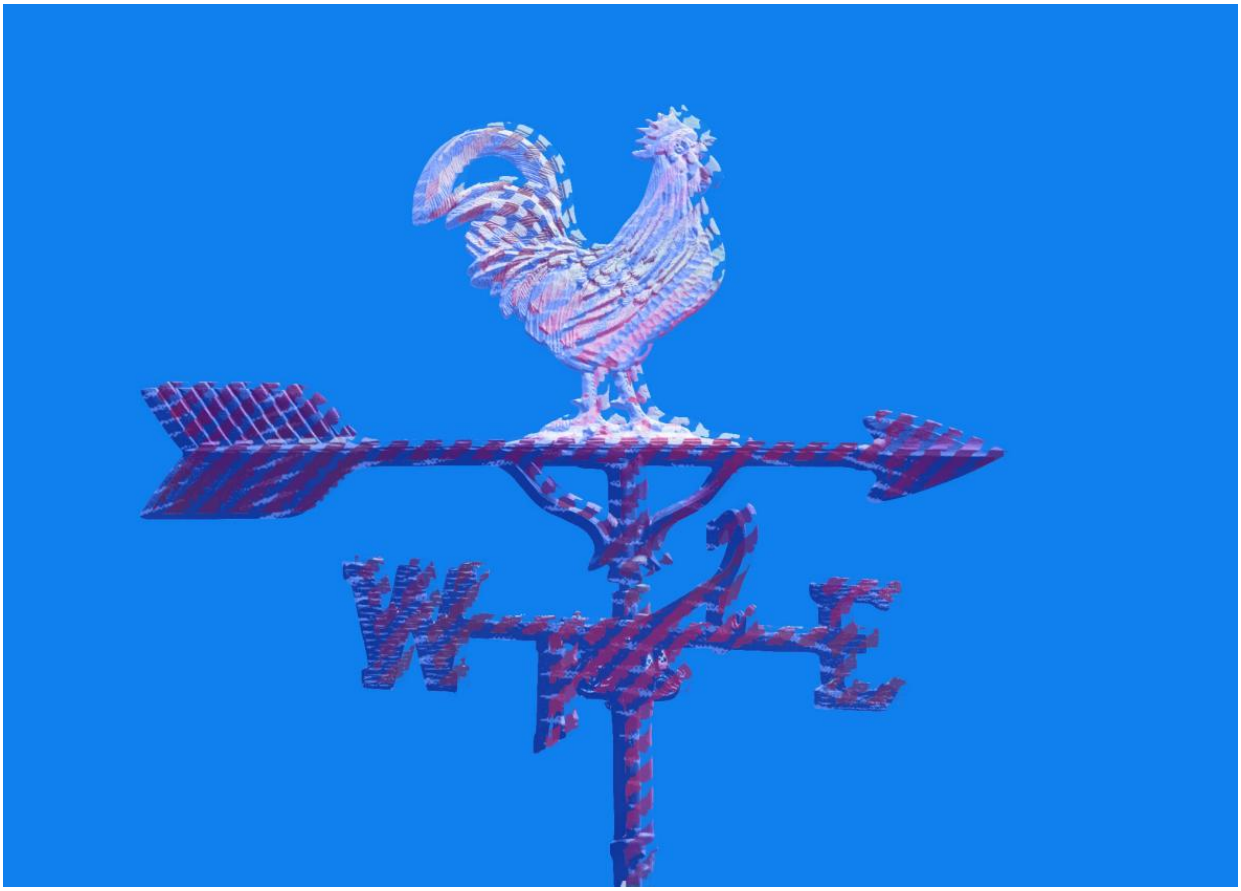
WHAT THE HECK IS THREATCASTING?

To imagine the future, we also need to think about potential dangers.

By Brian David Johnson and Natalie Vanatta



The power of threatcasting comes from the details that arise in looking to the future. Photo illustration by Natalie Matthews-Ramo. Photos by Thinkstock.

Harriet Downs had it all: a great job, a loving husband, and two beautiful children. She was an up-and-coming programmer at Goldman Sachs for the company's A.I. trading bots, on the fast track to management. She; her husband, Steve; and the kids had just moved into a beautiful new house in Sevenoaks. Life was good.

Then one day, on the train into London, a man with the lion tattoo on his neck stopped her and showed her a video. The video. She recognized the people on the screen. One of them was her. She remembered the terrible mistake she had made that night. Too much

to drink. Too much stress at work. It was never going to happen again. But somehow the man had gotten the video, knew everything about her life, her habits, her family, her work. And he wanted something. It was just a simple piece of code that needed to be inserted into the bots at work. No one would know or understand why the A.I. was selling millions of shares all at once. Yes, the markets would collapse. But just for a split second—long enough for the man's "friends" to make billions by shorting the stocks. Standing on the train, Harriet had a decision to make. If she said no, she would have no family, no job—nothing.

There is, of course, no Harriet Downs. But these sorts of near-future scenarios—rich with detail and fully drawn characters—can be a powerful tool that might help us prepare for uncertain tomorrows.

The device is called a science-fiction prototype, one of a range of tools used in threatcasting—a conceptual process used to envision and plan for risks 10 years in the future. By imagining future narratives in which organized criminals, terrorist networks, or state-sponsored adversaries could deploy technology, people and organizations can better plan for how to counter the risks they pose.

Threatcasting emerged in 2007 as a variation on the futurecasting process that one of us, Brian, created when working as a futurist and trying to imagine what individuals would expect from their technology products in the future. Threatcasting is also a descendent of scenario planning, a tool that allows organizations to image a range of possible and probable futures based upon overlapping forces or trends. Imagine you're a car company that envisions the possible futures of gas prices and the unemployment rate. If gas prices rise and unemployment falls, what might your sales look like? But what if both gas prices and unemployment rise? From these basic components, you can develop specific scenarios for your company and plan for them.

Scenario planning and other more traditional forecasting tools are necessary but not sufficient for the 21st century. Scenario planning can illuminate multiple futures, but it lacks specific details as well as clear actions that your organization could take. It presupposes that the future is fixed around specific parameters and that you or your organization has no control over your future. Traditional scenario planning assumes only two main driving forces will affect the future and that you will have limited control over them. For instance, scenario planning for the nuclear power industry might assume that the two driving forces would be a shift in the social/political environment and the evolution of technology. Each of the two forces could go more positive or negative, resulting in four potential views of the future. But what if the future is not on the extreme

ends of these forces or if regulation ends up being a game-changer? …. Then the industry isn't prepared.

The power of threatcasting comes from the details that arise from the narrative approach and the actions it specifies an organization can take. Threatcasting offers a framework and process to combine a wide range of inputs and exercises to imagine a broader range of future threat events. It also provides a systematic process to backcast (that is, look backward from the imagined futures), to understand the steps needed to disrupt, mitigate, and recover from these future threats.

We both work with Arizona State University's Threatcasting Lab, whose mission is to use threatcasting to envision futures that empower actions. (Disclosure: ASU is a partner with Slate and New America in Future Tense.) Twice a year, ASU's Threatcasting Lab gathers people from the military, the federal government, private industry, nonprofits, universities, and trade association to help identify and model potential dangers.
The session begins with short video presentations from experts in social science, technology, economics, cultural history, and other fields. They explore their top concerns and most recent work. The forecasted threats could be technological, cultural, or economic. Could a complex automated supply chain, run but artificial intelligence and drones, be hacked by terrorists to destabilize a city? What are the dangers of computer software that is so complex that no single human can understand or repair it? Will rising global income inequity undermine the nation's ability to innovate and compete? Threatcasting cuts through what can sometimes feel like hopeless uncertainty about tomorrow.

Then, working in small, collaborative groups, they construct a story set 10 years in the future. They imagine characters like the London-based Harriet Downs, a commodities trader living a "normal" life in 2027. (In fact, Harriet's sad tale comes from one of our collaborations with the U.S. Army Cyber Institute and was designed to envision coming hazards posed by weaponized artificial intelligence.) They imagine their relationships, families, jobs, and communities. Then they inject one of the forecasted threats. Perhaps it will target the character directly (as with Harriet), or the character could implement it for their own use. The group then develops a science-fiction prototype by imagining how the conflict might unfold, exploring its reverberating consequences in detail. One of the unique strengths of the threatcasting process is the details and raw data generated about each threat.

The threatcasting process might generate only negative visions if we stopped here. However, the group then use the science-fiction prototype to explore the factors and

events that led to the threat. This helps them think more clearly how to disrupt, lessen, or recover from the potential threats. From this the group proposes short-term, actionable steps to implement today to nudge society away from potential threats.

For instance, Harriet's story of future surveillance and coercion can help corporate chief security officers become more aware of insider threats and develop stronger HR practices for compromised employees and more robust engineering practices for the development of A.I. It can be difficult to convince management to commit resources today for something that may or may not happen in years to come. But reading a threat future and its consequences in vivid, visceral detail makes those investments feel much more pressing. For example, an HR manager reading Harriet's story might realize that she needs to implement a safe, unthreatening way for employees to report criminal activities. At its best, threatcasting cuts through what can sometimes feel like hopeless uncertainty about tomorrow, leading to more pragmatic approaches.

Other organizations, too, have begun using threatcasting to peer into the threats of tomorrow. Earlier this year, Cisco Hyperinnovation Living Labs brought together a cohort of industry giants representing about $500 billion in supply chain value—including Citi, DB Schenker, GE, and Intel—for a two-day summit to identify future industry pain points and rapidly prototype various countermeasures. To introduce the group to the possible future threats they wanted to address, CHILL released "Two Days After Tuesday," a science-fiction prototype derived from one of our reports. The prototype imagines a futuristic state-sponsored terrorist attack using smart refrigerators and pantries that place excessive dairy and produce orders to a complex automated supply chain. With the roads and ports now clogged, the terrorists exploit a weakness in the Red Hook, New Jersey, port system to sneak a dirty bomb into the country and detonate it in downtown New York.

Two Days After Tuesday
Cisco Hyperinnovation Living Labs

“People aren’t wired to imagine the future, 10 or even five years out, which is a blocker to innovation,” Kate O’Keeffe, senior director of CHILL, said in an email. “We need to create that world for them, so they can immerse themselves in this future scenario, making it immediately apparent what kind of solutions we need to prepare for that future.” Four out of the five concepts from the CHILL event received on-the-spot funding from the assembled cohort of companies.

Threatcasting is also influencing the work of the U.S. Army Cyber Institute, a military think tank tasked to prepare for near-future challenges the Army will face in the digital domain. With the rapid pace of technological change and a highly complex, networked world, there are near-infinite potential challenges to explore—so the institute turned to the threatcasting process to inspire a portion of its more focused research portfolio. Threatcasting is a powerful way to uncover and identify future threats, but it only works if the people who participated in the exercise take the next step. They are the ones who have the training and institutional knowledge to bring out the changes and investments needed to disrupt, mitigate, and recover from these futures. Additionally, no one organization can fully take these actions. Just as in the workshop, security professionals and researchers need to collaborate across industries, disciplines, and borders to be most effective.

However, threatcasting can't illuminate all threats we will face in the future. First, our sessions are scoped to focus not on the entirety of the future but in specific areas that thought leaders are concerned about. They are based on focus areas where we believe there is not enough active research. This scoping means we can't anticipate all threats. For instance, we don't include the discovery of sentient life in the galaxy in our threats, because it seems so unlikely. So if that happens in the next 10 years, our work will not help illuminate the resulting second- and third-order effects of that threat. Furthermore, the resulting raw data and visions of the future are inherently limited by people's imaginations. If no one can possibly imagine a threat, then we can't 'cast it. If we had performed a threatcasting in 1935, it is doubtful that we could have imagined that sheer destructive power of nuclear technology, new delivery mechanisms, and a change in national will would, together, lead us to anticipate the atomic bombs that killed hundreds of thousands of people in Hiroshima and Nagasaki in 1945.

There are things we know about the future. Over the next 10 years we will see the rise of artificial intelligence. Robots will become an everyday part of our lives, and we'll see autonomous vehicles on land, sea, and air. What threats do you see coming in this tomorrow? What stories would you tell to keep us safe?

This article is part of Future Tense, a collab

ALIDA DRAUDT
The Futurist Industry Is Overwhelmingly White and Male

JULIA ROSE WEST
The Real Moneyball Effect: Our Fetishization of Data

JACOB T. SWINNEY
How the Depiction of the Future Changed in Movies Over 80 Years

HEATHER SCHWEDEL
Psychics Didn't See the Internet Coming. Now They're Getting Into the App Biz.

KEVIN BANKSTON
Tech Policy and Sci-Fi Collide at a Weird and Wonderful Convention

ANNALEE NEWITZ
How to Write a Novel Set More Than 125 Years in the Future