Interview – Julia Slupska

https://www.e-ir.info/2022/09/18/interview-julia-slupska/

E-INTERNATIONAL RELATIONS, SEP 18 2022

This interview is part of a series of interviews with academics and practitioners at an early stage of their career. The interviews discuss current research and projects, as well as advice for other early career scholars.

Julia Slupska is a doctoral student at the Oxford Internet Institute and is a member of the Centre for Doctoral Training in Cybersecurity in the University of Oxford. She previously completed her MSc in Social Science of the Internet from Oxford. Her research is focused upon online safety and cybersecurity, particularly technology abuse like stalking and image-based sexual abuse ('revenge porn'). She is also exploring how feminist theories and methodology—such as participatory action research and ethics of care—can improve cybersecurity. Previously, she has worked on an LSE Law project on comparative regional integration and coordinated a course on Economics in Foreign Policy for the Foreign and Commonwealth Office. In 2020, she received the FTGS Graduate Student Paper honourable mention for her paper *"Safe at Home: Towards a Feminist Critique of Cybersecurity"*.

What (or who) prompted the most significant shifts in your thinking or encouraged you to pursue your area of research?

Carol Cohn's work—as well as other theorists writing in the tradition of feminist international relations and feminist security studies—made a big impression on me as an international relations undergraduate. In her pivotal study of the nuclear deterrence community, Carol Cohn (1987) found that defence intellectuals spoke much more passionately of the missiles they studied than of the human lives which they described impersonally as "collateral damage." Cohn argues that, "[i]f human lives are not the reference point, then it is not only impossible to talk about humans in this language, it also becomes in some sense illegitimate to ask the paradigm to reflect human concerns … [questions that] raise issues in human terms can be dismissed easily. No one will claim that the questions are unimportant, but they are inexpert, unprofessional, *irrelevant to the business at hand to ask*." (emphasis added, p.712).

After I joined a cybersecurity course in a computer science department, I repeatedly asked an irrelevant question which echoes Cohn: "is image-based abuse (commonly, but regrettably, known as 'revenge porn') a cybersecurity issue?" When I asked programmers and computer scientists—both lecturers and fellow students—this question, I was often met with confusion. Several times the answer was "no", because image-based abuse is more accurately a "privacy issue". In other words, it is irrelevant to the business at hand.

Yet when an employee in a company shares confidential information with an unauthorised third party, this is clearly identified as a cybersecurity issue, and an entire subfield of cybersecurity has been developed to protect companies from insider threat. To combat insider threat, cybersecurity experts develop social and technical 'access controls' which, for example, might revoke access to sensitive data if an employment ends acrimoniously. Why do similar access controls not exist for intimate relationships? Instead of developing programmes which revoke access to intimate data when a relationship ends and making such programmes accessible to the wider public, online safety advocates publish guides aimed at teenagers, advising them not to share intimate photos in the first place (see for example).

This question of relevance—what counts as a relevant security issue—is how power is exercised in research and policy, how some people's threats are made less important. Such oversights in categorisation motivated me to research online safety and cybersecurity in the context of domestic and intimate partner violence. More recently, critiques of white feminism as well as abolitionist theories have helped me understand limitations in my own work, including treating gender as a sole category of analysis (as opposed to a broader understanding of intersectionality) and understanding how research can be co-opted by the carceral state. This motivated me to consider technology abuse on broader scales, including surveillance of migrants as a part of the hostile environment and increasingly authoritarian border controls.

You are/were involved with the "Reconfigure Network" project, which sought to find out how cybersecurity would be configured if the concerns of ordinary citizens were taken into account. What did you discover and how did your findings correspond with popular notions about cybersecurity? Why is this approach important and how might citizen's concerns shape cybersecurity differently?

Cybersecurity that starts with ordinary people's concerns-rather than the integrity of data and information systems – is much more likely to point to problems linked to structural harms (such as harassment based on racism or misogyny, or lack of access due to financial inequality) – than vulnerabilities in code or product design. Likewise, true sources of safety in peoples' lives come from community support networks rather than cybersecurity products. In research, particularly computer science research, "real world impact" is often couched in terms of developing a product that can be patented or sold. By thinking outside of this research-for-profit framework, researchers can begin to recognise and build on these community support networks, in order to contribute more meaningfully to security.

For example, we partnered with an organisation named Voice of Domestic Workers is a support group by and for migrant domestic workers. In the absence of their families (who often remain abroad) and safety nets from the state, this kind of peer support group is crucial in providing safety in these women's lives. Our research with VoDW highlights both the structural causes of insecurity (gendered labour and racialised surveillance practices) and community support networks as sources of everyday security.

In your award-winning paper, you argue that cybersecurity risks recreating the issue of 'individualisation' of security problems in International Relations. What do you mean by this and how does it impact cybersecurity in practice? Further, how does the recreation of these issues modify our understanding of gendered spaces?

Feminist theorists of IR and security studies have noted the ways the "public/private" binary plays out in security research: violence such as war or terrorism are included in research on security, but gender-based violence like intimate partner violence or sexual assault are treated as "private issues" outside of the concerns of security research. A similar dynamic has played out in traditional cybersecurity research, which focused on defending militaries and businesses but not marginalised people. This has changed with an increase in concern over online harms such as misinformation and identity theft. However, the field is still much more likely to think of problems that can be easily understood within a profit motive rather than in terms of safety, empowerment, and dismantling hierarchies of difference based on gender, race or disability. Drawing on and extending feminist and abolitionist moves towards safety instead of security can help focus on building safer spaces online rather than profiting from fear in a way that extends carceral systems.

What are you currently working on?

I am currently working on writing up and finishing my PhD. Besides that, I am working with a group called No Tech for Tyrants on a project examining police abuse of surveillance technology. My interest in this project was prompted by the many similarities between intimate abuse online and state sanctioned surveillance: police will often use technology to harass, intimidate, and even humiliate marginalised people (as in cases where the police share surveillance footage as examples of "dumb criminals" on police Twitter pages or police reality TV shows).

What is the most important advice you could give to young scholars?

Take time and space to reflect on what you wish to accomplish in your work and how your work is shaped by institutional opportunities and constraints. Many of the individuals and organisations that have resources to fund research are also actors whose harmful practices call for rigorous and sustained critique. Of course, the responsibility to challenge these wider funding practices should not fall squarely on early career researchers, who are often the most precarious and least powerful members of academia. However, having an awareness of how these structures shape your work is the first step towards being able to resist them.