LAI Leading Authorities, Inc.

Tarah Wheeler

Cybersecurity Expert, White Hat Hacker

AI and Cybersecurity: What's Coming and What to Do About It Every organization is now an AI organization, whether it planned to be or not. That means every organization is also an AI security problem. On the offensive side, AI is making phishing attacks sharper, faster, and harder to detect. On the defensive side, it can reduce alert fatigue and give security teams fewer, better signals. The question isn't whether AI changes your risk profile. It already has. Tarah Wheeler is a cybersecurity CSO who runs nation-state incident response at TPO Group and an AI researcher at the University of Oxford. She isn't speculating about what AI might do to cybersecurity. She is watching it happen in real time. In this talk, she explains the threats and the tools in plain language, with concrete steps your people can take today. Whether your audience is a room of engineers or a room of executives who have never thought about information security before, Tarah calibrates to their level with facts, clarity, and enough humor to make the serious material memorable.

What AI Actually Is: A Researcher's Guide for the Rest of Us Most people explaining AI to general audiences have never built a model. Tarah Wheeler has. As a doctoral researcher at the University of Oxford, she builds and trains AI systems (natural language processing models, support vector machines, sequence alignment tools) to answer real research questions. That direct experience is what makes her explanations effective. She doesn't use analogies because she lacks technical depth. She uses analogies because she has the technical depth and wants the audience to share it. This talk removes the mystery from artificial intelligence. Using examples from her own Oxford research, Tarah walks audiences through what AI models actually do, how they learn, where they fail, and why that matters for every decision-maker in the room. No jargon, no hype, no doom. A precise look at how these systems work, from someone who builds them and who can explain in fifteen minutes what most whitepapers fail to convey in fifty pages.

This Is What Cyberwar Actually Looks Like Cyberwar is not a movie plot. It is happening now, and most of it looks nothing like what people imagine. Nations are attacking each other's infrastructure, stealing intellectual property at scale, and conducting influence operations that make the boundaries between espionage and combat difficult to identify. The laws of war were not written for this.
The people making policy often don't understand the technology, and the people building the technology often don't understand the policy. Tarah Wheeler works in both domains. Tarah has keynoted NATO CyCon, testified before the US Senate on the Cyber Safety Review Board, served as Senior Fellow for Global Cyber Policy at the Council on Foreign Relations, and conducted Fulbright research at Oxford's Centre for the Resolution of Intractable Conflict. Her team at TPO Group handles nation-state incident response for critical infrastructure. In this talk, she explains what cyber conflict actually looks like between nations, what is at stake for ordinary people and businesses

affected by it, and what we are getting wrong in our approach to defense.

Inside the Mind of a Hacker You don't have to be a hacker to think like one, but it helps to understand how they think if you want to stop them. Attackers don't break into organizations through genius. They break in through the gap between what leadership thinks is secured and what actually is. They exploit human habits, overlooked configurations, and the universal corporate assumption that a breach will happen to someone else. The good news: understanding how attackers find and exploit vulnerabilities is the single best investment any organization can make in its own defense. Tarah Wheeler is a white hat hacker, offensive security veteran, and the CSO of a firm that responds to nation-state attacks on critical infrastructure. She has been Head of Offensive Security at Splunk and a principal security advocate at Symantec. In this talk, she explains the attacker's methodology: how they select targets, find weaknesses, and move through systems. Then she provides the practical, actionable steps to address those weaknesses. This is not a talk designed to frighten. It is a briefing that leaves every person in the room, from the state IT director to the newest employee, more capable of protecting their organization and themselves.

Learning from Cyber Incidents: Why We Keep Making the Same Mistakes When a plane crashes, an independent board investigates, publishes findings, and the entire aviation industry learns from it. When a major cyber incident happens, organizations hire lawyers, issue a press release, and everyone else quietly hopes it won't happen to them. We have sixty years of proven methodology for learning from catastrophic failures, and we are barely using any of it in cybersecurity. That is a choice, and it is the wrong one. Tarah Wheeler co-authored the foundational Belfer Center paper on adapting aviation safety models (the NTSB framework) to cybersecurity, working alongside leading researchers in the field. She brings a rare combination: the technical depth to understand what went wrong in a breach, the policy expertise to understand what systemic change requires, and the practical experience of leading incident response at TPO Group. This talk gives CISOs, board members, and technical leaders a framework for converting every incident into institutional knowledge instead of repeated failure. It is for organizations that are tired of reading about the same breaches year after year and want to build something better.

Global Cyber Policy: What Nations Owe Each Other in the Digital Age The internet doesn't have borders, but the nations attacking each other through it certainly do. State-sponsored attacks, digital espionage, and the weaponization of technology against civilian infrastructure are accelerating faster than the international community's ability to establish norms. The question of what nations owe each other in cyberspace, and what happens when they violate those obligations, is one of the defining policy challenges of our time. Tarah Wheeler has shaped this conversation directly: as a Senior Fellow at the Council on Foreign Relations, in testimony before the US Senate and the European Union, at the OECD, and as a keynote speaker at NATO CyCon. Her Fulbright research at Oxford focused on defining cyberwar crimes and mitigating harm to civilians during nation-state cyber operations. In this talk, she explains what is working and what is failing in international cyber cooperation, and she describes what it will actually take to build a more secure and accountable

digital order. This is the conversation for policy leaders, diplomats, and anyone who wants to understand how international cyber norms are being established and by whom.