



Envisioning the Future to Empower Action

Natalie Vanatta, Army Cyber Institute

At a threatcasting workshop, participants imagined tomorrow's threats and identified concrete steps we can take today to mitigate them.

FROM THE EDITOR

Arizona State University's Threatcasting Lab (threatcasting.com) recently brought together diverse practitioners to envision possible threats 10 years in the future and determine what we might do about them today. —Brian David Johnson

A single tweet brings about the end of the world as we know it. It sounds highly implausible, but in 2027, it could be our reality.

Threatcasting Workshop West 2017, which was jointly sponsored by the Army Cyber Institute and Arizona State University, aimed to provide new clarity about tomorrow. In early May, 47 participants from diverse organizations used threatcasting to create 22 futures regarding complex issues: the advancement of AI, the diminishing ability to conduct covert intelligence gathering, the growing complexity of code, the future division of work roles between humans and machines, and more. *Threatcasting* is a conceptual framework that allows public, private, and academic multidisciplinary groups to envision and plan against future threats. Through this process, we not only described tomorrow's threats but also identified specific actions, indicators, and concrete steps we could take today to disrupt, mitigate, and recover from these threats.


Imagining life 10 years out was freeing. We weren't limited in our thinking of how technology might evolve, our society might morph, and the world order might shift. We wove compelling narratives about the risks of inaction over a decade in hopes of driving investment into underlying problems now. We then reverse engineered the environment in which the stories took place. What decisions did society make that ultimately enabled the bad actors? What technology development path did industry take that created vulnerabilities? What standards did regulatory authorities establish without consideration for security? What actions did the government take (or not take)? If we could surmise the potential path leading to these negative futures, we could explore paths to more positive futures.

We used a whole-of-society approach to suggest both small and large tasks that individuals and groups could champion. From small behavioral changes at home and at work by individuals, to massive changes in business

practices by companies, the key objective was to reduce the potential attack surface. For example, we suggested tasks to increase individuals' awareness of and ability to prevent spear-phishing email attacks. Other suggested solutions focused on industry, such as developing robust security systems that address both IT and OT (operational technology). Of course, government would need to take measures to protect the nation, but we chose to focus on empowering various communities to become agents for social change.

To a tech-savvy engineering community, the solutions and ideas we produced might appear to be common sense. But that's where these stories about the future come into play: they help educate the nontechnical community.

One idea became clear as we worked: the future environment will be complex, and the threats and attack vectors will be diverse. Therefore, our solutions must also be diverse and interconnected.

From my foxhole, threatcasting the digital domain is an important research endeavor. It incorporates thought leaders across industry, academia, government, and military. Therefore, we can address not only traditional cybersecurity and cyberoperation issues but also issues in the broader cyberspace. We'll continue threatcasting, but we need your help. What do you, as engineers and computer scientists, think should be explored? 

NATALIE VANATTA is an assistant professor and the deputy chief of research at the Army Cyber Institute. Contact her at natalie.vanatta@usma.edu.