Lech J. Janczewski and William Caelli (Eds). (2020). ***Cyber conflicts and small states*****. Oxford: Routledge, 232pp, ISBN: 978-0-367-59726-9. UK£36.99.**

Cyber conflicts and small states offers a compelling account of the various technological, institutional, regulatory, and normative factors influencing the cyber security of small states in the 21st century. With cyber infrastructure as the focal point of analysis, the authors explore how both technological dependence on larger states and a lack of effective civilian-military cooperation and planning can be detrimental to cyber resilience. They conclude with numerous policy and practical recommendations to tackle the issues highlighted throughout the text.

The authors trace the current state of affairs back to the disintegration of the bipolar international system in the late 1980s, producing a new order of multipolarity in which software (particularly firmware) became increasingly productised and commoditised. The book locates emerging security challenges around cyber-warfare, cyber-crime, and cyber-terrorism within this half-century transitional period, featuring the proliferation of Commercial-Off-The-Shelf (COTS) technology products and how increased availability has lowered the barrier to entry for cyber-attacks against states and their critical infrastructure. This amounts to a ‘meshing’ of sovereignty, where lines between states and non-state actors have been obfuscated and the Westphalian order is imploding. Cyber asymmetries are identified as a key variable in the analysis, with the capacity for covertness and plausible deniability of cyber operations also examined in detail.

Editors Janczewski and Caelli underscore the dichotomy between ‘technology producers’ and ‘technology consumers’, with small states almost exclusively falling into the latter basket. These consumers often find themselves beholden to the interests and goals of their larger counterparts, who dominate the technological landscape. The authors interestingly note how close corporate and government collaboration in controlled technologies means that certain governments can exercise authority to influence their development, to the benefit of the producer state (such as installing spyware or other backdoors). From this analysis, the authors expound how structural technological imbalances – accelerated by the emergence of great powers as technological centres of gravity – have generated asymmetries between small and large states. They then tease out the second-order effects on the modern nation-state, its sovereignty, and also its ability to protect and promote its security, prosperity, and interests with an ever-expanding and diversifying threat matrix.

The text then studies how the asynchronicity of technological change and legislation has left many states playing catch-up, often without policy tools to address root problems and – importantly – prepare for future developments through resilience-building. Further, the inherent vulnerability of cyber systems attributed to COTS is identified as systemic, so the authors draw system-wide policy recommendations and best practices to address this issue within small states, including the foundational role of deeper public-private sector collaboration. The proposed countermeasures section of this book therefore places a strong emphasis on business continuity and resilience, bolstering critical national infrastructure, and prioritising inter-agency response instruments which encompass private sector stakeholders in decision-making processes. Trust is central to this framework, underpinning any planning around the countervailing forces explored earlier (namely, data haemorrhaging, limited talent pools and human capital flight, dependence on global value chains, and deep-rooted cyber vulnerabilities). The authors emphasise the power of learning from other states’ mistakes to reduce the learning curve and associated costs of experimentation.

Cyber conflicts and small states is the product of considerable research expertise and experience in this domain, including insights from high-level practitioners such as William Caelli, Ian Fletcher, Hendricus Luiijf, and Chris Roberts. Their work places heavy emphasis on the technical aspects of top-down cyber strategy, some of which can seem arcane to an outsider. However, one inherent weakness of this text is the outsize focus placed on states which would not traditionally be classified as 'small' and are incompatible with the political, technological, and socio-economic conditions of most small states in the world.

The case selection may have been impacted by biases pertaining to the authors' past exposure and experiences. For example, Australia, New Zealand, Poland, and the Netherlands are employed as case studies in a dedicated chapter, entitled 'National Cyber Security Organisation'. While the cyber security postures of these states prove to be interesting cases from which many lessons can be derived, the dimensions of this analysis may not be directly applicable to some small states. Interestingly, the authors do not explicitly articulate the definition of a small state being employed throughout the text; rather, small states (referred to as 'technology colonies') are only identified in contradistinction to large states, the designated technology providers in the international system. This lack of methodological clarity presents some challenges for the generalisability of the findings, compounded by the concentration on economically developed and liberal democratic states situated in the Global North. It can therefore be argued that the readership which can derive actionable insights from this text is significantly impeded by its case study selection and that greater cross-case applicability is needed in further studies: to speak, for example, to the circumstances and needs of Small Island Developing States (SIDS).

While it is clear that *Cyber conflicts and small states* makes significant technical and analytical contributions to the literature, the broader strategic and theoretical implications appear to be underexplored. Despite mention of Huawei and ZTE, the book fails to elucidate the ongoing Sino-US technological decoupling and its potential implications for small states in particular. Although a passing remark is made to global value chains in the semiconductor industry, this would have been an excellent opportunity to consider Taiwan's unique position, as a small state successfully leveraging specialised innovation ecosystems and deep domain expertise to more effectively defend its territorial integrity and national security.

Cyber conflicts and small states is nonetheless a valuable contribution to the literature on cyber conflicts and how small states can meet these challenges while reducing dependence on larger states in the international system. The key message communicated is that the needs of small states are fundamentally different from those of large states, which the existing literature is fixated upon. Janczewski and Caelli propose that small states should focus on integrating civilian enterprise with national infrastructure, building sustained resilience through deeper collaboration in the cyber domain. This thesis that small states require a more holistic approach to cyber security due to international power imbalances is supported by a wealth of evidence analysed in the book, offering a sustained, convincing argument to readers.

Jamie Croucher
Department of War Studies
King's College London
United Kingdom
jamie.croucher@kcl.ac.uk