# Statement of Interest: Bringing Cybersecurity Governance Insights to AI Red Teaming

Judith Kankam-Boateng
University of Southern Denmark
Department of Mathematics and Computer Science
Odense, Denmark
jukan@imada.sdu.dk

## Abstract

This statement outlines my interest in participating in the HEARTS workshop at CHI 2026. As a cybersecurity PhD student researching governance and mental models in SME security practices, I aim to contribute insights from traditional security evaluation to the emerging field of AI red teaming. I bring qualitative research expertise, experience studying stakeholder misalignments across organizational hierarchies, and a fresh perspective on scaling evaluation practices while maintaining human expertise and well-being.

**ACM Reference Format:**
Judith Kankam-Boateng. 2026. Statement of Interest: Bringing Cybersecurity Governance Insights to AI Red Teaming. In . ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

## 1 Background and Relevant Experience

I am a cybersecurity PhD student in the Department of Mathematics and Computer Science at the University of Southern Denmark, researching cybersecurity practices and governance in Danish SMEs within the defence and IT/telecommunication sectors. My doctoral work, funded by Industriens Fonden, employs qualitative and quantitative methods to map security practices, elicit mental models of cybersecurity across three stakeholder levels (policymakers, industry associations, and SME implementers), and identify misalignments between policy intent and organizational reality.

My research has revealed significant gaps between how different stakeholders conceptualize and implement cybersecurity. For instance, our just-submitted study (presented at CHI26) found that SMEs often treat cybersecurity as a compliance checkbox rather than a strategic practice, while policymakers assume organizations approach security strategically. These misalignments create governance challenges that compound as security practices attempt to scale.

I have extensive experience with qualitative research methods, including focus groups, interviews, and thematic analysis, having conducted studies with policymakers, industry associations, NGOs, multinational companies, and SMEs. I have also served as a teaching assistant for cybersecurity courses twice. While my primary research focus has been traditional cybersecurity, I have been increasingly engaging with AI safety literature and attending talks on AI evaluation and safety through conferences like EUROUSEC.

*Conference'17, Washington, DC, USA*
2026. ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

## 2 What I Hope to Gain

I am drawn to HEARTS because AI red teaming faces strikingly similar challenges to those I study in traditional cybersecurity governance: how to scale evaluation practices while maintaining quality, how to align diverse stakeholders with different mental models, and how to support the humans doing the critical work.

I want to understand how governance frameworks for AI red teaming are evolving and whether they face similar stakeholder misalignment issues. I am particularly interested in learning what mental models different actors (AI developers, red teamers, policymakers) hold about the effectiveness of red teaming and how these might diverge. Additionally, I want to explore how worker well-being considerations are being integrated into red teaming at scale, particularly around risk disclosure and training.

This workshop represents an opportunity to explore how my expertise in traditional security governance can translate to the emerging field of AI safety evaluation.

## 3 What I Hope to Contribute

I bring three areas of potential contribution to the HEARTS workshop.

### 3.1 Methodological Expertise in Qualitative Stakeholder Research

My experience conducting focus groups and interviews across organizational hierarchies could inform approaches to studying red teamer experiences, mental models, and needs. Understanding how red teamers conceptualize their work—and how that differs from how developers or policymakers view red teaming—could reveal important alignment gaps.

### 3.2 Insights from Traditional Security Governance

Many challenges in scaling AI red teaming echo patterns I've observed in cybersecurity regulation: the tension between compliance and strategic thinking, the gap between documented processes and actual practices, and the difficulty of maintaining expertise as practices scale. Lessons from how these issues manifest in SME cybersecurity could offer useful parallels.

### 3.3 Fresh Interdisciplinary Perspective

As someone coming from traditional cybersecurity with a growing interest in AI safety, I may help bridge concepts between established security practices and emerging AI evaluation needs. My experience identifying and analyzing stakeholder misalignments could

inform discussions on governance frameworks and accountability mechanisms for red teaming.

I am particularly interested in the workshop's governance and worker well-being threads, as they closely align with my research on stakeholder alignment and organizational security practices. I'm eager to learn from practitioners and researchers across academia, industry, and policy, and to explore how my background in traditional cybersecurity can contribute to the development of more humane, scalable AI evaluation practices.