National Security Conference Seeks Partnerships in Advanced Autonomous Robotics, Cybersecurity

July 13, 2009

Tiffany Fox

Dan Goldin, chairman and chief executive officer of the San Diego-based Intellisis Corporation and chairman of the event, says the La Jolla Conference on Innovation Support for National Security will be "first in a series that will bring together the leadership of the nation with the incredible capability here in San Diego."

Watch webcast videos of select panels and talks. [*Windows Media Player and broadband connection required; click for information on the latest version, and on players for Mac and Linux users*].

If a recent conference at the University of California, San Diego is any indication, the gap between science fiction and battlefield reality is narrowing faster than a MIG jet fighter in an inverted dive.

The La Jolla Conference on Innovation Support for National Security, held last month at the California Institute for Telecommunications and Information Technology (Calit2) at UC San Diego, brought together thought leaders from the U.S. military, the defense industry and local research institutions to identify challenges, threats and solutions in the areas of advanced autonomous robotics and cybersecurity.

"Recent technological innovations have begun to change the way in which the country will operate and defend against threats, both on the battlefield and in cyberspace," said Duane Roth, chief executive officer of CONNECT, a regional non-profit organization established in 1985 to educate the San Diego region on how to commercialize local research-based discoveries (CONNECT co-sponsored the event).

"San Diego has exceptional research capacity," Roth continued, "and is more than capable of creating and implementing new solutions for our nation's defense."

The conference's four panel discussions and 18 presentations, which were held in Calit2's Atkinson Hall, revealed that autonomous robotics (or 'bots) and cybersecurity are playing an increasingly significant role in U.S. war-fighting efforts around the world. With its history of pioneering technologies and its regional expertise in various defense, robotic and information technologies, San Diego is poised to launch critical new technologies to help the U.S. military conduct more efficient combat maneuvers, prevent loss of life and cope with potentially devastating menace of cyber attacks.

James "Raleigh" Durham, director of Joint Advanced Concepts for Acquisition and Technology for the U.S. Department of Defense, said that advanced autonomous robots and innovations in cybersecurity represent the military's next transformational technologies.

"The world is a very dangerous place," said Dan Goldin, chairman and chief executive officer of the San Diego-based Intellisis Corporation and chairman of the event. "The fact of the matter is, America must be superior to every other nation in the world by having these very, very critical technologies. That really is the genesis of why we felt it was important to have this particular conference, and we hope this is a first in a series that will bring together the leadership of the nation with the incredible capability here in San Diego."

In his keynote address, James "Raleigh" Durham, director of Joint Advanced Concepts for Acquisition and Technology for the U.S. Department of Defense, said that advanced autonomous robots and innovations in cybersecurity represent the military's next transformational technologies and are comparable to the introduction of the personal computer. But, he stressed, any further innovations in these areas must be made affordable.

"Innovation in and of itself is wonderful, but it doesn't get anywhere," Durham said. "All of our challenges are inseparable: We need the 'bots, and the cybersecurity aspect is also becoming more important, but the budget will always be with us. We have to consider the financial outlook, too."

Sonia Martinez, an assistant professor of MAE at UCSD, made the case that future military missions will depend on large, networked groups of sensor-equipped vehicles.

In regard to autonomous robotics, Durham went on to emphasize innovation in three related areas: 1) controlled autonomous operations in unforgiving environments (terrain, weather, threat, distance, etc); 2) artificial intelligence, or learning on-the-job to react quickly in fast-changing tactical situations; and 3) collaboration with other friendly unmanned and manned systems to integrate air, surface and subsurface as circumstances dictate.

"Fully autonomous robotic capability is game-changing," he noted. "But then, we've got to move beyond the 'bot and move toward systems of 'bots. We've got to move to where, in order to perform a function, they do like we do: They collaborate. We've got to move away from the operator controlling all the individual parts to the point where an operator gives the robot a mission and tells it go on."

Engineers at UC San Diego are on the cusp of developing such robotics, as evidenced by several presentations at the conference.

Professor Tom Bewley of UCSD's Department of Mechanical and Aerospace Engineering (MAE) and its Coordinated Robotics Laboratory, demonstrated the advanced autonomous capabilities of several robots. His three-wheeled iHop creation, which resembles a high-tech pogo stick, incorporates a dual four-bar mechanism to achieve forward motion so it can tmake running leaps over obstacles.

Stefan Savage, an associate professor in the Department of Computer Science and Engineering, spoke about his work as director of the Collaborative Center for Internet Epidemiology and Defenses (CCIED), a collaboration between UCSD and the International Computer Science Institute.

The two-wheeled younger "sister" of iHop, dubbed "iLean" can climb stairs by using a specially designed "toe" and "pole" design, while a third version of iHop uses a butterfly maneuver to facilitate hopping.

"Another big military application for robotics is to explore buildings," Bewley added. "By using small cameras and managing data, robots can take pictures of walls and patch them together in a process I call 3-d photo stitching. This creates a virtual reality of a specific room, so a warfighter has an idea of the room she or he is actually going into."

Bewley said his team is also looking into using robots to examine atmospheric plume forecasting to detect chemical, biological and nuclear contaminants in the air.

"We're not just theorizing about this," he noted. "We have a team here at UCSD and at Los Alamos National Laboratory. We're doing flight tests now, leading up to a multi-year project to test these things. We're really looking forward to the synthesis of all these ideas."

Sonia Martinez, an assistant professor of MAE at UCSD, made the case that future military missions will depend on large, networked groups of sensor-equipped vehicles, which can be deployed in extreme conditions with little to no human intervention.

"Inspiration can be taken from biological groups like schools of fish, flocks of birds," she continued. "These will be multi-robot networks, where each individual senses its environment, communicates with others, processes information gathered and takes local action in response."

Yet Martinez cautions that such a strategy presents numerous research challenges, including the need for systematic methodologies and the means for verifying various algorithms, for example.

"We have a collective responsibility to not just come up with good ideas," noted Allan Rutherford, director of UAV Systems for Science Applications International Corporation (SAIC). "The world is littered with good ideas that never make it. Programs die horrible deaths when they get off the path of meeting explicit needs."

"Clearly when we have a single robot, we know what it's capable of doing when it works in isolation," Martinez explained. "But when you put a bunch together lots of things can happen. It's like going from linear system to a nonlinear system, where the group is more than the sum of its parts. How can we calculate those and verify it's going to work?"

In the area of cybersecurity, UCSD's Stefan Savage, an associate professor in the Department of Computer Science and Engineering, spoke about his work as director of the Collaborative Center for Internet Epidemiology and Defenses (CCIED), a collaboration between UCSD and the International Computer Science Institute. With additional support from its industrial partners, including Yahoo, Google, Cisco and Microsoft, CCIED tracks worldwide Internet attack activity and develops fully automated defense systems for both network and host environments.

Savage says that part of the problem with current efforts to combat cyber attacks is that defenders are emphasizing the wrong part of the problem. The real Achilles heel, Savage says, is the profitability of spam and malware campaigns. Although a single spam campaign must send out an average of 12 million spams to get one purchase, that campaign can still accrue about $1.5 million/year in revenue.

"There is a fallacy that many of us in the community have ascribed to that cybersecurity is a technical problem," explained Savage. "In fact, there are a lot of other factors involved and one is this issue of economics. In the last six years, we have seen the emergence of profit-making malware. This has created a platform economy, where the platform is botnets.

"In turn, the economies of scale provided by botnets have made it cost-effective to harness millions of compromised computers to support individual criminal enterprises - including spam, phishing, information theft and denial-of-service." Savage also argued that several "structural asymmetries" make it difficult to fight cyberattacks.

He explains: "For one, defenders are reactive, attackers are proactive. They can be so much more agile because they have nothing invested. The best case we're going to be in is to play catch-up and find yesterday's stuff."

"My premise is that we want to be focusing on the economic bottlenecks, but to do that we need to understand how their business works," Savage concluded. "There are points where you can go on the offense and undermine the economics of this. At the same time, it also suggests that there are better places for defense than others. Rather than defend your host, first defend your e-commerce credentials."

Aside from these significant research challenges posed by advanced autonomous robotics and cybersecurity technologies, scientists and entrepreneurs hoping to come up with the "next big thing" face another significant obstacle along the way: Selling their ideas. Allan Rutherford, director of UAV Systems for Science Applications International Corporation (SAIC) and one of the panel speakers, had a little advice for scientists and engineers in that regard.

"We have a collective responsibility to not just come up with good ideas," Rutherford noted. "The world is littered with good ideas that never make it. Programs die horrible deaths when they get off the path of meeting explicit needs.

"Selling your idea once isn't good enough; you have to keep coming back to your user communities to keep them interested and excited. If you let them drift away, you're toast. Your idea becomes yesterday's news."

But, says Roth, the La Jolla Conference on Innovation Support for National Security demonstrated that progress in both advanced autonomous robotics and cybersecurity is being made, although "there is still much to be done."

"There were many connections made at this event," Roth remarked at the conclusion of the day's discussions. "I'm certain when we meet next year there will be partnerships formed as a result of this year's conference."

Media Contact: Tiffany Fox, 858-246-0353, tfox@ucsd.edu