TALES OF AN SSC ATLANTIC CYBER WARRIOR

One Man on the Front Lines of America’s Cyber Wars Fights Every Day to Stay One Step Ahead of the Enemy

Space and Naval Warfare Systems Center Atlantic
OVERVIEW

Red teams test the U.S. military and defense establishment’s cyber infrastructure as an enemy would to find loopholes, weaknesses and areas for improvement. This is the story of Jason Jurand, the leader of Space and Naval Warfare Systems Center (SSC) Atlantic’s Red Team.

Space and Naval Warfare Systems Center Atlantic - Charleston, SC
Public Affairs Contact: Jack O’Neill - john.oneill1@navy.mil; lonnie.cowart@navy.mil

Prepared for BEST by
THE CENTER FOR HOMELAND SECURITY AND RESILIENCE

Submission Date
March 23, 2018
Something told Jason Jurand he was on the wrong career path. It was the late 1990s and Jurand was doing basic computer networking and troubleshooting at home in South Carolina.

But Jurand, who currently works for the U.S. Navy’s Space and Naval Warfare Systems Center (SSC) Atlantic in Charleston, SC, says he always wanted something more. Growing up, when he wasn’t playing soccer, Jurand says he spent all his time on computers. That passion followed him into adulthood. He studied pre-med as an undergrad and considered medicine as a career before eventually backing away.

Then Jurand changed gears.

He started looking more closely at the government, in particular at the intelligence community. He interviewed at the CIA, but instead took a job as a contractor at the National Reconnaissance Office (NRO), a government entity that primarily uses satellites to collect vast amounts of data for use by the military and intelligence agencies to support everything from anti-terror and organized crime missions to research about natural disasters and global warming.

He switched jobs a few more times, moving from the NRO to the Defense Intelligence Agency (DIA), where he got his first taste of the world of cybersecurity, he says. It was the late 90s, and by 1999, on the cusp of the Millennium Y2K computer virus threat to the world’s networks, Jurand had transitioned once again, this time to the Pentagon supporting the Army and the Pentagon Reservations Network, where he helped establish their cybersecurity team.

He stayed there for a few years. As the Assistant Manager responsible for incident response activities and one of the Pentagon’s original cyber team members, Jurand was thrown into delicate situations quickly. In the spring of 2001, a U.S. Navy signals reconnaissance aircraft and a Chinese fighter aircraft collided, resulting in what Jurand calls a “cyber skirmish.” It was a term he’d become intimately familiar with in the coming years, but at the time, it was new territory.

The incident was sparked by the collision of a U.S. Navy EP-3E Aries II aircraft, with a Chinese F8 fighter. It unfolded about 50 miles southeast of China’s Hainan Island, in the South China Sea. The American plane, based out of Japan, made an emergency landing on Hainan, where the 24 crewmembers were held for 10 days.

As the Pentagon’s Information Assurance Manager for the building’s computer network, Jurand saw the skirmish from the inside. Long before the era of fake news, Russian hacking conglomerates and open-sourced leaking organizations like WikiLeaks, computer savvy professionals like Jurand watched an incipient cyber warfare landscape evolve in real time. With the American aircrew still held inside China, American and Chinese hackers were going to town against each other, “defacing each other’s web pages,” Jurand says. The goal: to disrupt and unnerve the enemy in the cyber world as much as possible, in the hopes that it might translate into leverage in the physical world.

“The military, the Pentagon, commercial outfits, the sky was the limit,” Jurand says, “And it brought to light that maybe the Defense Department needed to have a better kind of cyber response system in place.”

Eventually, the Chinese conflict was resolved, and the American aircrew returned home safely, but the incident left Jurand more resolved than ever that the cyber skirmish he’d just witnessed was just a harbinger of more to come, he says.

At that time, cyber security programs across the Defense Department were still “emerging from the primordial sludge,” Jurand says. He was vacationing in Paris during 9/11, waiting in line to ascend the Eiffel Tower, when a hijacked jetliner struck the Pentagon. Twenty percent of the building was gone, and with it, 20 percent of the Pentagon’s network.
Jurand’s team worked on the side of the building opposite of where the plane struck, and as a result, “we had no idea anything had happened until we lost network activity,” he says. As the news started to trickle out, Jurand says he learned along with everyone else. Back at his hotel later that night, he started trying to get in touch with his network via a call chain. It was a slow and laborious process, he says, and it would be a lesson for him in the years to come.

**Cyber Warrior**

Jurand kept developing his skill set. He returned to the DIA in a government civilian job as a cyber threat analyst. While there, he got a peek into the cyber habits of the enemy. The war against Al Qaeda in Afghanistan had yielded a treasure trove of data from terrorists who often kept elaborate plans stored on laptops. When U.S. troops seized those computers, the intelligence flowed. And along with things like maps, communications, inventories and other key data points, terrorists often used their computers for more personal ends.

As these and other threats morphed and evolved, Jurand’s ambitions as a cyber warrior grew in tandem, he says. After stints at the DIA and elsewhere, he went back to school and earned a Master’s Degree in computer fraud and forensics investigation, at George Washington University in 2004.

Jurand began to study how cyber threats were evolving, which countries had the ability to affect the critical infrastructure of the United States, and what their motives might be. He pored over reports from the National Intelligence Council, which is the primary source for the entire intelligence community’s long-term analysis as well as its bridge to policymakers in Washington.

He reviewed the literature diligently, he says. He’d become a senior intelligence analyst, and was helping represent the DOD on cyber issues to the rest of the

*Space and Naval Warfare Systems Center (SSC) Atlantic employee Jason Staker conducts a cyber forensics examination on a computer hard drive. Staker works in the Digital Media Criminal Forensics Investigations Laboratory at SSC Atlantic. (U.S. Navy photo by Joe Bullinger/Released)*
intelligence community, which meant attending briefings alongside the CIA, the Treasury Department, the FBI, the Department of Justice and a host of other agencies.

“I got to know what our adversaries were like pretty well,” Jurand says. He was also learning that when it came to cybersecurity, the best defense was understanding the adversaries’ offense.

“If you’re going to play defense, you have to have an appreciation for what the opponent’s offense is going to do to you,” he says. “You have to know something about your adversaries.”

It was, in an important way, a key lesson taken straight from the playbooks of the older generation of spies. He was learning that you couldn’t bludgeon your enemies with weapons alone, he says. You had to learn to think like them, understand them, and adopt their ways and their methods. To beat them, he says, you had to become as much like them as possible without crossing the line.

“The more you know about the bad guys, the wiser you are going to be,” he says. If the Navy was starting to pivot toward the Arabian Gulf, for instance, you might want to start to be more interested in that area, too.

**Growing Threat**

Cyber threats are mounting and becoming increasingly sophisticated. In 2012, Saudi Aramco, the world’s largest oil company, was hit with a cyberattack that destroyed tens of thousands of computers. The breach was so bad that the Saudis tossed their entire network and started over.

According to the recently released Worldwide Threat Assessment of the U.S. Intelligence Community, cyber threats lead the list of global threats. “The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected— with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits.”

The assessment also notes that, “Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations.”

“If hostilities commenced, it could lead to a cyber Pearl Harbor,” Jurand says. “People are talking a lot about how bad things can happen, and who is responsible.”

Today, much of his work involves a kind of pre-emptive strategic thinking — deducing what the cyber threats of the future will look like based on trends, demographics and the daily news cycle.

“Part of this job is grappling with the general evil of being connected to the Internet,” he says. “You can make a lot of money off this stuff that we’re protecting.” He points to the aging Chinese population. “There are countries that would kill to have access to western medicine,” he says. “Health care related research is valuable. So, we have to worry about that.”

Jurand moved to SSC Atlantic in 2006 as a contractor and to a government position in 2009 becoming a key player in developing the organization’s red team.

The U.S. military and defense establishment use red teams to test cyber vulnerability. Red teams deliberately go after an organization’s cyber infrastructure, as an enemy would, to find loopholes, weaknesses and areas for improvement.

While the concept of red teams has been around for decades, their practical use in the military and intelligence establishment increased dramatically after the September 11th attacks. The U.S. Army established its red team in 2004, known as the Army Directed Studies Office.

**‘Sharp and Shiny’**

Teams across the DOD require certification by the National Security Agency, and can only be accredited by U.S. Cyber Command. It can be a long and laborious process, Jurand says.
“Our ability to defend is demonstrably better,” says Jurand. “It keeps the edge sharp and shiny. We’ve gotten so much benefit about building this capability, but it’s hard to keep an adversary out and if you can find them, and converge on them really fast, that’s a good day at the office.”

Jurand views the hacking threat as a disease, he says. You know you’re sick, he says. You’ve got symptoms, and there’s even treatment but, like cancer, you never really know if you’ve gotten everything.

“How do you know if you’ve got every account they had access to?” he asks. “It’s like proving a negative.”

Under Jurand, SSC Atlantic’s Charleston, South Carolina-based red team of about 13 government personnel is at the forefront of cyber defense. Due to SSC Atlantic’s contracting strategy the team can surge as needed utilizing authorized industry partners while maintaining government oversight.

SSC Atlantic has worked for military and medical organizations since the early 2000s, installing firewalls, intrusion detection systems and caching to provide network protection. Around 2005, military health systems began providing encryption services between 100 or so main hospitals to more than 500 clinics via small firewalls devices. After several years of applications and complex accreditation procedures, the National Security Agency finally gave SSC Atlantic a red team accreditation in 2014, making it one of only nine such teams nationwide.

“That accreditation makes us eligible to do assessments anywhere,” says Jurand. “The authorization letter differentiates what we do from illegal hacking. It gives us authorization to do these assessments. On the legal side of things, it is how we know we’re a good guy. No one wants to deal with accusations of impropriety.”

Some adversaries have a taste for medical information, Jurand says. DOD has invested $4.3 billion in the Military Health System Genesis program, a public private partnership that will control some 9.4 million DOD health records spread across a series of hospitals.

SSC Atlantic has been asked to do the organization’s security assessment.
TOGETHER, WE’RE INVENTING THE FUTURE

DoD LabS

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA