St Antony’s International Review (STAIR)

Call for Abstracts

Whose Security is Cybersecurity?
Authority, Responsibility, and Power in Cyberspace

Abstracts of 500 words to be submitted by 23 November 2018.
Final Articles of maximum 8000 words to be submitted by 27 January 2018.

To what extent has the emergence of cyber technologies affected how we think, and should think, about international relations? Has there been fundamental change, or are we simply seeing a continuation of existing trends? The dynamics of cyberspace seemingly challenge traditional approaches to the study of world politics. They raise important questions regarding what the potential sources of threats are, who is responsible for addressing them, and who or what is most vulnerable. In short, whose security is cyber security? From influence campaigns to internet censorship, cyberspace has become a contested and volatile realm within, among, and beyond states. As we move further into the Digital Age, it becomes increasingly imperative to interrogate the way in which we think about security in cyberspace, and examine how notions of authority, responsibility, and power may be transforming with the global proliferation of new cyber capabilities. STAIR’s May 2019 issue will explore this topic, and is looking for contributions related but not limited to the following subtopics:

- **Responsibility, governance, and norms in cyberspace**: the role of state and non-state actors in establishing and upholding regulations and norms of behavior in cyberspace; the primacy of the state and the nature of sovereignty in an increasingly cyber-dependent world; the character of norms and norm diffusion in cyberspace

- **Cybersecurity and the changing nature of conflict**: the definition and boundaries of war and conflict in cyberspace; who is vulnerable to cyber threats and who bears responsibility for providing cybersecurity; the influence of cyber technologies on the nature of conflict; the proliferation of cyber capabilities and their effects on tactics employed in conflict

- **Cyber capabilities – development and asymmetries**: assessing the extent to which advances in cyber capabilities are asymmetrical and the implications for global power dynamics; what cybersecurity means for the developing world; the role of cyber technology in IPE; how advances in AI affect cybersecurity

This issue of STAIR aims to encourage new contributions that push beyond the scope of the existing literature on cybersecurity through interdisciplinary dialogue about the nature of and relationships between authority, responsibility, and power in cyberspace. We welcome submissions across various disciplines, such as international relations, political science, law, strategic studies, economics and political economy, development studies, political theory, area studies, as well as more technical fields such as engineering, computer science and IT.

Please submit your abstract by November 23 via the [STAIR Submissions Form](#). For more details regarding the submissions procedure and the style guide, please consult our website. For any other inquiries, please email Taylor Grossman (taylor.grossman@politics.ox.ac.uk).