Don't Give Up the Computer

By Joe Moreno '93

How do you defend yourself when you don't know you're being assaulted, surveilled or disrupted? Your doors are locked, the windows are shuttered and everything is quiet, yet you are under attack. During World War II, as the battlefield extended into the sky, the Commandant of the Marine Corps changed the fourth line of the Marines' Hymn from "On the land as on the sea" to "In the air, on land and sea." Earlier this year, the current Commandant of the Marine Corps, General Robert Neller, USMC, stated that the present day battlefield has expanded yet again. He speculated that tomorrow's fight will include "conflict across five domains: land, air, sea, cyber and space." But the challenge with cyber warfare is it doesn't exist in the visible world.

We knew we were attacked at Pearl Harbor. We knew we were attacked on 9/11. But cyber warfare is vastly different. How do we defend against it? Simply protecting critical information isn't enough. How do we defend ourselves in a world where not only our data (content) is at risk, but so is our metadata (context). Metadata is the data that describes our data and it can reveal more than we realize. While data such as the contents of a phone call might be unknown, would you want someone analyzing your phone bill to discover that you called a support group for alcoholics or a suicide hotline at 2:30 a.m.? Given the exponential rise of information we produce

every year, we have seen an increase in industries and governments specializing in finding ways to attack and defend our computer systems.

How do the Navy and Marine Corps prepare for new threats? The same as before, by studying them, including wargaming scenarios in training, executing plans in combat and then reviewing the results. The Navy began taking cyber security seriously in 2010 by reactivating the Tenth Fleet as the force provider for the U.S. Fleet Cyber Command. The Naval Academy is also taking cybersecurity seriously as it has begun incorporating cyber studies into its formal curriculum. All midshipmen, regardless of major, now take two cyber security courses. More telling is that $120 million was earmarked in last fiscal year's federal budget to build the Academy's Center for Cyber Security Studies building, which will be the first academic building constructed since Michelson and Chauvenet Halls were built in 1969.

But what does a cyber warfare curriculum look like? That's what Captain Paul J. Tortora '89, USN (Ret.), is defining. As the director of the Academy's Center for Cyber Security Studies, Tortora said, "Cyber is a bit broader than computer science" as he was challenged with how to look at a new major in the cyber field. The Class of 2016 graduated the first 27 Navy and Marine officers with the new cyber operations major, while 2017 will include 50 midshipmen in the major. In the fleet, these graduates won't find themselves sitting behind a desk. Among the cyber operations graduates, one each will be a SEAL, Marine and EOD officer. Four will enter the submarine community, six will be pilots and two will be NFOs.

The Academy's cyber operations studies also include three non-technical courses, Cyber Law & Ethics, Cyber Planning & Policy, and a course that includes social engineering. Social engineering is a type of attack that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Social engineering frequently uses pretexting, which is a false motive—in other words, lies to obtain privileged information. Deception in warfare goes back before the time of Sun Tzu, but using it to circumvent strong computer security is a new vector.

Malware, a common cyber warfare weapon, is used to attack computer systems. Typical malware can use tools such as worms that are standalone programs or viruses that hide themselves inside legitimate programs like a Trojan horse. In the same manner that an application can be programmed to do most anything, so can malware. Except with malware, the target may never know its computer system was compromised.

Today, computers are no longer standalone devices. They are embedded in nearly everything that uses electricity, from automobiles and televisions to phones and microwaves. What we don't see is that, in addition to these systems housing sensitive information, they also spew out pollution in the form of metadata. Data emissions can be found nearly everywhere, from our searches in Google, to where we travel with our phones, to credit card purchases, both online and at brick and mortar stores. These data emissions reveal more about our activities than we realize. And that's just the metadata we're emitting without knowing it. Sometimes, our metadata is so specific that it can reveal more about us than the data itself. First, consider that even a single piece of metadata could reflect an individual's location, movement, associations, health issues, etc. Then consider that military units are made up of hundreds or thousands of individuals emitting data

Each year the President invites the winners of the Commander-In-Chief's Trophy to the White House for recognition. This year, he welcomed back the Navy football team along with the first class of midshipmen graduating with cyber degrees.

"In a few months, 17 of these seniors [on the football team] will be ensigns and 15 will be commissioned second lieutenants in the Marine Corps," said President Barack Obama. "They will be joined in their service by another historic group of midshipmen who are here today … We are welcoming today the first students ever to graduate from the Naval Academy with a degree in cyber ops. Their expertise is going to be even more critical than ever to our national security. We are very proud of them, and want to congratulate them."

and metadata. On the battlefield, real or virtual, these concerns are magnified as we move between private lives and our secure, classified spaces.

Cyber Hygiene: What can you do to protect yourself?

- Secure your home network, using WPA-2 encryption
- Control who joins your network and don't use your name as the network name
- Don't conduct private matters (banking, healthcare) on free or public wi-fi
- Update and maintain anti-virus software on all devices
- Use firewalls
- Back up data regularly
- Keep your operating system software up to date
- Only download official software or applications
- Encrypt your hard drive
- Turn off your computer and network when not in use
- Don't take USB/thumb drives from strangers
- Don't open attachments or links from unknown senders

Adapted from a presentation by, and used with permission from, Captain Paul Tortora '89, USN (Ret.), director, Center for Cyber Security Studies

Second Lieutenant C.R. Johnston '16, USMC, was a cyber operations major and initially had no intention of majoring in a computer-related field. Johnston, who grew up in Jacksonville, FL, had multiple teachers who had served in the Navy and Marines; two teachers, in particular, introduced the Naval Academy to him as an option after high school. As a midshipman, Johnston initially considered majoring in chemistry with the hope of attending medical school. He changed his mind after taking a mandatory plebe class on cyber security.

Interestingly, Johnston was not a "computer guy" before attending the Naval Academy. "Frankly, I was surprised at my lack of computer education and knowledge. From first grade to 12th grade I had received maybe three computer courses in total. These courses focused mostly on typing, Excel spreadsheets and Microsoft Word. At no point in my educational career, prior to attending the Naval Academy, was 'security' ever mentioned," he said.

How did we get to the point that it seems like technology is getting away from us? Rear Admiral Grace Hopper, USN, who invented the computer compiler and lead the development of the COBOL language, once said, "Life was simple before World War II. After that, we had systems." Her witty wisdom underscores how technology has become increasingly complex in the last century.

A hundred years ago, at the height of the Industrial Revolution, we saw factories spewing out smoke and raw waste. Today, we look back at the reckless pollution and cringe. Perhaps, a century or two from today, people will look back at us and be amazed at how much digital pollution we emitted from our personal lives.

What can we do to protect ourselves and limit our emissions? "Cyber hygiene should start from an early age, like the need to wash your hands and brush your teeth," said Johnston. His comments speak volumes about what cyber security is and is not about. It's not about technology, rather, it's about people—well-disciplined people who have been properly trained.

Bruce Schneier, a leading cryptographer and computer security expert, initially believed that cryptography would solve all of our internet security problems. After writing his first book, "Applied Cryptography," in the early 1990s, Schneier became distraught. He saw strong security broken by weak habits such as "bad programming, a lousy operating system or someone's bad password choice."

What Schneier learned the hard way by seeing computer systems compromised through poor practices, Ensign Zac Dannelly '16, USN, learned in an academic and hands-on environment. Dannelly is 10th generation military and knew that service in the armed forces would be a part of his future. He looked at different majors and saw that most covered areas he found uninteresting. After seeing the cyber operations major he said, "it offered both the coding and physical systems classes that interested me and tied them together in an interdisciplinary approach. It additionally explored the human elements of why we build things the way we do and the greater implications of those creations."

Learning isn't limited to the classroom. Cyber operations majors also spend their summer "cruise" training blocks interning at the National Security Agency as well as civilian corporations such as Microsoft, CACI and Booz Allen Hamilton.

The cyber security skills learned from high-tech corporations transfer well to military operations since there is little

"Cyber hygiene should start from an early age, like the need to wash your hands and brush your teeth."

—2ndLt C.R. Johnston '16, USMC

difference between military and civilian IT computer systems.

In conventional warfare, defenders have the advantage. Think of how well protected the White House is against a physical attack. Online, in the cyber world, the opposite is true. It is nearly impossible to protect a computer that's connected to the internet from every possible attack. Part of this is due to the fact that our networked computers are specifically designed to spread information, not contain it. With a valid login and password, a computer cannot easily distinguish between a U.S. military officer or a hacker from North Korea. While there's an arms imbalance between people and governments in that a private citizen may own a rifle while a government may own a tank, the tool used to carry out a cyber attack is a computer with an internet connection, or simply a smartphone.

Attacks in cyberspace are different than attacks in the physical world. In the physical world, attacks are about moving atoms. In cyberspace, attacks are about moving electrons in such a subtle way that one cannot easily tell the difference between friend or foe. Generally, hackers aren't looking to sabotage a computer system (server). That's an attack that has yet to be successful on a large scale. Rather, hackers want to monitor or copy information on a computer and usually accomplish this without anyone knowing. After all, how would you know if someone was accessing your computer at this very moment? We think of hacking computer systems as people attacking them as in traditional warfare. But the current state of international hacking is more like spying than attacking, neutralizing or disabling. Cyber spying, like traditional intelligence collection, happens during peacetime as well as wartime. So far, we haven't had belligerent nations physically attack each other, on a large scale, in cyberspace. But this type of attack isn't hard to visualize; imagine an enemy neutralizing our GPS satellites.

"Think of all the stuff we do that requires space-based, satellite-based communications: GPS, munitions, precision," said General Neller earlier this year. "If you were to lose that, what would that do to the way you thought you were going to fight?" Without GPS, not only would an Uber driver not be able to pick up a passenger, but airplanes would have to resort to radio beacon navigation. What's more, and often overlooked, is the timing synchronization from GPS satellites that the military relies on. While a pilot can still navigate a plane without GPS, military hardware without GPS or internet connectivity can be very susceptible to time drift, where internal clocks fall out of synchronization. One may think that building more precise timing circuits could solve the problem, but it's not that simple. GPS satellites are designed to include the relativistic effects of Einstein's special theory of relativity, yet nearly all hardware built to rely on GPS for timing is not that sophisticated.

One of the most publicized cyberattacks between multiple nations occurred in 2010 when a cyber weapon called Stuxnet was covertly deployed to sabotage Iran's nuclear program. One can only speculate on how the worm was delivered to the target system, resulting in the destruction of an Iranian centrifuge that was processing uranium. Did a spy sneak into an Iranian laboratory to install the worm? Or was it more clandestine such as an Iranian engineer purchasing a USB mouse that had been hacked to install the Stuxnet worm once it was plugged into a computer controlling the centrifuge?

As Johnston points out, "the current feeling among internet and computer users in the United States seems to be that there is protection in numbers. I believe that the 'I am of no interest to hackers' and 'the likelihood of me being affected is so small' are common misconceptions." Security through obscurity is a dangerous proposition.

It seems the only way to be completely safe from cyberattacks is to not rely on anything digital, an impractical expectation in the 21st century. In the meantime, the Naval Academy tackles the problem head on, moving forward with construction of a new academic building, expanding its programs to counter a new threat and preparing midshipmen to engage cyber attacks directly, in the invisible territory linking all of us. ⚓

Joe Moreno '93, a former software engineer at Apple Inc., currently gives speaking engagements to businesses on Apple's design and marketing philosophy.