# Race and Coloniality in Cybersecurity

https://www.e-ir.info/2023/11/10/race-and-coloniality-in-cybersecurity/

DENSUA MUMFORD AND JAMES SHIRES, NOV 10 2023

As the debates on the uses and benefits of Artificial Intelligence (AI) intensify, many are warning of its potential to reproduce multiple forms of domination, including racism, misogyny, ableism, and others. Timnit Gebru – a former Google ethics lead, Stanford alumni, and head of the Distributed AIR Research Institute (DAIR) – and her team have provided ample evidence of the racialised and gendered nature of AI's training data and AI's racialised effects on society. Organisations such as Black in AI as well as scholars working on digital technologies more broadly, such as Safiya Noble (2018), Syed Mustafa Ali (2018), Shoshana Zuboff (2020), Cathy O'Neil (2017), Nick Couldry and Ulises Ali Mejias (2019), have raised similar warnings. Through painstaking investigations, they have informed us about how the Eurocentric, White, masculinist, capitalist, and military origins of technologies shape not just their development but also their teleology; that is, what we imagine technology is for in the first place. Technology has often been created to realise visions of a narrow elite at the expense of a good life for the global majority.

Cybersecurity, on the other hand, has largely managed to avoid such important debates about the effects of race, despite the fact that race is tangibly present in the way the field is studied and practiced. Prevalent theories in cybersecurity studies (for example, Gartzke & Lindsay, 2015; Kello, 2017; Fischerkeller et al., 2022), despite their otherwise sophisticated accounts of the interaction between society and technology, would struggle to explain why evident racialised dynamics might exist in the first place and how they shape material outcomes. Only rare and isolated initiatives such as #sharethemicincyber highlight stark racial gaps in participation in cybersecurity research and practice.

Our research, published in *Security Studies*, contributes to these critical debates by showing that race has significant effects in constituting cybersecurity threats and responses. Based on original data from cybersecurity expert communities in the Gulf, we argue that race operates as a marker of who is a legitimate holder of dominant Euro-American knowledges and who is not, and therefore whose understandings, experiences, and practices of cybersecurity are privileged. Thus, the racial-epistemic hierarchies (Taylor, 2012) we identify are constitutive of the environment in which cybersecurity expertise is developed.

Specifically, our interviews and empirical observation identify three stereotypical subject-positions in cybersecurity expert communities: White Euro-American experts, Gulf clients and 'native' managers, and South Asian contractors. Note that these categories are not natural facts, but rather constructions of the community itself, with many individuals (such as British Asian experts) not fitting neatly into those categories. Furthermore, experts across the board possessed similar standards of knowledge, attended the same conferences, and had similar advanced degrees from institutions in the United States (US) and United Kingdom (UK). Nevertheless, race has created hierarchies amongst them and shaped cybersecurity outcomes. Those racialised as South Asian or other non-Arab people of colour are heeded less despite their equal training. Meanwhile, those racialised as White are privileged as experts by local Gulf business and government actors.

Based on this data, we conceptualise two interrelated racial-epistemic hierarchies. First, we note a 'hierarchy of rationality' in which reasonable, rational experts are coded White while individuals of other racial categories are considered cognitively inferior, irrational, and naïve. In particular, our interviews show that the Gulf region is seen as backward, lacking in skills, and generally a consumer rather than producer of cybersecurity knowledge when compared to Euro-America. Second, we identify a 'hierarchy of authority' in which the warnings and advice from

those marked as racially lower in the hierarchy are not taken seriously by those in decision-making roles. In this regard, South Asian interviewees shared their experiences of having their knowledges dismissed, risking the frustration of their Gulf superiors when speaking out about threats or complaining, and working in a general atmosphere where their contributions are not valued.

We turn to decolonial thought to explain the racialised condition of cybersecurity expert communities and why race has been absent in cybersecurity studies (in IR, see Rutazibwa, 2019; Shilliam, 2011; Blaney & Tickner, 2017, amongst many others). Decolonial thought offers an incisive characterisation of the modern/colonial epistemic origins of international relations and knowledge production more broadly. It is therefore an excellent perspective through which to understand how knowledge making is constituted by and in turn constitutes racial dynamics. In particular, decolonial thought helps to reveal how colonial modes of domination developed over 500 years are reproduced in technological fields often unquestioningly thought of as 'neutral' and 'progressive'. For example, development scholars have argued that the introduction of new technologies, such as industrial farming techniques in India, was a key means for colonizers to maintain racial superiority, even after independence, by demonstrating greater technological competence (Gupta, 1998).

According to this perspective, Euro-American modernity has been constructed as part of a duality whose underside is coloniality. While modernity is constructed as representing progress, rationality, and the future, coloniality encompasses all the cultural subjugation necessary to realise modernity (Mendoza, 2015; Maldonado-Torres, 2007). Thus, colonial powers conceive of a progressive Euro-America by direct reference to the barbaric 'Other' who must be tamed. Race has been a crucial way to distinguish those who are rational, knowledgeable builders of progress (White) from those who lack sense and must be tutored (non-White; though there are gradations amongst this group based on proximity to Whiteness) (Quijano, 2000; Wynter, 2003). In the process, highly particular Euro-American knowledges are constructed as objective, neutral, and therefore universally applicable, while other forms of knowledge are deemed as peculiar and valueless (Mignolo, 2009).

The semicolonial history of the Gulf helps us better understand the impact of coloniality on cybersecurity. Intelligence and military cooperation between Euro-America and what are now the Gulf states, which started under empire (although the Gulf territories were never formal colonies), included British and American companies winning key military and technological contracts. Britain also maintained intelligence outposts and satellite installations in various locations in the Gulf throughout the twentieth century – some of which are still there today. After the fall of empire, Gulf states continued their dependence on the US and UK for technological expertise and equipment in various fields, especially security. In this context, powerful stereotypes have evolved that depict rich Arab clients of Euro-American products who are nevertheless incapable of using the technology in a sophisticated manner. The Gulf is also notable for its reliance on the kafala system, where migrant workers from outside of the Gulf (mainly South and South-East Asia) provide cheap, exploitable labour. Another practice originating in the colonial era, it ensures a racialized hierarchy with Asians and Africans at the bottom.

Cybersecurity has evolved within those same colonial structures, with Gulf states receiving cyber- and other high-tech security assistance, often delivered by US and UK companies – although Gulf states remain targets of digital intelligence gathering themselves. At the same time, digital 'cheap labour' now includes relatively low-paid South Asian contractors with high job insecurity (relative to cybersecurity wages, which are nonetheless extremely highly paid compared to manual or domestic labour), which upholds the authority of both Gulf locals and more privileged Euro-American consultants. The longstanding colonial epistemic trajectories of military Orientalism (Hashim, 2019) and racialized kafala hierarchies help us to understand how race constitutes who in cybersecurity is a legitimate knower of dominant Euro-American knowledges and who is not.

Our findings have significant implications for the study and practice of cybersecurity today: primarily, that cybersecurity must work to unmake its colonial practices. To foster much needed changes, we call for a decolonial research programme for cybersecurity. While many present cyberspace and digital technologies as domains that require new practices, institutions, and modes of thinking (e.g. Kello 2017, Fischerkeller et al. 2022), our research instead points to continuities with far older structures rooted in colonialism. Decolonial praxis is therefore just as relevant in this field as with any other. Similar calls have been made in the fields of big data, computing, terrorism, AI,

and of course IR. We call for three necessary (but non-exhaustive) moves in the field of cybersecurity:

First, further investigations are needed to interrogate the coloniality of the field, particularly in relation to concepts such as technological 'maturity', which reproduce Euro-America as legitimate leaders of the digital future and the global majority as passive tutees receiving their knowledge. Colonial powers regularly used technological prowess as a means of evaluating the cultures they encountered. Silencing non-Euro-American influences and origins of those technologies was a corollary practice. Cybersecurity continues to rely on the concept of 'maturity' in international benchmarking programmes and capacity-building projects, which risks importing racialised meanings rooted in colonial dynamics.

Second, more work is needed to characterise and investigate *who* is empowered by structures of race, gender, etc, to occupy dominant positions and to reveal their particularities and situatedness, thus counteracting their supposed objectivity. We suggest the concept of a 'transnational techno-elite' who are diffuse and networked across centres of power such as Silicon Valley, foreign ministries, intelligence agencies and the military, international organisations, Euro-American universities, and consultancy firms, amongst others (for related thinking see Chimni, 2004; Noble & Roberts, 2019; Wark, 2006). They tend to be male, young, and English-speaking. The transnational techno-elite is constituted by a belief in a technological race to the utopian future in which progress is a linear inevitability that other cultures must 'catch up' to. Myths of post-racial equality and meritocracy paradoxically enable them to marginalise as 'immature' knowledges from the global majority: the Global South, women, LGBTQI+ persons, indigenous peoples, the working class and so forth.

Third, a decolonial cybersecurity will itself be constituted by the knowledge systems and life practices of a plurality of communities, not just Euro-America and the transnational techno-elite. That means cybersecurity should theorise (in)security as experienced by various marginalised groups, from LGBTQI+ people to Black women to indigenous peoples and more. It also means cybersecurity experts should themselves emerge from and be located in a plurality of communities, especially marginalised ones. A cybersecurity developed to address threats only to the state or other powerful institutions representative of the transnational techno-elite will reproduce coloniality and further deepen insecurity for the global majority.

**Bibliography**

Ali, S. M. (2018). Prolegomenon to the Decolonization of Internet Governance. In D. Oppermann (Ed.), *Internet Governance in the Global South: History, Theory and Contemporary Debates* (pp. 109–183). NUPRI University of Sao Paulo.

Blaney, D. L., & Tickner, A. B. (2017). Worlding, Ontological Politics and the Possibility of a Decolonial IR. *Millennium: Journal of International Studies*, *45*(3), 293–311. https://doi.org/10.1177/0305829817702446

Chimni, B. S. (2004). International institutions today: An imperial global state in the making. *European Journal of International Law*, *15*(1), 1–37.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). *Cyber Persistence Theory: Redefining National Security in Cyberspace* (1st ed.). Oxford University Press.

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Akhil Gupta, *Postcolonial Developments: Agriculture in the Making of Modern India* (Durham, NC: Duke University Press, 1998).

Hashim, A. S. (2019). Military Orientalism: Middle East Ways of War. *Middle East Policy*, *26*(2), 31–47. https://doi.org/10.1111/mepo.12419

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Maldonado-Torres, N. (2007). On the Coloniality of Being: Contributions to the development of a concept.*Cultural Studies*, *21*(2–3), 240–270. https://doi.org/10.1080/09502380601162548

Mendoza, B. (2015). Coloniality of Gender and Power: From Postcoloniality to Decoloniality. In L. Disch & M. Hawkesworth (Eds.), *The Oxford Handbook of Feminist Theory*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199328581.013.6

Mignolo, W. D. (2009). Epistemic Disobedience, Independent Thought and Decolonial Freedom.*Theory, Culture & Society*, *26*(7–8), 159–181. https://doi.org/10.1177/0263276409349275

Noble, S., & Roberts, S. (2019). Technological Elites, the Meritocracy, and Postracial Myths in Silicon Valley. In R. Mukherjee, S. Banet-Weiser, & H. Gray (Eds.), *Racism Postrace* (pp. 113–132). Duke University Press.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York: NYU Press.

O'Neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy* . Penguin Books.

Quijano, A. (2000). Coloniality of Power and Eurocentrism in Latin America. *International Sociology*, *15*(2), 215–232. https://doi.org/10.1177/0268580900015002005

Rutazibwa, O. U. (2019). What's There to Mourn? Decolonial Reflections on (the End of) Liberal Humanitarianism. *Journal of Humanitarian Affairs*, *1*(1), 65–67. https://doi.org/10.7227/JHA.010

Shilliam, R. (2011). Decolonising the Grounds of Ethical Inquiry: A Dialogue between Kant, Foucault and Glissant. *Millennium: Journal of International Studies*, *39*(3), 649–665. https://doi.org/10.1177/0305829811399144

Taylor, L. (2012). Decolonizing International Relations: Perspectives from Latin America:*Decolonizing International Relations*. *International Studies Review*, *14*(3), 386–400. https://doi.org/10.1111/j.1468-2486.2012.01125.x

Wark, M. (2006). INFORMATION WANTS TO BE FREE (BUT IS EVERYWHERE IN CHAINS). *Cultural Studies*, *20*(2–3), 165–183. https://doi.org/10.1080/09502380500495668

Wynter, S. (2003). Unsettling the coloniality of being/power/truth/freedom: Towards the human, after man, its overrepresentation—An argument. *CR: The New Centennial Review*, *3*(3), 257–337.

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First Trade Paperback Edition). PublicAffairs.

---

## About the author:

**Dr. Densua Mumford** is Assistant Professor of International Relations at the Faculty of Governance and Global Affairs, Leiden University. Her research primarily explores the international relations of African peoples and states. Within this broad theme, she focuses on the role of regional organisations such as the African Union, ECOWAS, and SADC in the political and economic dynamics of the continent. She is currently investigating the discursive context of

African regionalism. She also has a robust research interest in the politics of the internet and digital technologies, with a current project on the political narratives of cryptocurrency evangelists. Her work contributes to decolonising perspectives on international relations.

**James Shires** is the Co-Director of the European Cyber Conflict Research Initiative (ECCRI), and Senior Research Fellow in Cyber Policy at Chatham House. He was previously an Assistant Professor in Cybersecurity Governance at the Institute of Security and Global Affairs, University of Leiden. He is also a non-resident Fellow with The Hague Program on International Cyber Security. He has written widely on issues of cybersecurity and international politics, including cybersecurity expertise, digital authoritarianism, spyware regulation, and hack-and-leak operations. He is the author of The Politics of Cybersecurity in the Middle East (Hurst/Oxford University Press 2021).