Maintaining the Edge - NPS, Information Dominance, and the New World

Naval Postgraduate School Public Affairs Office

Naval Postgraduate School

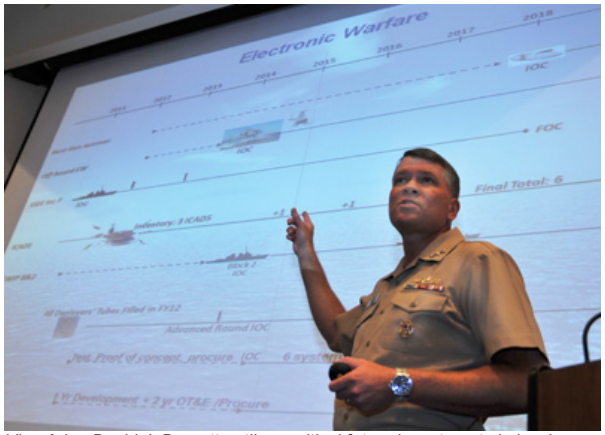
Maintaining the Edge - NPS, Information Dominance, and the New World

Article By: Amanda D. Stein

Clouds of smoke billowed from the beaches of Veracruz as hundreds of men faced the uncertainty of their fate. Outnumbered 300 to one and facing a long, difficult battle with the Aztecs, Spanish explorer Hernán Cortés ordered his men to burn their ships. Eliminating any chance they had of retreat, Cortés had left his crew with only two options – succeed or die.

The year was 1518, and the battle to secure the territories of what is now Mexico waged vehemently. With a courageous, resolute leader and almost certain death if they were defeated, Cortés' men accepted his challenge, and conquered the Aztecs against immeasurable odds.

Today, the U.S., if not the world, is facing a different kind of adversary – one that has no single identity and outnumbers us at equally staggering odds. It is the war over information and it requires bold leadership and an unwavering approach. The Chief of Naval Operations (CNO) has referenced Cortés' brave mentality, even echoed it in his battle to secure and obtain information – a field that has come to be known as Information Dominance.



Vice Adm. David J. Dorsett outlines critical future investments in hardware to meet the growing challenges in Information Dominance. Dorsett addressed a large contingent of IDC students at NPS during a campus visit, August 23, stressing the U.S. military's, and the Navy's commitment to maintaining an edge in Information Dominance.

Even before it became a key area of concern for the Department of Defense (DoD), NPS had faculty and students exploring the possibilities of using information as a weapon against potential adversaries. One such professor, Dr. John Arquilla of the Defense Analysis Department and Director of the Information Operations Center, coined the term Information Dominance in a 1994 article titled "The Strategic Implications of Information Dominance." Arquilla brought that concept to NPS and has since become one of the country's leading experts on information-age warfare.

Arquilla imagined a chess board with one player able to see only his own pieces and moves, and his opponent able to see the entire board, including the pieces and moves of his competitor. For Arquilla, that concept clearly demonstrated that a really strong enemy could be defeated by an opponent, even one with fewer pieces, who had the information advantage. That is also a concept explored by students within the Defense Analysis Department, where they are exposed to courses on information operations, irregular warfare, culture, cyberspace conflict and intelligence.

"I think information technologies both empower our military and imperil it," explained Arquilla. "Many of the technical efficiencies that make us so dominant in battle have also made us very dependent upon their availability. And the disruption of these systems, many of them fully automated, could profoundly degrade our combat capabilities. In this respect, information technology is a double edged sword and we have to proceed carefully. That said, despite the risks I think the benefits are quite great."

As technology has become more prevalent in our culture and our military, it has become even more critical that the systems upon which we rely are properly secured. The topic of information dominance has picked up momentum within the Department of Defense over the past few years, and has become a key area of focus for military leaders such as Vice Admiral David J. Dorsett, Deputy Chief of Naval Operations for Information Dominance and Director of Naval Intelligence. He and Chief of Naval Operations, Adm. Gary Roughead have committed to making the Navy a strong leader in the ID field, which includes several different information communities.

"The CNO has directed that the Navy be the most prominent and dominant service in the areas of intelligence, cyber warfare, command and control, electronic warfare, battle management and knowledge of the maritime environment," said Dorsett. "This aspiration is only possible if we continue to break down barriers between fields, professions and skills … and create a dramatically more competent and influential information-focused workforce for the future."

That desire to maintain the most capable ID forces has lead to the establishment of the Information Dominance Corps (IDC) within the Navy. The IDC incorporates all of the ID relevant fields and serves to establish ID as a core warfighting capability within the service.

Retired Rear Adm. Andy Singer speaks with student Lt. Beth Jasper outside Root Hall on the NPS campus. Recognizing that intelligence is a critical area of opportunity over adversaries and to maintaining dominance

One aspect of the IDC, intelligence, has long been understood to be a critical area of opportunity over adversaries. NPS' Intelligence Chair and Director of the Information Dominance Center of Excellence, retired Rear Adm. Andy Singer, noted that ID comes down to gathering information and using that information in a way that gives us an advantage over our adversaries. In that role, the Intel community is critical to maintaining dominance in the information realm.

"All the communities in the IDC are hunters and deliverers of Intelligence," explained Singer. "While Naval intelligence focuses on delivering knowledge of the enemy, it takes the communities collective work to make that knowledge as complete as possible and from it find the opportunities to anticipate, know, predict and change the adversary's desired effects. NPS is giving Navy Intelligence professionals the technical and regional expertise needed to master information advantages for our nation. In today's Navy, Intelligence is the key to knowing first and therefore acting first and best."

While gathering information is critical, protecting it is equally important and the U.S. has stepped up in response to a threat that hasn't always been as prevalent. In May 2009, President Barack Obama issued a press release on the importance of remaining diligent in cyber defense. He noted that the threat to our digital infrastructure would undoubtedly affect daily life in the U.S. as a nation so connected through networks.

"From now on, our digital infrastructure, the networks and computers we depend on every day will be treated as they should be; as a strategic national asset," said Obama. "Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter,

prevent, detect and defend against attacks and recover quickly from any disruption or damage."

critical area of opportunity over adversaries and to maintaining dominance in the information realm, Singer guides intel educational efforts as NPS' Adm. Bobby Inman Intelligence Chair, as well as Director of the Information Dominance Center of Excellence.

Secretary of Defense Robert Gates has vowed to establish a strong force to respond to cyber security threats, one of the growing concerns within the ID communities. On May 21, Gates activated the United States Cyber Command (USCYBERCOM) to be headed by NPS alumnus and current Director of the National Security Agency, Army General Keith B. Alexander. CYBERCOM supports the joint services in cyber defense, and is tasked with all aspects of protecting the DoD networks from potential threats.

"In the Information Age, we are only as strong as our information infrastructure and those who protect it. That protection may come from the physical or cyber domain, though cyber investments are always less expensive," explained Navy Cmdr. Sean Heritage, IDC Officer and Current Commanding Officer of the Navy Information Operations Command Pensacola. "From an organizational standpoint, the stand-up of CYBERCOM is extremely significant. Within the Navy, the re-establishment of [Fleet Cyber Command], the realignment of [Navy Cyber Forces] functions, as well as the birth of the Information Dominance Corps are more than symbolic gestures."

Alexander's vision for the new command is one that is dedicated to ensuring that sensitive information is secure, and that the military is properly prepared to respond to threats against government networks, or networks that, if compromised, would threaten our national security. He adds that doing so in the most open manner possible is a high priority.

"I think that perhaps the most important problem facing CYBERCOM will come out of concern over what the military and the intelligence community is doing in the networks," explained Alexander. "The solution to that is transparency. Transparency with the American people, with Congress, and with the Administration so everyone knows exactly what we are doing and how we are doing it. Future commanders and directors have to have both the technical capability and the ability to communicate those issues so that people understand and have trust and confidence that we are doing that mission correctly."

Part of his visit as the September graduation speaker, Army Gen. Keith Alexander, far right, takes the opportunity to meet candidly with a select group of NPS' Information Dominance Corps students about their roles in the executing DoD's mission. Alexander serves as the current Director of the National Security Agency/Chief, Central Security Service and is head of the newly established U.S. Cyber Command.

Because cybersecurity is a fairly new concern, there is little known about what would constitute a 'cyber war'. One of the critical realities that come with cybersecurity is how extensively the cyber domain and the physical world intersect, and what the consequences can be to our homeland security if the DoD was ill-prepared for an attack. Hospital records, bank accounts, air traffic control, power grids, and even life-saving electrical equipment are all operated using systems that can become vulnerable to attack if not developed with the proper security measures. Compromising these technologies could mean serious consequences in terms of personal safety, economics, and the ability to respond to an attack.

"The problem is that if somebody gets into your network, you don't know who they are," explained Distinguished Professor of Defense Analysis, Dorothy Denning, one of the nation's foremost experts on information security. "You have to be concerned with everybody. You don't know their motivation or what data they are after. You don't know what kind of malicious code they may leave behind that can cause problems later. So you have to take every attack seriously."

Faced with thousands of attacks each day, the DoD has an enormous task on their hands in trying to secure and protect those networks. The kinds of threats facing the cyber domain are vastly different from the traditional acts of war, leaving traditional warfighters unfamiliar with the kinds of technology being used to defend. To mitigate those threats and create a strong ID force, NPS strives to create the kinds of academic programs that could help military officers and DoD civilians understand and develop ways to respond to attacks. One such program, the Center for Information Systems Security Studies and Research (CISR), focuses on meeting the Information Assurance (IA) needs of the warfighter by providing a comprehensive network defense based curriculum.

"Adversaries currently have an asymmetric advantage: they do not have to work very hard to succeed, yet defense is very hard," said Computer Science Professor and CISR Director, Cynthia Irvine. "Our biggest challenge is to find ways to make the work factor for an attack by sophisticated adversaries much larger, thus tipping the scales in favor of the defender through robust, resilient systems built on a solid foundation and that can support dynamic defense. There is a great deal of work ahead. Fortunately, NPS personnel have a deep understanding of cyber security, some acquired over many decades, and can creatively address today's challenges."

CISR is just one of many ID relevant programs offered to both U.S. military and international military students at NPS. Because the Internet has become such a global institution, and adversaries can attack the DoD network from almost anywhere in the world, NPS programs offer the training and understanding for our global partners to help in the information and cyber defense efforts. Threats most often come not from state governments looking to incite an act of war, but from individual radical groups or 'patriotic hackers' looking to gather sensitive information or disrupt system operations.

"I think there are two parts to engaging global partners," said Alexander. "We will have to come up with a way of establishing rules of the road for operating in cyber space. What constitutes an act of war? What are the red lines that each country has? What is normal behavior? All of those will have to be addressed. Along with that will have to be a whole new theory on deterrence and how to deter in cyber space. We will have to develop all of that over time."

As the tactics and capabilities of potential adversaries evolve beyond the traditional battlefield, the U.S. military remains vigilant in maintaining an information edge. While Cortés chose to burn the ships behind him to force a course of action, today it's NPS' education, training and awareness in the ID fields that will drive that vigilance. The struggle for Information Dominance will be an ongoing one, with enemies and strategies constantly changing. The one certainty is that there will be no turning back for the U.S.' commitment to maintaining dominance in the information domain.