Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Editorial introduction

Joyce Hakmeh

To cite this article: Joyce Hakmeh (2020) Editorial introduction, Journal of Cyber Policy, 5:2, 159-162, DOI: 10.1080/23738871.2020.1808033

To link to this article: https://doi.org/10.1080/23738871.2020.1808033

JOURNAL OF CYBER POLICY
2020, VOL. 5, NO. 2, 159–162
https://doi.org/10.1080/23738871.2020.1808033

Routledge
Taylor & Francis Group

Editorial introduction

How can this generation avoid being remembered as the generation that ruined the early promise of the internet? in his remarks to the last Internet Governance Forum, the UN Secretary-General's response focused on the importance of a collective effort that addresses the digital, social and political divides currently threatening an accessible, free, secure and open internet. But how can we achieve this amidst a number of challenges that include a constantly changing landscape, the proliferation of malicious actors and the fusion of technology with geopolitics, economic competition and international affairs? A good starting point could be to establish better connections between the different digital areas and to have an in-depth understanding of the intersection between them as well as their impact on the socio-economic and political dimensions.

How for instance is technological development impacting on human rights and democratic processes? What is the importance of technical standards and why is maintaining the existing internet architecture crucial not just for its resilience but also for protecting human rights? What are some of the national, technical and local responses that countries can opt for? Volume 5 Number 2 of the *Journal of Cyber Policy* brings together a collection of articles which try to answer these questions.

Cameran Ashraf discusses in the first article the impact of AI on the rights to assembly and association online, highlighting multi-stakeholder efforts that could be deployed to protect those rights. Adam Henschke, Matthew Sussex and Courteney O'Connor stress in their article the magnitude of the threats emanating from foreign influence campaigns in the cyber sphere to the democratic processes and states, suggesting several measures to safeguard against such hostile interference. Christopher Whyte talks in his article about DeepFakes and their impact on the political integrity and security of democratic institutions and states, outlining what policymakers can do to respond to these threats. Ying Miao offers insights into managing digital contention in China and how the incentivisation of grassroots reporting has become a key strategy of internet governance by the Chinese Communist Party.

Stacie Hoffmann, Dominique Lazanski and the Journal's editor Emily Taylor discuss in their article the efforts that China is exerting in international standards organisations to legitimise its new technologies; the article delves into China's latest proposal, the 'new IP' and the impact that this could have on the resilience of the internet and the human rights of its users. Eugenio Lilli talks in his article about President's Obama's pioneering role in adopting a structured holistic approach to internet governance in the US. Eviatar Matania and Eldad Tal-Shir discuss the importance of continuous terrain remodelling (CTR) as an effective strategy for disrupting most phases of cyberattacks. In the last article of this issue, William Hatcher, Wesley L. Meares and John Heslen propose a series of policy recommendations – based on a detailed survey of 168 US municipalities – to empower municipalities to effectively implement their cybersecurity policies. The issue concludes with a book review.

Artificial intelligence and the rights to assembly and association – Cameran Ashraf

The academic literature on the impact of Artificial Intelligence on human rights has focused primarily on the rights to privacy and freedom of expression. Cameran Ashraf discusses the impact of AI on the 'neglected' rights to assembly and association online. Ashraf shows how AI can be used to determine what content we see, whether through personalised newsfeeds or search results, or through AI-driven content moderation. These practices risk limiting rights to assembly and association online. Ashraf concludes with policy recommendations, emphasising the need for state and corporate efforts to protect freedom of assembly and association.

Countering foreign interference: election integrity lessons for liberal democracies – Adam Henschke, Matthew Sussex and Courteney O'Connor

Drawing upon the case study of the 2018 midterm elections in the US, Adam Henschke, Matthew Sussex and Courteney O'Connor identify five vulnerable components of liberal democracies (the five 'I's): democratic institutions, election infrastructure, private industry, individual citizens and the ideas that undergird democratic norms. The vulnerability of each component is explained, and it is maintained that the greatest threat to democratic processes and states is posed by 'foreign influence campaigns in the cyber sphere' – principally including the targeting of social groupings and individual voters with disinformation. Sussex, Henschke and O'Connor propose eight measures to safeguard democracies and democratic processes from such hostile interference.

DeepFake news: AI-enabled disinformation as a multi-level public policy challenge – Christopher Whyte

Developments in AI systems have engendered a new challenge for those who seek to eliminate fake news and disinformation in the digital realm: such systems now facilitate data-tampering and the generation of 'DeepFake' content. Christopher Whyte maintains that whilst DeepFakes do not constitute 'a revolution in disinformation techniques', the burgeoning ability to produce them rapidly and at scale, combined with the appropriation of neural networks to outwit fake-detecting algorithms, place the digital information environment at greater risk than ever before. Whyte delineates how increasingly sophisticated DeepFakes may impact upon the political integrity and security of democratic institutions and states, and outlines how policy-makers may respond to these threats.

Managing digital contention in China – Ying Miao

While top-down censorship is a well-known method of content control in China, the development of peer-to-peer reporting culture has been established under the Xi administration. Ying Miao demonstrates how the incentivisation of grassroots reporting has become crucial for a flexible and adaptive strategy of internet governance by the Chinese Communist Party. Using the *People's Daily* as a case study, she examines the differing strategies adopted by the Chinese Communist Party to mediate and demobilise contention around key events. Miao argues that the single party state legitimises certain socio-moral grievances while closing off others, creating certain areas of online politics which are controlled through participatory management.

Standardising the splinternet: how China's technical standards could fragment the internet – Stacie Hoffmann, Dominique Lazanski and Emily Taylor

Stacie Hoffmann, Dominique Lazanski and the Journal's editor, Emily Taylor, examine China's drive to standardise technologies which alter the internet's fundamental architecture to reflect local policies. The authors examine China's strategy of undermining trust in existing internet infrastructure and how its proposed new standards would necessitate a multilateral, top-down approach to internet governance. New Chinese technologies would then be legitimised and adopted in the global marketplace through the Belt and Road Initiative. The authors discuss how, in a worst-case scenario, the splintering of internet technologies could increase the internet threat landscape and they make recommendations for governments to intensify collaboration in order to limit the ramifications of fragmentation.

President Obama and US cyber security policy – Eugenio Lilli

The Obama administration can be recognised as a critical turning point in the history of US cyber policy and of international internet governance. Eugenio Lilli observes that although cybersecurity policy had been discussed since at least the 1960s, it was only under the Obama administration that it became a national security priority. The era saw a transition of US cyber security policy from a collection of ad hoc and sector-specific measures to a holistic approach. Lilli states that Obama's individual leadership played a key role, examining his personal interest in the field, statements from campaign speeches and specific actions taken to develop a structured holistic approach to internet governance.

Continuous terrain remodelling: gaining the upper hand in cyber defence – Eviatar Matania and Eldad Tal-Shir

A growing body of scholarly opinion challenges the received wisdom that in cyberspace, offence has the advantage over defence. Eviatar Matania and Eldad Tal-Shir propose the use of continuous terrain remodelling (CTR) to create asymmetric advantages for defenders in cyber conflict by taking advantage of the malleability of cyberspace and their genuine ownership of the 'cyber terrain'. The authors demonstrate that by adopting CTR, defenders can take the initiative, rather than playing catch-up with offensive technologies. They argue that CTR can be effective in disrupting most phases of cyberattacks, even in some cloud-based architectures. They conclude with an expected trajectory of offensive actions in an era of terrain remodelling.

The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices – William Hatcher, Wesley L. Meares and John Heslen

William Hatcher, Wesley L. Meares and John Heslen offer an evidence-based study of the cybersecurity policies of cities in the United States. The article examines responses to a detailed survey from 168 municipalities with populations greater than 10,000. While more than 70 per cent of municipalities have a formal cybersecurity policy, only one-third maintain a record of cyberattacks against them; the levels of training are low and few cities work with outside orders or professionals to review their policies regularly.

The authors propose a series of policy recommendations to address these shortcomings, and call for increased funding to enable municipalities to effectively implement their cybersecurity policies.

Joyce Hakmeh
Co-Editor, Journal of Cyber Policy, Chatham House
JCPeditorial@chathamhouse.org