How AI Can Outsmart Criminals and Improve Society

USC Professor Milind Tambe has been working on AI-based security solutions since 2007. Now he wants to apply that knowledge to help society, from climate change to gang violence.

By S.C. Stuart

Updated April 9, 2018

If you're a fan of heist movies like ÇÐĞùÂķ Õ≈ŗ ú, you're familiar with the scene where the bad guys gather around a map, and the kingpin says something like: "The guards do a security patrol at 05:30 hours. Synchronize your watches. We'll enter here at 05:47 hours. Fingers will disable the alarm before Maxi and her team enter the building via the roof."

Thanks to artificial intelligence, it's a plot point Hollywood can't use anymore, as many security companies now use AI-configured game theory to randomize patrols. The best known is ARMOR, developed by Dr. Milind Tambe, a professor at USC's Viterbi School of Engineering, and in use at locations like LAX.

PCMag met Professor Tambe in his AI lab at USC's Salvatori Computer Science Center to learn more about this, as well as his focus on using AI to address society's ills as co-founder of the USC Center for Artificial Intelligence in Society (CAIS). Here are edited and condensed excerpts from our conversation.

Dr. Tambe, tell us how you got interested in AI as a field of research.
[**MT**] When I was growing up in India, AI belonged to the future, a world portrayed in ĎÂ ŵť I ŵẎ and ĎÂ ŵÇŵĜÏ, and in the science fiction I read, mostly Asimov. In fact, the 60s original series of ĎÂ ŵÇŵĜÏ started playing in India in the 1980s, and I found it fascinating. That was the genesis of how I learned about the field. Then I ended up coming to the US and got my PhD in AI at Carnegie Mellon.

You're now using AI to solve a lot of society's problems, including security issues, with the ARMOR software, which has won many awards.
We have been working with AI for security since 2007. It started here at LAX following 9/11. But terrorist attacks happen everywhere. For example, the train attacks in Mumbai in 2006 brought the issue very close to home for me, as my mother travels on that line. So I wanted to contribute to counter-terrorism, to start to improve security. Our ARMOR software has since been modified to be used by the US Federal Air Marshals (as IRIS) and, as PROTECT for the US Coast Guard for maritime security.

Who funded the original research?
ARMOR was developed in partnership with the University of Southern California through grants from the Department of Homeland Security, Department of Defense, and the US Army Research Office. There are so many federal agencies, with relatively limited resources, and so many areas of the US to protect.

Many of these agencies came to prominence during the Cold War.
Indeed. But we're dealing with very different adversaries now. What is needed today are new, advanced, artificial intelligence operations, such as ours, to randomize and provide highly evolved risk assessment tools.

In 2011, your book—*Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*—was published. Then, in 2013, you co-founded a commercial spin-off of the ARMOR software, into a company now called Avata Intelligence. Avata, which means "open" in Finnish, develops products that bridge the gap between data and decisions. The core technology was developed here at USC, and Avata has taken that work into diverse areas such as public safety and infrastructure, defense, healthcare, global awareness, and social impact. I retain my Chief of Research role there, but spend most of my time here with my PhD students, iterating new concepts in AI to further this field.

What's the tech platform behind the original ARMOR software?
We built the algorithms ourselves, which randomize the security patrols and provide risk assessment scores, none of it is plug-and-play, we can have it up and running within 30 days at a new organization.

Right, and the code layers are probably not available on GitHub either.
[œ ÃþDŸ] No. But it is published research work. I told our program managers at the TSA and Department of Homeland Security, 'If you want this work validated, what better way to get it

peer-reviewed at international conferences by the top people in AI?' The security comes from the obfuscation, the randomizing. We don't hide anything in secret, because that invites break-ins. The strength is that, due to the algorithms, you don't know what's going to happen tomorrow, because the AI hasn't decided it yet.

Are you using machine learning?

We're starting to do that now because there's a growing body of historical data. We assume that the adversary is very strategic, always thinking of [how to] inflict great damage on us. When we go to domains where the loss isn't as consequential as human life, and the adversaries are not as strategic, say wildlife poaching, then we can be more aggressive, and we have much more data on poaching. We can develop models based on exploiting known weaknesses there.

Talking of poaching, you're moving your AI to focus not just on security, but also on social issues.

In October 2013, I attended a joint event hosted by the USC Suzanne Dworak-Peck School of Social Work and the Viterbi School of Engineering. The idea was to introduce social work faculty to new concepts in technology, and engineering faculty—who were interested in social problems—to emerging needs in that field. It was there that I got talking to Eric Rice, associate professor [at the] School of Social Work. Eric's team had just finished collecting HIV risk and prevention activities among several panels of social networks of homeless youth in Los Angeles. We then collaborated to create an algorithm to identify the most efficient peers within a social network of homeless youth.

This then became a formal collaboration?

Yes, we then set up the USC Center for Artificial Intelligence in Society (CAIS). Our mission there is to draw inspiration from the Grand Challenges of Social Work, the Grand Challenges of Engineering, and the United Nations Sustainable Development Goals, and the United Nations Millennium Development Goals, which provide important new directions for AI and social science research. Based on these goals, our initial projects focus on ending homelessness, fighting substance abuse, preventing suicide, improving access to health care, social responses to global climate change, reducing gang violence, and protecting wildlife.

And you've taken the algorithms and machine learning behind the HIV work into other preventable diseases.

We are now heavily involved in using AI for public health, to help allocate the right resource, most recently in at-risk groups for tuberculosis in India.

What's next for you?

This is basic research in early stages, but we're starting to build a qualitative understanding of how gangs function, together with a quantitative response to their culture, particularly with recruitment and radicalization, using game theory to model predictive algorithms and provide a useful response.

Not just keeping LA citizens safe, but also getting inside the gang culture to protect vulnerable youth from recruiting?

Exactly. It's exciting work. Much of AI doesn't leave the lab, in that it doesn't get validated in the real world. So there are hundreds of academic papers which have never been proven in society. That's why we believe the work we're doing is so important. In all of our research and development, using AI for "good domains," whether it's security, social work, public health or poaching, we have empirical data to show that the AI supports professionals in the field and helps them do their jobs more effectively.