Dear Faculty Search Committee,

I am writing to express my interest in the position of Lecturer in the Department of Science, Technology, Engineering, and Public Policy (STEaPP) at University College London. I am currently an Assistant Professor of International Affairs in the Bush School of Government and Public Service at Texas A&M University. My interdisciplinary PhD in Technology, Management, and Policy from MIT’s Engineering Systems Division combines computer science, international political economy, and operations strategy. I believe integrated research, engagement, and teaching is key to understanding contemporary and emerging challenges facing Internet infrastructure governance and security, and for developing the next generation of policy analysts and researchers that contribute to solving global challenges such as cybercrime, platform governance, and improving Internet infrastructure in developing regions. My research provides significant insights into the politics of the epistemic communities managing the Internet’s infrastructure and security, and the implications for integrating these untapped resources into evidence-based policy making and the global governance system. Over the past ten years, my engagement with these communities has created regional and global impact, including developing of cybersecurity communities in developing regions and addressing cybersecurity data governance challenges. In the last four years my teaching has integrated this work into a comprehensive, research-led cyber policy programme, blending theory, case studies, and innovative teaching methods to

develop students’ critical thinking skills

applied to project-based deep dives into substantive domains that

that hones the skills necessary for policy analysts and researchers to bridge the gaps between policy and technical communities.

I believe my current and emerging research, upcoming policy engagement, and well-developed cyber policy curriculum is exceptionally well-suited to STEaPP and the Digital Technologies Policy Lab (DTPL). My current research complements existing work on infrastructure (McCarthy sp?), development (Julius and Jakub), and abuse (Tanczer). I believe my emerging work on co-regulatory approaches to combating disinformation and data governance would be a substantive contribution to the DTPL. I explicitly designed my cyber policy curriculum for social scientists from diverse intellectual backgrounds. The introduction to cyber policy and data science courses can easily be adapted for an undergraduate curriculum; my advanced courses on platforms and politics, and the advanced cyber course would appeal to students in the digital route and doctoral students. The DTPL and the Policy Impact Unit would ideal homes for programmes I am planning with industry and non-profit partners on cybersecurity data governance and the ongoing challenges facing collaborations between technical communities and law enforcement. I believe my intrinsically interdisciplinary portfolio is a rare and valuable complement to STEaPP’s mission and programmes, and I would be absolutely thrilled at the opportunity to join your department.

**Research** My research strategy has always been interdisciplinary. I started my academic life in computer science as a software engineer, focusing on programming languages and network security, but soon realized technical knowledge alone was insufficient to understand the complex sociotechnical dynamics shaping Internet development and cybersecurity challenges. My doctoral research at MIT combined international political economy, operations strategy, and computer science to conduct extensive fieldwork examining on-the-ground practices in Internet infrastructure management and cybersecurity. I funded the last year of my dissertation work as the primary author on a Google Faculty Research Award ($85,000).

As a Postdoctoral Cybersecurity Fellow at Stanford, I won two grants (totaling $125,000) evaluating the informal collaboration between global cybersecurity communities and law enforcement. I developed and executed the research plan, managed budgets and research assistants; and ran workshops and focus groups bringing together cybersecurity professionals, law enforcement, lawyers, and policymakers in the US, Africa, and Europe. The cumulative *Combined Capabilities* report evaluated these collaborations in terms of credibility and legitimacy norms within these groups and in the broader global governance system. In collaboration with colleagues at the Shadowserver Foundation, we are continuing this work in a report for Europol. This report documents and evaluates the technical, legal, and coordination learnings from the Avalanche botnet takedown, one of the largest concerted applications of Mutual Legal Assistance Treaties (40 jurisdictions).

My research has three common themes:

the coproduction of expert knowledge,

how it facilitates the adaptation necessary to keep pace with changes in technology and emerging security threats, and,

importantly, how to integrate expert knowledge into policy development, regulatory design, and global governance processes.

My [chapter on planned adaptation](https://link.springer.com/chapter/10.1007/978-3-030-05252-2_13) presents a generalized model for evaluating ad hoc and systemic planned adaptation in the regulation of complex engineering systems. In collaboration with Dr. I. Brass, [our article](https://link.springer.com/chapter/10.1007/978-3-030-05252-2_13) in *Regulation & Governance* presents a planned adaptive regulatory framework for IoT security regulation and standards. My [article](https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1754443) in the *Journal of Cyber Policy* comparatively evaluates consolidation in digital platforms, highlighting how governance and accountability strategies employed by communities in the Internet’s infrastructure preclude the predatory practices typically associated with platform consolidation. In an article currently under review with International Organization (included as a writing sample), I contribute to the literature on epistemic communities by empirically evaluating how institutions coordinating the Internet’s infrastructure, in the absence of state regulation, accrued authority, and how to more effectively integrate these authorities into the broader global governance system. I believe my common research themes are exceptionally aligned with STEaPP’s mission to mobilise deep expertise in complex engineering systems and policy to solve wicked global policy problems.

To coordinate across funded research projects, I created and fund the Internet Infrastructure and Policy Research Group (IIPRG), where I supervise four masters-level student researchers. IIPRG projects include

the politics and governance of submarine cables critical to Internet communication;

mix-methods modeling of the relationship between types of autocracy and Internet shutdowns, with technology transfer as an intervening variable;

studies of Internet infrastructure development in developing regions, with a special focus on Africa and Latin America; and

multilevel network analyses (combining organizational and individual ties) evaluating the globally diverse institutional complex that ensures the stability, safety, and security of the Internet, with a special focus on identifying gaps between this dense institutional network and the broader global governance system.

The submarine cables work has produced one student-authored publication in the Journal of Policy and International Affairs, co-authoring a second that is under review by Contemporary Security Policy. My co-authored five-case piece on autocracies and Internet shutdowns is under review by the Journal of Peace Research, with a second using hierarchical clustering to further test our model on shutdown data from 2016 to 2021 in progress. I believe these research streams would not only benefit the DTPL, contributing additional novel and impactful research, but would also create fruitful linkages with the infrastructure and development research clusters. In addition to these work streams, through my engagement discussed below, I am developing new research streams on data governance and disinformation. Interdisciplinary research environments are my native habitat, and I am excited at the prospect of collaborating with colleagues in STEaPP and the DTPL on these projects.

**Engagement and Impact Through Science Diplomacy** My deep, novel research findings would not be possible without continuous and trusted engagement with the epistemic communities managing the Internet’s infrastructure and security. In the last ten years I have interviewed over 100 actors across these communities, at over 40 network operations and cybersecurity conferences around the world. Since completing my PhD, my engagement is best categorized as impact-driven science diplomacy. By demonstrating I speak technical, political, and business vernaculars, I have established a reputation as a trusted honest broker that brings a deep understanding of the complex, sociotechnical governance and management problems endemic in establishing collaborative engagement between these transnational institutions, policy makers and regulators, and law enforcement. I have developed rare (and hard won) access to diverse formal and informal institutions critical not only to combating cybercrime, but that also provide the access and empirical evidence necessary to developing rich, theory-based understandings of the kinds of collaboration necessary for keeping pace with continuous innovation by cybercriminals.

As a research fellow and advisor to the Anti-Phishing Working Group (APWG), I chaired the 2018 Symposium on the Policy Impediments to e-Crime Data Exchange, bringing together cybersecurity experts, lawyers, and policy-makers to highlight the GDPR as an opportunity to resolve the tensions between operational security groups, advocacy groups, and data protection authorities wrestling with tensions between privacy and security challenges. APWG’s Secretary General Peter Cassidy recently shared that a number of participants from the 2018 Symposium indicated it was one of the most impactful meetings they have attended. This year we are continuing this work, planning an annual series of Cybersecurity Data and Governance Symposia to kick off in November 2022. Also with the APWG (in collaboration with Dr. L. Weissinger at Tufts’ Fletcher School of Global Affairs) we evaluate the perverse incentives created by ICANN’s ill-conceived GDPR compliance. The research findings will contribute to a collaboration with Senator Ed Markey’s (D, MA) staff to develop model legislation to ensure the accessibility of data critical to cybersecurity incident response.

As a senior advisor to the Messaging, Malware, and Mobile Anti-Abuse Working Group (MAAWG), starting in 2016 I worked with the MAAWG Board to redesign their Outreach initiatives, creating and leading programs developing anti-abuse capabilities and capacity in Latin America and the Caribbean, Asia Pacific, and Africa, considering each regions’ culture, values, and resource endowments, including critical support for engagement with regulators, law enforcement, and international organizations. I am also the co-chair of MAAWG’s IoT Special Interest Group (SIG), working with Internet Service Providers (ISPs) to understand and evaluate the feasibiliy of IoT reputation models. I have included reference letters detailing these engagements from APWG and MAAWG leadership in the supporting documents.

Working with global partners in the cybersecurity, law enforcement, and policy communities, I apply my research on collaboration and governance to the development of impactful organizations that continue to develop cybersecurity capabilities and capacities in developed and developing regions. This engagement provides unique insights critical to my work. Understanding the real-world challenges of developing these collaborations provides rare, valuable, and pragmatic empirical evidence for both theory- and policy-relevant research contributions. On-the-ground work also provides unique perspectives into the diverse cultural and regional challenges facing Internet infrastructure development and security. These insights facilitate both impactful, responsible engagement and contribute significantly to my research-led teaching.

**Teaching** Understanding the social, political, and economic challenges presented by emerging trends in Internet operations, operational cybersecurity, online platforms, and cybercrime requires engaging students in contemporary, real-world problems. In my current role I developed my department’s Cyber Policy Concentration [[1]](#footnote-1) from the ground up, creating a comprehensive curriculum and development programme for masters students coming from diverse disciplinary backgrounds. This interdisciplinary, research-led programme (now in its third year) provides accessible deep dives into digital technologies that highlight the politics of these complex systems’ design, operations, and security.

The four courses I developed and teach in this program have been well received by students and faculty:

* *Introduction to Cyber Policy* offers foundations in policy and governance issues related to Internet infrastructure management, jurisdiction and attribution challenges, privacy and surveillance, encryption, consolidation, disinformation, and cybercrime, among others.
* *Data Science and Visualization for Policy Analysis* focuses on applying exploratory data analysis methods, such as cluster analysis and visualization, for hypothesis generation and case selection. Although based on R, I have specifically designed this course for students with little to no programming experience; it can be scaled down for undergraduates or up into doctoral level course. I have included the flier and syllabus for this course in the attached supporting documents.
* *Internet Infrastructure: Platforms and Politics* focuses on the governance and politics of online platforms and infrastructures that intermediate our social, political, and economic lives (such as Facebook, Google, and mobile platforms). This is an advanced course for students interested in a deeper dive into topics such as the politics and transnational security challenges facing specific elements of the infrastructure such as submarine cables, Internet routing, and the nuanced intersection of platform economics and security.
* *Advanced Cyber Policy* takes a deep dive into the diverse complex of institutions shaping Internet governance, political authority and legitimacy challenges facing these institutions in the broader global governance system, and co-regulatory approaches to effectively developing cyber policy.

I have also led group projects and cumulative capstones in which students engage with public and private stakeholders to apply these lessons first-hand. Building on my research, I have led capstones engaging with the National Cyber Forensics Training Alliance (NCFTA) and the FBI to understand the challenges of collaboration between private cybersecurity actors and international law enforcement, with a focus on business e-mail compromise, ransomware, and synthetic identity scams.

I have considerable experience teaching, developing, and evaluating technology and policy programmes, focusing on a pedagogy that integrates understanding the technical (complex system) dynamics necessary for rigorous, evidence-based technology policy analysis and prescriptions. This balance prepares students to be not only effective analysts and scholars at the policy-level, but to also serve as the increasingly important bridge between technologists and state actors on topics such as privacy and surveillance, cybersecurity, disinformation and misinformation, platform politics, and transnational infrastructure management. This fundamentally interdisciplinary education in technology policy is in increasingly high demand by students, academia, and public and private sector employers—I cannot count the number of times colleagues in both the public and private sector have asked me to send them good students that understand the nuance of the technologies at play, *and* domestic and international policy processes. I am extremely excited at the potential opportunity to further develop both the applied and theoretical elements of this curriculum with colleagues in STEAPP and the DTPL. I also welcome the opportunity to adapt my curriculum to complement existing undergraduate, masters, and doctoral curricula. In particular, I believe my interdisciplinary background in engineering systems, political economy, and cybersecurity could substantively contribute to the Centre for Doctoral Training in Cybersecurity.

I am quite excited at the prospect of bringing my ongoing research projects, teaching, access to expert networks, and engagement initiatives to STEAPP. Please do not hesitate to contact me at [jesse.sowell@gmail.com](mailto:jesse.sowell@gmail.com) or +1 517 214 1900 with any questions about this application. Thank you for your time and interest, I am looking forward to hearing from you.

Sincerely,

1. Concentrations are similar to MPA routes in STEAPP. Our two-year masters requires students to complete two (optionally three) concentrations to graduate. [↑](#footnote-ref-1)