

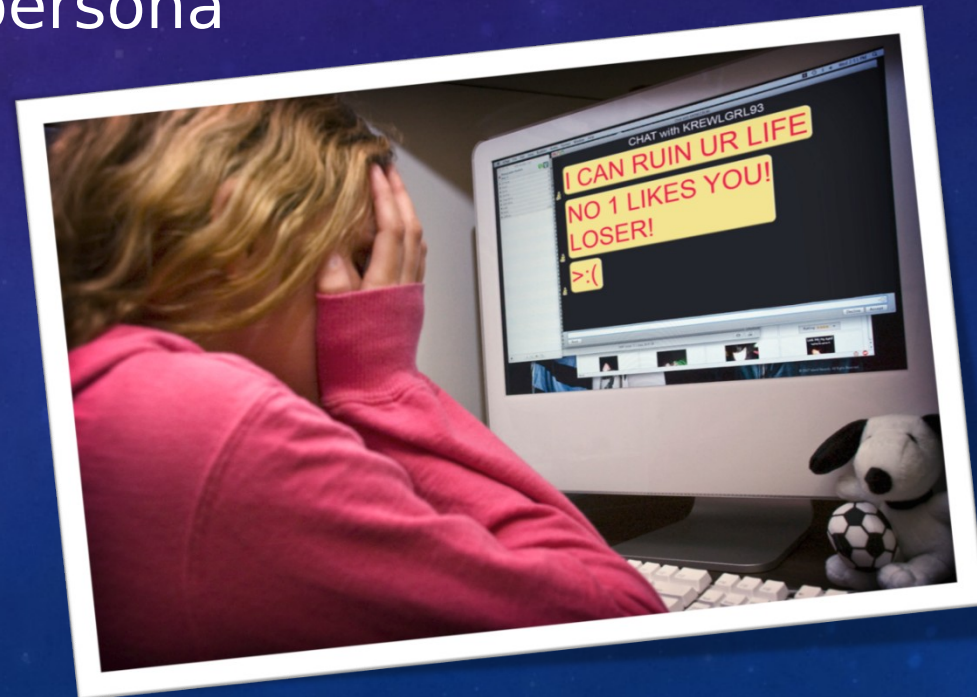
The background features a dark blue gradient with faint, light blue circular patterns and a scale. The scale is a large arc on the left side, with numerical markings from 40 to 260 in increments of 10. Several smaller circles and arcs are scattered across the background, some with arrows indicating direction. The overall aesthetic is technical and futuristic.

IEEE TECHNOLOGY- FACILITATED INTERPERSONAL CONTROL WG: WORK IN PERSONA MODELING

JESSIE LOWELL, PHD, CIPT

THE IEEE TECHNOLOGY-FACILITATED INTERPERSONAL CONTROL WG

- Working on standards related to preventing and mitigating coercive technology-facilitated interpersonal control
- Several subgroups, of which persona modeling is one



WHY PERSONA MODELING?

- To understand and mitigate threats, we have to understand threat *actors*.
- In order to understand how threat actors and their targets interact, we also have to understand the *targets*.
- Traditional cybersecurity tends to be focused on enterprises and/or nation-states.



USEFUL REFERENCE DOCUMENTS

- eSafety guide for developers (Australia):
 - <https://www.esafety.gov.au/sites/default/files/2024-09/SafetyByDesign-technology-facilitated-gender-based-violence-industry-guide.pdf?v=1727156355932>
- Carnegie Mellon University's discussion of three persona modeling methods
 - <https://insights.sei.cmu.edu/blog/cyber-threat-modeling-an-evaluation-of-three-methods/>
- LINDDUN GO
 - <https://linddun.org/go/>
- Dev et al. MAP paper
 - <https://dl.acm.org/doi/fullHtml/10.1145/3544548.3581484>
- IBM on coercive control-resistant design
 - <https://www.ibm.com/downloads/documents/us-en/10c31775c2540c22>
- IBM design principles to combat technology abuse
 - <https://web.archive.org/web/20240617222211/https://www.ibm.com/policy/five-technology-design-principles-to-combat-domestic-abuse>

HOW SHOULD WE MODEL PERSONAS?

- We liked the flexibility of card-based approaches
- MAP paper was useful for thinking about taxonomies
- To model victim personas, or not?

DIFFERENCES FROM IETF DULT THREAT MODELING I-D

- Broader scope
- Shallower scope (does not need to take specific protocols into account in the same way, at least not yet)
- Starting out with an informational document for the larger working group

The screenshot shows the IETF Datatracker interface for the document "DULT Threat Model" with the draft ID "draft-ietf-dult-threat-model-00". The page includes a navigation menu with "Groups", "Documents", "Meetings", "Other", and "User". Below the title, there are tabs for "Status", "IESG evaluation record", "IESG writeups", "Email expansions", and "History". A "Versions:" section shows a timeline with two versions: "00" (highlighted in blue) and "00" (highlighted in yellow). The timeline indicates that the yellow version was active from June 2024 to September 2024, and the blue version was active from September 2024 onwards. Below the timeline, a table provides document details:

Document	Type	Active Internet-Draft (dult WG)
	Authors	Maggie Delano ✉, Jessie Lowell ✉
	Last updated	2024-10-01 (Latest revision 2024-09-18)
	Replaces	draft-delano-dult-threat-model
	RFC stream	Internet Engineering Task Force (IETF)
	Intended RFC status	(None)
	Formats	txt html xml htmlized bibtex bibxml
	Additional resources	Mailing list discussion
Stream	WG state	WG Document
	On agenda	<input type="checkbox"/> dult at IETF-121

CONCEPTUAL CROSSOVER WITH IETF HRPC WORK

- Not all human rights threat actors have nation-state level resources (some are paramilitary groups, etc).
- Gender-based violence should be understood as a human rights violation.
- Gender-based violence often comes up in the context of war, conflict, political violence, and state repression.
- Taxonomy-based approaches may also have relevance in the larger human rights context.

QUESTIONS?