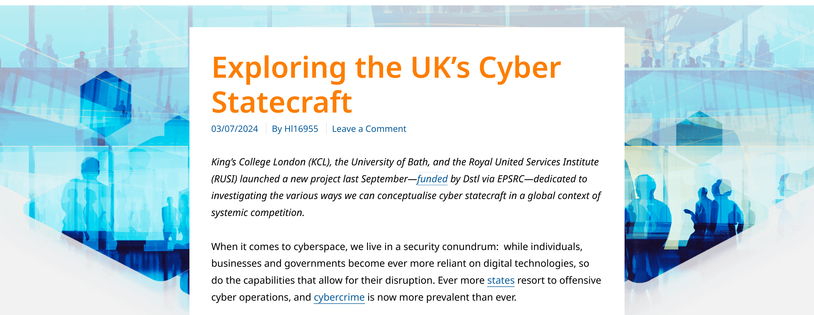

Exploring the UK's Cyber Statecraft

03/07/2024 By HI16955 | Leave a Comment

King's College London (KCL), the University of Bath, and the Royal United Services Institute (RUSI) launched a new project last September—funded by DstI via EPSRC—dedicated to investigating the various ways we can conceptualise cyber statecraft in a global context of systemic competition.

When it comes to cyberspace, we live in a security conundrum: while individuals, businesses and governments become ever more reliant on digital technologies, so do the capabilities that allow for their disruption. Ever more states resort to offensive cyber operations, and cybercrime is now more prevalent than ever.

Efforts to develop the rules, norms and values of cyberspace express competing political visions of what and who cyber security is for. What is more: these efforts reflect shifting international power dynamics. Liberal democracies advocate for an open and interoperable system, involving a multitude of stakeholders—from NGOs to the private sector—in its governance. This is challenged by China, Russia, and their strategic partners, who champion models of cyber sovereignty based on national territories and interests.

It is in this competitive environment that the UK's Integrated Review and National Cyber Strategy have outlined the country's ambition of projecting itself as a 'responsible, democratic cyber power'. This pathway includes exerting influence in international cyber security based on liberal democratic values. The question remains as to which liberal values should be applied to national and international policymaking with regards to cyber activities. What are the necessary institutional steps and relations that the UK must establish to be successful? What is considered responsible or irresponsible state cyber practice? How can the UK engage in sound and responsible cyber statecraft?

The University of Bath and King's College London organised the workshop "Cyber Statecraft in Practice: Mapping the UK's Actorness in Cyberspace" in February 2024 to explore some of these questions. It identified and examined the different elements that make up the UK's cyber statecraft in theory (what is cyber statecraft?) and in practice (what is the institutional and normative landscape?).

What is Cyber Statecraft?

Statecraft can be seen as the 'art of conducting state affairs'. It involves the construction of long-term strategies used by countries to achieve their national interest. In cyber statecraft—*the combination of multiple strategic approaches for securing the national interest in and through cyberspace, using all levers of national power and marshalling the private sector and civil society in a 'whole-of-society' effort*—practitioners must confront novel threats and opportunities that demand policy responses even if they do not grasp their technical nature and security implications. Indeed, the nature of cyberspace presents multiple challenges to traditional ways of thinking about statecraft. Its ease of access (including to offensive tools), borderless nature, private-sector predominance, and profound centrality to advanced societies and economies distinguish it from all prior forms of statecraft.

Engaging with Responsible Cyber Statecraft

Cyber statecraft is also linked to questions of responsibility. Responsible state behaviour in cyberspace requires a great degree of legitimacy to build trust and confidence, and cooperation in norm creation and interpretation. Transparency is also key to ensuring responsible state behaviour, as it can facilitate communication, cooperation and trust-building among countries. Inclusion—particularly of non-governmental actors—is essential. Greater representation of previously underrepresented groups can improve the diversity of outcomes and enhance the openness and legitimacy of cyber statecraft.

There are, however, different interpretations of what responsible cyber behaviour can involve. More importantly, responsible and irresponsible behaviour in cyberspace are not necessarily opposite terms: context plays an essential role when determining what different responsible behaviours entail. State actions play a key role in shaping perceptions about state responsibility in cyberspace and influence emerging international law and norms. State actions also condition how threats are addressed, such as supply-chain vulnerabilities and the growing fragmentation of cyberspace governance.

Cyber Statecraft: Role and Use

Exploring statecraft—that is, the art of conducting state affairs—can help us better address the unique challenges engendered by cyberspace. Engaging with cyber statecraft can address questions about how to ensure UK's cyber security. It can also help to keep assets safe and reduce cyber threats by collaborating with international partners and allies. These threats are multifaceted and transcend the traditional categories used to classify them (particularly between state and non-state actors). This makes cyber statecraft an essential theoretical and practical tool in service of the UK's aspiration to become and act as a responsible and democratic cyber power.

All these different questions and topics have important links to the core policy and security concerns of UK cyber statecraft. They involve different aspects of cyber statecraft, such as its diplomatic and security aspects. It is only by engaging with cyber statecraft as a concept that we will be able to understand the theoretical, empirical and normative dimensions of state interactions in and through cyberspace.

– Carmen Chas (University of Bath) and André Barrinha (University of Bath), June 2024

Filed Under: Uncategorized

PREVIOUS

RISCS PGR Placement: Kester Brookland

NEXT

Cyber Statecraft in an Era of Systemic Competition – project workshop write up by Kester Brookland

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Anti-spam*

Anti-spam word

To prove you are a person (not a spam script), type the words from the following picture or audio file.

Name * Email *

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT