



Reaching Beyond the Law: The Question of Accountability in International Cyber Affairs

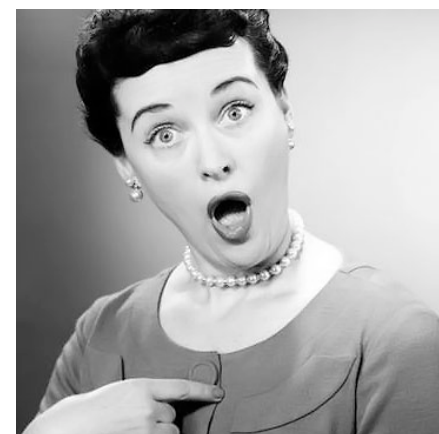
Madeline Carr, Cardiff University



My task...

How can we cultivate an inclusive culture of cyber security where various actors assume accountability towards each other?

How do we create a system of international cyber security with optimized and mutually supportive stakeholder roles and responsibilities?





- **The problem of attribution for accountability**
 - Attribution introduces a new layer of anarchy or
 - Attribution doesn't matter all that much

- **The problem of agency for accountability**
 - To whom (or what) can we attach expectations of responsible behavior?
 - To what extent do actors *acknowledge* their commitments?

- **What is the potential value of opacity?**





The problem of attribution for accountability



- **Attribution introduces a new layer of anarchy**
 - Our ideas about the states system, international society, and therefore, international order, all rest on the (previously sound) assumption that state actors are readily and accurately identifiable. This is integral to state actors' ability to engage in diplomacy, war and international law.
- **Attribution doesn't matter all that much**
 - Generally, recovery and mitigation to limit the damage are prioritized over establishing who was behind an attack.
 - But some have such serious implications that they become elevated to issues of international relations

+ The problem of agency for accountability



- To whom (or what) can we attach expectations of responsible behavior?
 - Ambiguous agency
 - New actors
 - Complex interactions
 - Plausible deniability here too!
- To what extent do actors *acknowledge* their commitments?
 - Problems of the public/private partnership
 - Problems of 'multi-stakeholderism'



Accountability for what?

- **Governments**
 - National interest
 - Right and wishes of citizens
 - Commitment to international society
- **Private sector**
 - Shareholders
 - Law
 - Abdication of government accountability
(information sharing in the UAE)
- **Civil society organisations**
 - Funding and revenue
 - Online privacy vs personal accountability and transparency in cultures based on communitarian values.



The value (?) of opacity...

And of multi-disciplinarity





Zero Knowledge Proofs...

- I know that 26781 is not a prime since it is 113 times 237, to **prove to you** that fact, I will present these factor and demonstrate that indeed $113 \times 237 = 26781$.
- A typical by-product of a proof is that you **gained some knowledge**; not only are you convinced that 26781 is not a prime, but you also learned its factorization.

*In instances where we don't want to share knowledge, but would like to prove accountability, **transparency** may not be the end goal.*





So...

- *How can we cultivate an inclusive culture of cyber security where various actors assume accountability towards each other?*
- *How do we create a system of international cyber security with optimized and mutually supportive stakeholder roles and responsibilities?*
 - Transparency can help
 - But so (perhaps) can opacity.
 - By acknowledging that norms are not ideals. They're points of agreement, of mutual or shared interest.
 - Clarity (and honesty) about roles and responsibilities
 - Identifying why and when accountability matters