PREPARING THE U.S. NAVY FOR 21ST CENTURY WARFARE: THE U.S. NAVAL ACADEMY TRAINS MIDSHIPMAN FOR CYBER OPERATIONS

http://www.sldinfo.com/preparing-the-u-s-navy-for-21st-century-warfare-the-u-s-naval-academy-trains-midshipman-for-cyber-operations/

2015-02-23 By Ed Timperlake and Robbin Laird

The Naval Academy Motto is; Ex Scientia Tridens –Through Knowledge Sea Power, and that captures the vision for a 21st century Cyber Operations Major being developed at the US Naval Academy.

In preparing the U.S. Navy for 21st Century Warfare, the U.S. Naval Academy is in the formative stages of beginning to train Midshipman for Cyber Operations.

The USNA Cyber Center, the catalyst for dynamic innovative course development, is temporally housed in Leahy Hall on the Academy Yard.

The building is named for Fleet Admiral William Leahy who was the most senior US Navy Admiral in World War II. The Hall is across the street from the actual path of light that allowed USNA Professor Albert Michelson Class of 1873 to experiment in measuring the speed of light.

The scientific and engineering tradition at Navy is moving ahead at flank speed in embracing all things "cyber."

The effort is building on a distinguished lineage of scientific and engineering history. Midshipman Albert Michelson, Class of 1873, and then USNA Professor Michelson, in the late 19th Century pushed the theoretical boundaries of physics at the Naval Academy for the 20th Century Navy.

Now on the banks of the Severn River the beginning of a dedicated Cyber Center is preparing midshipman to enter today and tomorrow's fleet.

Every year Nobel Laureate Professor Michelson is honored at the Michelson Memorial Lecture Series in which many distinguished Nobel Laureates and other prominent world-class scientists provide their insights on critical issues.

The Michelson Memorial Lecture Series commemorates the achievements of Albert A. Michelson, whose experiments on the measurement of the speed of light were initiated while he was a military instructor at the U. S. Naval Academy. These studies not only advanced the science of physics, but also resulted in his selection as the first Nobel Laureate in science from the United States.

For example, in 2009, Professor Christos Papadimitriou Hogan Professor of Computer Science at University of California Berkeley presented a paper entitled:

"The Algorithmic Lens: How the Computational Perspective is transforming the Sciences"

In the questions, which followed the presentation, Professor Papadimitriou was asked for his view on which country is advancing computer science the most.

His answer was very direct in stating that with all due respect to his colleagues around the world he believed that the United States was in a leading position for two simple reasons. America has freedom of expression, which generated a framework for the development of innovative approaches, and the financial support was significant for innovative research and applications as well.

Cyber science is a new academic discipline for advancing military combat operations and it clearly is intellectually exciting to be a Midshipman at the Naval Academy during this significant moment in time.

The Midshipmen are "plank holders" in a new field of study.
And it is a field of study, which is foundational for 21st century warfare.

Cyber is one of the key domains of warfare, which a modern sea service must master to be successful in a wide spectrum of operations.

The modern warships and systems already deployed with the USN and USMC as well as those coming on line and anticipated in the future all rely on digital content, communications and effective C2 capabilities to ensure mission success.

Admiral Greenert, the Chief of Naval Operations, has prioritized the importance of cyber, and has even compared to the importance, which he places on nuclear deterrence.

“The level of investment that we put into cyber in the department is as protected or as focused as it would be in strategic nuclear.”

He highlighted why cyber was so important to the USN in an interview published in May 2013:

For the U.S. Navy, cyber security is critical because its ability to coordinate ships, planes and personnel depends heavily on computer networks and satellites.

“We’ve got to understand how to defend them, how to exploit them ourselves and how to, as necessary, be able to do offensive effects,” said Greenert, who will attend this week’s IMDEX Asia maritime defense show in Singapore.

“Many people who look at the future of warfare say it’s bound to start in cyber. The first thing you’d want to do is shut down their sensors, interrupt their power grid, confuse them … and presumably guard against that kind of thing and recognize if it’s starting.”

The U.S. Navy has enjoyed advantages in traditional sea, undersea and air warfare but times have changed, he said. “In the cyber domain, a lot of people – civilian hackers, anybody – can get into this,” Greenert said.

Cyber is often confused with computer and information security. But it is really about cyber operations within the context of rapidly evolving concepts of operations, as digital systems become dominant players in the evolution of war fighting capabilities.

Our visit to CVN-78 highlighted the centrality of C2 and related systems to the operation of the next large deck carrier.

In fact the CVN-70 is designed specifically with the need to embrace the dynamic nature of evolving cyber capabilities.

There are 17 compartments in the Aircraft Carrier that can be constantly configured and reconfigured to be dedicated to a specific or general use of computers.

The ship was designed with tremendous excessive power to facilitate all electronically powered systems yet to come, from advanced computers facilitating state-of-the art communications, radar and other sensor systems to lasers as weapons.

Additionally there are three software upgradeable aircraft flying today – the Australian RAAF Wedgetail, the Navy's advanced Hawkeye, and the F-35 – and two of these aircraft will fly off of the Ford and intersect with the software upgradeable radars and C2 systems onboard.

And working collaboratively to integrate strike and defense capabilities with the rest of the Navy force, the joint force and coalition partners rests upon effective cyber operations. This means that cyber is part of the evolving concepts of operations for the maritime, joint and coalition force. It is not an add on; it is not a standalone; it is part of the integrated warfighting effort.

The CNO underscored in a speech October 2013, the importance of the educational process to prepare the Navy for the way ahead in operating 21st century forces:

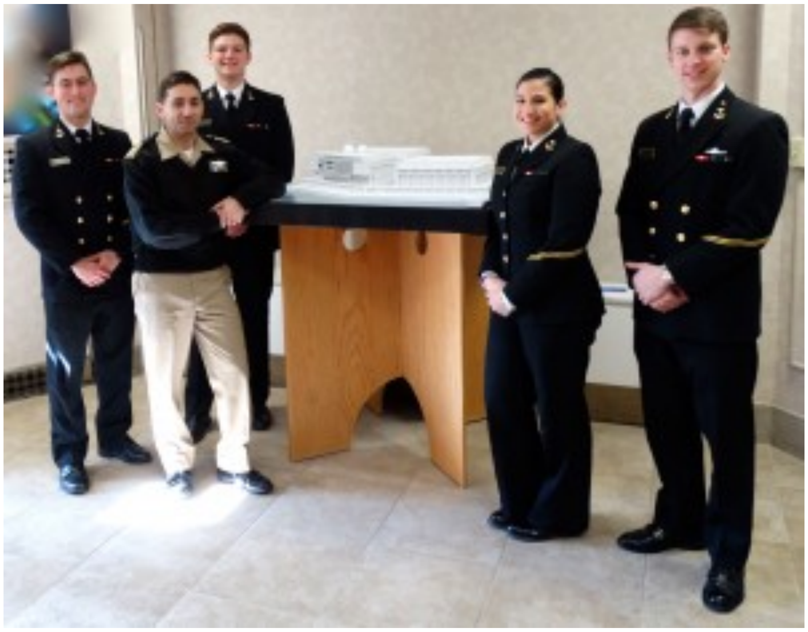
"We're going to have to teach our people to understand the value of this spectrum and cyber.

We just need to break out of our training techniques."

The US Navy CNO on Cyber Operations from SldInfo.com on Vimeo.

The US Naval Academy is at the cutting edge of "breaking out of our training techniques." To understand the role, which the Academy is playing, and the approach the USN is taking to shaping new approaches we visited the U.S. Naval Academy in February 2015.

We had a chance to discuss the evolving approach with Captain Paul Tortora, Director of the USNA Center for Cyber Security Studies, and with four second class midshipman (college juniors) who are part of the first class of majors in Cyber Operations.



Captain Tortora and 4 students in the cyber major after the SLD interview. Credit: Second Line of Defense

Captain Tortora is a 1989 graduate of the Academy as a math major, who then became a Navy Nuclear trained officer serving on a fast attack submarine and then mid-career switching over to become an intelligence officer aboard the USS Eisenhow

Because the field is in flux, the challenges are in flux, the approaches to deal with the challenges being shaped, and the mix of skill sets being defined to operate as cyber warriors, Captain Tortora is pursuing an open ended approach to shaping the Center.

First, it is a center not an academic department.

Academic departments tend to become very close ended and rigid in defining subject areas, an approach which would lead to failure to dealing with the emerging subject of cyber operations.

An academic department is being set up in order to have tenured faculty, with a goal of approximately 6 departmental members, 3 military and 3 civilian, but the Center-led effort will remain crucial to the continual process of engaging with and shaping the field of endeavor.

And as the first classes go into the field and experience feed back to the Academy the subject itself will be redefined, reworked, and taught differently as fleet experience folds into the teaching process.

Captain Tortora explained that there are two different but intersecting processes in play at the Academy.

The first is the requirement to teach ALL Midshipmen cyber awareness and cyber security fundamentals.

And the expectation is that this beginning effort will be revitalized over time as the graduates lead the way in shaping the 21st century USN and USMC. There are two mandatory cyber courses all Midshipmen take, one as Plebes (freshmen) and another as Juniors, both of which cover basic cyber awareness, security and electronic warfare.

The all things digital approach is being laid down and built upon in shaping cyber engagement.

The second is standing up a dedicated Cyber Operations major, which is really more about how to effectively operate across the breadth of the cyber domain, similar to more of a con-ops rather than a narrowly technical cyber security curriculum.

Here the goal is to combine the technical fundamentals of this domain, with the non-technical policy and legal aspects to understand the social dynamics within which cyber attack and defense is an operational reality.

As Captain Tortora said in discussing the cyber attack/defense enterprise, “we have no problem saying ‘attack’, we are, after all, educating future Naval Officers.”

The interaction among the students and faculty is crucial to shaping what should be included in shaping the curriculum and what is necessary for an appropriate education. Captain Tortora repeatedly emphasized the key role, which the students were playing in shaping the major and how to forge an effective curriculum.

“**They are the ones crucial to helping us build out an effective curriculum; sometimes they refer to themselves as intellectual guinea pigs.”**

The three year track followed by majors at the Academy (and remember the 2nd Class ‘16 are first ever Cyber Operations majors at the Academy) involves technical issues, policy issues, legal issues, social issues and then in the third year seminars and papers. The curriculum already has a number of courses dealing with the non-technical aspects of cyber operations, to shape a more comprehensive understanding of the operational dynamic.

The interactive nature of shaping the field is reflected in the fact that the students in the field are engaging in various outside organizations and attending external conferences and sessions, such as attending the Cy-Con Conference in Estonia.

Internships are crucial as well at places like NSA, and with various Centers located in industry and government which are engaged in shaping approaches to dealing with cyber operations.

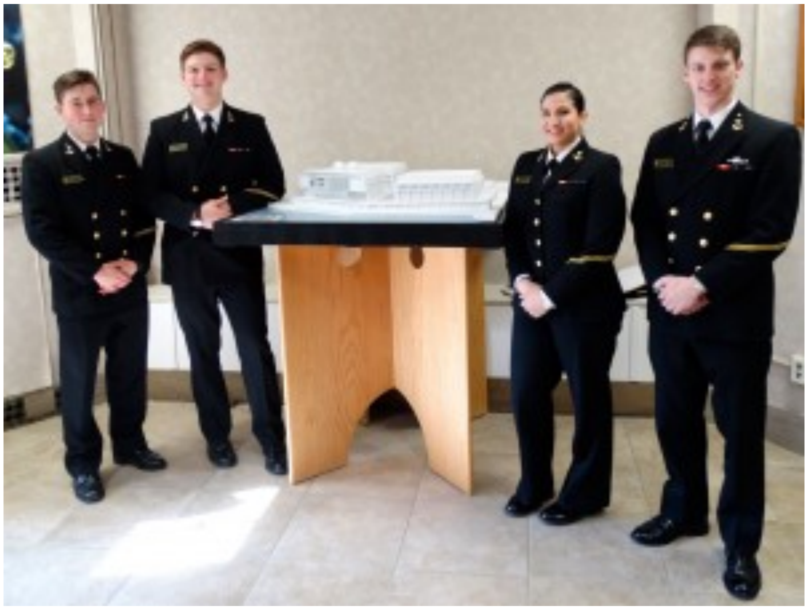
The initial launch class of Cyber Operations majors has 28 students and the sophomore class behind them as 55. The goal is to have 40-60 students per each level, with three sections, which can be managed by two instructors per cyber course.

Midshipmen take 140-150 total credit hours of classes while at the Naval Academy with 15 dedicated courses, or 50 credit hours, in a major as part of those total hours.

Only four of the majors could potentially go directly into Information Warfare openings, with another two potentially into the Information Professional community, while the rest will proliferate into all possible fleet positions, and some could go to fields like Marine Corps Aviation or Navy SEALs. This means that in addition to the basic course work taken by everyone at the Academy, the Navy is looking to proliferate officers with a cyber major throughout the fleet.

And as Captain Tortora put it: “It won’t be long before fleet admirals will want to have with them an experienced cyber officer and team to help them deal with and generate cyber effects as part of cyber operations.”

The four midshipmen who participated in the roundtable had a wide variety of interests and backgrounds and illustrated that the approach being taken to prepare for cyber operations was not narrowly technical.


The four Midshipman Majors interviewed at the Center for Cyber Security Studies, US Naval Academy. Credit Photo: Second Line of Defense

Sitting in during our interview with Capt Tortora were four members of the Class of 2016.

All are 2/C and will be among the first to graduate with a major in Cyber Operations. The Midshipman were, Zachary Dannelly, Erin Devivies, William Young, and Max Goldwasser.

Because all Midshipman participate in athletics one was a competitive swimmer another played Squash a third was the Brigade Heavy Weight Boxing Champion, and Midshipman Devivies throws the Javelin for the woman's track team. She is the proud daughter of two career enlisted Marines. Additionally, all four qualified as shooting "expert" on the range with both the pistol and rifle.

As one midshipman put it: "IT builds the car; Cyber Operators drive the car. I want to drive the car."

Obviously, there needs to be technical proficiency and competence, but one Midshipman was thinking about becoming a history major, another a Chinese major, and they felt that these interests could be met by dealing with the social, policy and legal dynamics of cyber operations.

These are not folks headed down the path of firewall technicians; but rather participating in military operations, which will subsume cyber operations. And the graduates from the Naval Academy as cyber operations majors will form, in the words of Captain Tortora, “a bow wave of young officers coming into the force that will force change more broadly in the Navy.”

We proposed that the process is similar to the ground forces coming out of World War I with the coming of the tank, and that the tank had huge impact on concepts of operations. Captain Tortora commented: “The concept of change is good but it is more like the combustion engine changing warfare rather than the tank. The Navy did not stand up an Aviation Department at the Academy until AFTER World War II. What we are doing here is trying to get ahead of the curve.”

The course is so new, that the process of accreditation by ABET can only happen after the first class graduates, but the staff is working to try to ensure accreditation by ABET.

ABET is a non-profit and non-governmental accrediting agency for academic programs in the disciplines of applied science, computing, engineering, and engineering technology. ABET is a recognized accreditor in the United States (U.S.) by the Council for Higher Education Accreditation.

A key challenge in shaping a Center on Cyber Operations is to be able to attract staff and to try to keep graduates in the Navy after their obligatory period will be over.

Of 60 or so PhDs who received their degrees last year in cyber related fields only a handful went into academics. This means that the Academy will take flexible approaches to appropriate staffing, drawing upon visiting professors, and other ways to bring in the kind of practitioners who would both contribute to and benefit from the dynamic and highly interactive environment Captain Tortora and his team have put in place.

In short, it is not surprising then that the U.S. service academies are standing up cyber learning approaches in their curriculums and setting in motion and educational revolution for the digital warriors coming to the force.

But the US Naval Academy is certainly at the cutting edge of these efforts, and has set in motion an approach designed to prepare the future

Marines and Naval officers who are trained at the Academy for both sensitivity to and understanding of cyber operations.

Editor's Note: The video seen earlier in the article provides the CNO's perspective on cyber operations as published on October 28, 2014.

Shipmates,

Recently I visited Navy Cyber Forces Command in the Hampton Roads area.

After holding a great All Hands Call with our cyber warriors and reenlisting some motivated Sailors, I sat down with two Shipmates to discuss what our cyber forces do and why their mission is important.

In this episode of "Conversation with a Shipmate," we discuss cyber security and warfighting.

Understanding Cyber

All of us, not just cyber warriors, need to understand the role that cyber security plays in our everyday operations.

Electromagnetic Spectrum

The Electromagnetic spectrum is also a hot issue for our Navy, and the exploration of that focus area goes hand in hand with what we're doing on the cyber warfront.

Warfighting on the Sea and in Cyberspace

The Navy is has an inherent and unique need to combat cyber threats.

Our resources, ships and bases around the world are connected by the very networks our cyber warriors defend.