield and with the ability to integrate cyber effects into the kinetic battlefield. Since the late 1990s, the United States Military Academy at West Point has been educating such leaders through its cyber security education program, which includes West Point's Cyber Research Center and the annual Cyber Defense Exercise.

Held annually since 2001, the CDX is a cyber security event sponsored by the NSA that involves undergraduate competitors from the five service academies, along with graduate student teams fielded by the Air Force Institute of Technology, the Naval Postgraduate School, and the Royal Military College of Canada (although rules state that only the undergraduate teams can compete for the NSA Director's Trophy). West Point has won the CDX Trophy more times than all other service academies combined, which demonstrates the skill of the cadets and the commitment that the Academy has made to educate leaders in this critical domain.

For the cadets involved in the CDX, getting to the competition has been a journey. Making the CDX team requires them to take part in a rigorous, four-year preparatory program organized by West Point's Cyber Research Center (formerly the Information Technology and Operations Center). Part of the Department of Electrical Engineering & Computer Science (EE&CS), the Cyber Research Center takes an interdisciplinary approach to cyber security education and research and seeks to educate all cadets in cyber security, not just CDX team members. Every cadet receives substantial cyber security training in West Point's two core Information Technology courses and the cadet Cyber Warfare Club boasts members from every academic department.

CDX team members must also undergo supplementary education and training, which runs the gamut from upper-level electives to Academic Individual Advanced Development internships. Some team members also have given up their Second- or First-Class Spring Leave to prepare for the competition by taking intensive cyber security training courses, while others attend security conferences, such as DEFCON and ShmooCon, where cadet teams have presented their research to audiences of 1,000 or more security professionals. Many of these CDX-related activities were made possible by generous gifts from the SANS Institute and from Marshall N. Carter '62, in memory of his father Lieutenant General Marshall S. Carter '31, a former Deputy Director of the CIA and Director of the NSA. To support the broader cyber security education program, the Cyber Research Center selectively seeks

Above left: Members of the 2011 CDX team reacting to NSA "Red Team" intrusion attempts.

additional sponsored research and education funding, often building faculty and cadet research teams to help solve pressing needs for organizations such as U.S. Cyber Command, NSA, Army Cyber Command, Office of the Secretary of Defense, and the FBI. The results have been impressive and have resulted in widespread media attention, including coverage by the *New York Times*, BBC, *Time*, MSNBC, the *Economist,* and the Associated Press.

Over 40 cadets were on West Point's 2011 CDX team, and their mission was to design and implement networks that are representative of the systems and services normally found in a command post. They then had to defend these networks against an attacking NSA "Red Team," a group of over 40 network security experts from the NSA, U.S. Cyber Command, and their contract partners, who relentlessly hammer all of the academies' networks, finding and exploiting vulnerabilities wherever they can. If a team can maintain the availability of services as well as the confidentiality and integrity of critical data stored on their networks, they'll score points in the exercise.

It is now day three of the four-day CDX competition, and the Red Team has penetrated the networks of all but two teams: West Point and Air Force. Scoring favors the Falcons, but the West Point CDX team, as indicated by Cadet Christina West '11, remains optimistic: "We're up there right near the top so it's anybody's game at this point and we really think that today is going to be the day that we pull it off."

Success in the CDX requires a careful balance between securing the network and ensuring availability of network resources to those authorized to access them. "We know how to secure physical assets, put up walls and fences, and add guards," says Cadet Anthony Rodriguez '11, USA 2011 CDX Team Executive Officer. "Now we are trying to figure out how to translate that to the digital realm, putting those same fences and guards up to prevent people from getting in." An age-old system administrators' edict states that "the only way to make a system 100 percent secure is to unplug and bury it." Unfortunately, this prevents anyone from accessing your website or exchanging email with your employees. It is very difficult to maintain both availability and security, and in the CDX, availability points are critical. Before system configuration even begins, the cadets need to design a network sophisticated enough to ensure the security of critical resources, but simple enough to keep everything running if a Red Team attack compromises one portion of the network.

To do this, an incremental approach to developing a CDX network is preferred. Here, the team first builds the network, then deploys the services (such as web, email, and file sharing), and finally, when everything is working, it starts hardening the network. This is difficult because the security group has to wait until the network is operational before they can begin their work, reducing the potential for parallel efforts. While the cadets must design and build the network, several Academy faculty and staff members act as coaches and volunteer their expertise in computer science, network administration, and information security.

It is the last day of the competition, and the CDX organizers are analyzing final scoring data. West Point's CDX team, along with scores of cadets, staff, and faculty gather for the final teleconference. After opening remarks, the Deputy Director of NSA's Information Assurance Directorate, Rob Joyce, makes the presentation: "The academy winner in 2011 for the Cyber Defense Exercise is . . . the United States Military Academy at West Point!" The room erupts as the team celebrates their hard-fought victory and sound dethroning of the 2010 champ, Navy.

Members of the winning CDX team with the NSA Director's Trophy in front of the mess hall, before the trophy presentation with NSA Deputy Director Chris Inglis.

In a field as dynamic as cyber security, to stand still is to fall behind. West Point aggressively continues to evolve its cyber security program through educational innovation, outreach, and partnerships. In terms of education, the EE&CS has an ongoing self-organized group working toward the Certified Ethical Hacker and Certified Information Systems Security Professional certifications. In addition, West Point is the first undergraduate-only institution to receive the NSA's prestigious Center of Academic Excellence in Information Assurance Education designation, and is now pursuing certification in the NSA's new Center of Academic Excellence in Cyber Operations program. West Point is also in the process of building a Sensitive Compartmented Information Facility to provide classified operational briefings and facilitate classified research. Seeking to outreach, West Point faculty have spent summers working at NSA, U.S. Cyber Command, and Army Cyber Command, and one was deployed as Officer in Charge of U.S. Cyber Command's Expeditionary Cyber Support Element in Iraq. Lastly, pertaining to partnerships, West Point's NSA Fellow, Howard Taylor, is working to organize a new cyber warfare course to be used by West Point and later by other service academies and ROTC programs. Army Cyber Command and the NSA also have helped to develop post-graduation internship programs, enabling select second lieutenants to experience strategic cyber operations before beginning their branch-specific Basic Officer Leader Course. Finally, a team of cadets and faculty recently worked with experts from Raytheon to help seek solutions to the insider threat problem.

With the Department of Defense's recognition of cyberspace as an operational domain alongside Air, Land, Sea, and Space, and with the formation of U.S. Cyber Command and Army Cyber Command, the Army is preparing to defend the nation against aggressive and persistent adversaries threatening its global online network. Given the high stakes, a robust cyber security program is a critical component of the Academy curriculum that prepares our graduates to be leaders of the 21st century Army. West Point currently offers one of the best cybersecurity programs and is training its cadets to become technically literate leaders who have the knowledge to understand the domain of the cyber battlefield and the strategic ability to win in cyber warfare. Perhaps General Keith Alexander, NSA Director and Commander, U.S. Cyber Command, says it best: "The reality is, five years from now, if the cadets who went through [the CDX] learned something that can help defend our nation, then we all win." ✯

Colonel Conti is an Associate Professor in the Department of Electrical Engineering & Computer Science as well as the Director of West Point's Cyber Security Research Center. Lieutenant Colonel Raymond is an Assistant Professor in the Department of Electrical Engineering & Computer Science, and he is the lead instructor for CS482, Cyber Security, and faculty advisor for West Point's Cyber Defense Exercise team.

Below: A Beat Navy nametape using the hacker alphabet. The CDX is West Point's cyber Army-Navy Game.

Visit WestPointAOG.org/CDX
to connect with the team on Facebook.

Branch Results for the Class of 2012

By **Jay Olejniczak '61,** Guest Writer

Speaking on behalf of the 50-Year Affiliation Class of 1962, Lieutenant General (Retired) Ted Stroup described his branch night to those firsties who were eagerly awaiting their own branch assignment. Back then, only five branches were offered—Armor, Artillery, Engineers, Infantry, and Signal Corps. He described how each classmate was called based on general order of merit: each stood, surveyed a screen showing the number of slots available for each branch, and announced his choice. Then, the officer in charge erased that slot and updated the number remaining on the overhead slide with a grease pencil. To illustrate the procedure, Stroup called the names of several '62 classmates in attendance, and they rose to proclaim their choice of branch.

When the time came for the branch assignment envelopes to be opened by this year's cadets, pandemonium erupted in the auditorium, cell phones were immediately pressed into service to inform friends and family of the news, and dozens of digital cameras immortalized the moment with the photos being immediately uploaded to social media sites. Cadets then scattered to various rooms to receive their first set of insignia from branch representatives. After the ceremony, members of the class regrouped at Ike's Riverside Café, where snacks and beverages awaited.

In total, 1,027 members of the Class of 2012 received branch assignments as detailed in the charts to the right.

Go to WestPointAOG.org/BranchNight
for video.

COMBAT ARMS	
Air Defense Artillery	51
Armor	99
Aviation	120
Engineers	134
Field Artillery	145
Infantry	239
SUPPORT ARMS	
Adjutant General's Corps	23
Chemical Corps	9
Finance Corps	6
Medical Service Corps	20
Military Intelligence	53
Military Police Corps	15
Ordnance	33
Quartermaster Corps	23
Signal Corps	38
Transportation Corps	19

54 cadets branch-detailed into AR, FA, IN