

Fleet Highlights

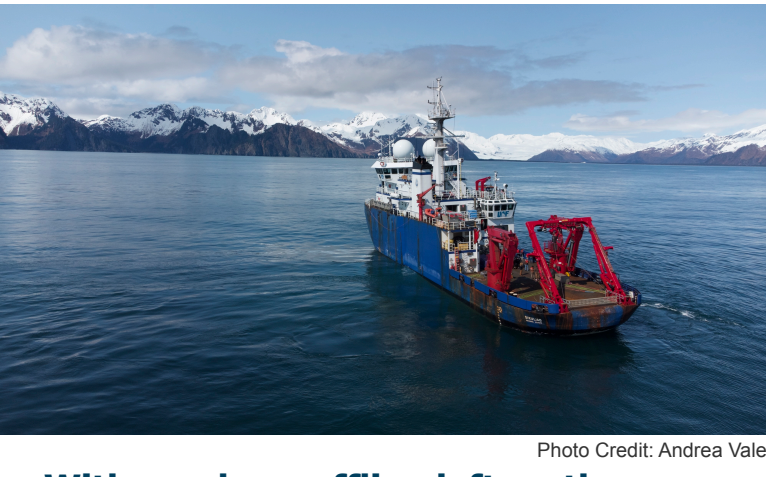


Photo Credit: Andrea Vale

With nowhere offline left on the map, what does it mean to be secure at sea?

R/V *Sikuliaq* Cyber Cruise - Written by Andrea Vale

Just a few years ago, “marine cybersecurity” was an oxymoron — once ships left port, they were off the grid. But as information technology develops, no matter how far out to sea research vessels travel, they’re constantly on. And with increased connectivity comes increased risk.

“Before, cybersecurity was a bit of an afterthought, because the vessel could be considered offline,” said Julian Race, IT Manager for [R/V *Sikuliaq*](#). “It’s what we call air gaps. There’s no way to get from the internet to the vessel. Now there’s constant connectivity. There are more bad actors out there, and vessels have more and more risk, because they are connected all the time. We really have to pay attention.”



Marine Technician Tyler Peterson observes some of the many monitors working in real time in the computer lab aboard R/V *Sikuliaq*

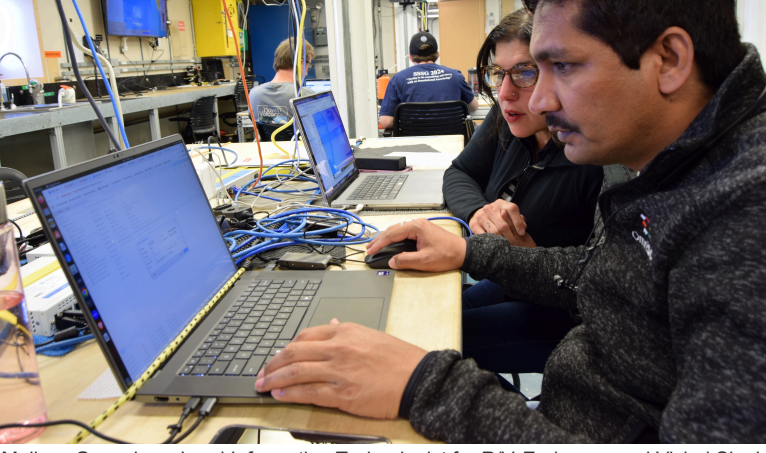
Photo Credit Andrea Vale

While cybersecurity on land may follow standard protocols, when at sea there’s an entirely new set of concerns, limitations and considerations to take into account. For instance, Race pointed out that during onshore cybersecurity attacks, hackers generally block access to various crucial systems, whether an individual’s bank account or an entire hospital HVAC. In these cases, it’s possible to simply shut down the threatened system and bring operations to a halt to prevent further damage. But at sea, that’s not exactly an option.

“These days, more and more vessels are becoming computer controlled,” Race described. “So if an attacker were to target a ship and potentially gain control or shut down critical systems, the vessel could be, as we say, ‘dead in the water.’ It is not out of the realm of possibility that an attacker could literally drive a ship off course and cause an accident or run her aground. So cybersecurity at sea is really important because it’s not just monetary loss that you might experience. It could be loss of life, loss of property, damage to critical infrastructure.”

Race, who oversees all cyber systems in use aboard R/V *Sikuliaq*’s research operations, noticed that *Sikuliaq*’s “transit” cruises — which are usually void of science parties, and simply aimed at getting the ship from one port to another quickly — left valuable berth and lab space open. He had the idea to use these transit periods as opportunities to train professionals in a variety of maritime skills.

That’s how the Sea-based Education for Advanced Cybersecurity Understanding and Research Experiences in IT (SECURE-IT) came to be. From April 9-20, *Sikuliaq* hosted the second iteration of a training cruise focused specifically on exploring the unique challenges and opportunities of the rapidly-developing marine cybersecurity field. While *Sikuliaq* made its way from Honolulu, Hawaii, to its home port of Seward, Alaska, 22 professionals across the IT and marine technology fields joined together to share ideas and learn from one another.



Melissa Gonsalves, Lead Information Technologist for R/V *Endeavor*, and Vishal Singh Bhardvaj, a security analyst at OmniSOC, discuss how to build a FortiGate system for

R/V *Sikuliaq*.

Photo Credit Andrea Vale

“My goal was to try and fill the boat with people who don’t normally get to go to sea, and really understand what it takes to run a modern research vessel out at sea,” Race said.

It was particularly important to give IT professionals who support vessel operations, but who don’t typically get the opportunity to sail, the ability to go out to sea and better understand the challenges faced offshore. That hands-on experience can illuminate why policies that work at onshore institutions may not translate well to offshore research vessels (for instance, Cloud-based programs aren’t nearly as helpful at sea, where it is difficult to connect to Cloud systems.)

“Generally, on vessels like this, bunks are at a premium,” Race said. “So there’s never an opportunity for the more IT-focused people to come to sea and experience it.”

Topics covered during SECURE-IT included everything from cyber hygiene to updating legacy systems to security crisis protocol. Besides listening to others speak on their topics of expertise, participants had the opportunity to get hands-on training in up-and-coming programs like FortiGate firewalls, 3D printing, and data-collection systems.



There is a unique set of cybersecurity concerns while aboard a research vessel at sea that may not apply back on land.

Photo Credit Andrea Vale

There was also an emphasis on giving students and early career professionals the opportunity to broaden their understanding of what an IT career can encompass, and introduce them to possibilities of working at sea. The cruise hosted five [STEMSEAS](#) students — all studying in the cyber field — as well as a [UNOLS-MATE](#) intern.

“We’ve brought along some undergraduate students to try and encourage them to see that there are more opportunities than just sitting in a cubicle,” Race said. “Be open to different experiences ... There are a lot of opportunities that maybe aren’t obvious.”

UNOLS-MATE intern Raymond James Gallant is now rethinking the possibilities for his future based on his experiences during the SECURE-IT cruise. He is an Information Systems major approaching his senior year at Eastern New Mexico University, with plans to pursue graduate studies. While he has studied cybersecurity in school, being able to apply it in a hands-on experience at sea is crucial, especially because “You don’t have a day-to-day use for [these tools] anywhere else in the world,” Gallant said.

The SECURE-IT cruise has shown students like Gallant that an IT career spent at sea is not only possible, but increasingly needed to ensure that safe marine research can continue for decades to come.

“I think it’s overlooked,” Gallant said. “[*Sikuliaq*] was built in 2014, and cybersecurity wasn’t as prevalent then. Now it’s at the forefront. If you read some of the new documents coming out from the Coast Guard and NIST and other governing bodies, they’re baking cybersecurity into the ships ... Hopefully in the future, we can build these new vessels to withstand changes in technology.”

The ultimate hope is that by bringing together IT and marine technology thought leaders together for experiences like the SECURE-IT cruise, a standard cybersecurity protocol will emerge, able to be shared across the UNOLS fleet. Ideally, roving science parties and marine technicians that work between multiple vessels would have a similar IT infrastructure to work with, making their work easier — and minimizing cyber threats along the way.

“Our goal with this project ... is to make it a more unified experience from vessel to vessel, so that the learning curve is much shallower,” Race said. “That’s just better for everyone all around.”



As offshore connectivity methods continue to expand, participants of the SECURE-IT cruise now have the framework to solve key issues of cybersecurity at sea.

Photo Credit Andrea Vale