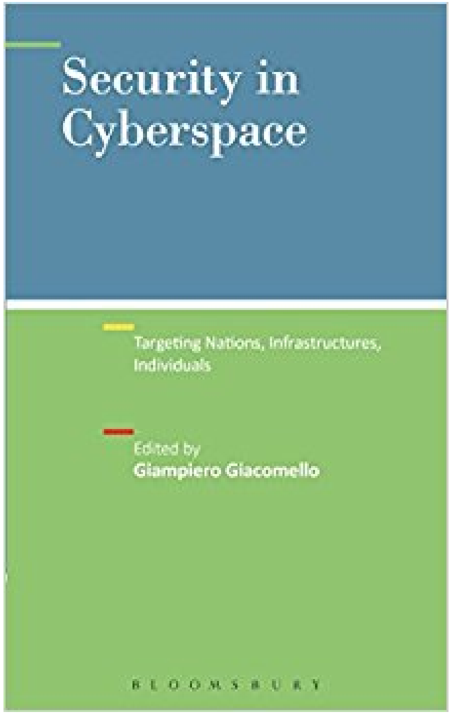
Book Review: Security in Cyberspace: Targeting Nations, Infrastructures, Individuals edited by Giampiero Giacomello

blogs.lse.ac.uk/lsereviewofbooks/2015/01/02/book-review-security-in-cyberspace-targeting-nations-infrastructures-individuals-by-giampiero-giacomello/

02/01/2015

Giampiero Giacomello's edited collection is a welcome addition to the still sparse academic literature on cybersecurity, writes Patricia Hogwood. Framing diverse perspectives is never easy, but Giacomello sets an accessible yet analytically challenging framework for a wide-ranging discussion on the emerging field of cybersecurity.

Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. Giampiero Giacomello (editor). Bloomsbury Academic. 2014.



Find this book:

Developments in the economy of cyberspace have prompted a shift from a proprietary system restricting use to governments and major organisations to a global system open to almost all at minimal cost. Awareness of the need to protect national and global critical infrastructures from cyber-attacks has grown since the early 1980s (The 'Tengelin Report', 1981), promoting a securitisation of cyberspace. High-profile cases and statistical evidence illustrate the types of threats facing nation-states and individuals: Google's clash with the Chinese government; breaches of security systems by hackers; use of Twitter and Facebook to mobilise support during the Arab Spring; the explosion of cybercrime against individuals; breaches of web privacy perpetrated by the National Security Agency (NSA); and whistle-blowers including Edward Snowden and Private Chelsea Manning.

This volume focuses on the concepts and empirical realities of cyberthreats to the nation state, and to the infrastructure and the individual. It draws on European and US perspectives, alongside a solitary contribution from China. Giacomello's introduction frames the volume well. He clearly draws out the separate strands in cybertechnology, explaining how each presents a threat to sovereign states in terms of their physical security; 'semantic' security (threats to the ways in which the state is perceived from the outside); and 'syntactic' security (threats to the software and protocols controlling network flows). At the level of physical security, nation states are increasingly interested both in cyber-defence and the potentialities of cyber-offence as a precursor to, or to avert, conventional warfare. Individuals are largely concerned with the syntactic level that allows full use of the social function of cyberspace without risk to their personal security or information integrity.

Giacomello draws on 'principle agent theory' (PAT) as an analytical approach to cyberspace relations. He argues that, in cyberspace, the government must delegate some of the defence and maintenance of crucial infrastructures to private agencies, and, in some cases, to users of cyberspace. The security of 'national' access to cyberspace may be compromised by the complexity of principal-agent relationships and incentives/sanctions that arise from the interdependence and multiple ownership of cyberspace infrastructures. While a PAT approach is certainly plausible and helps to visualise the phenomenon of cyberspace (ab)use, it needs further elaboration than the edited volume format allows to address the ambiguities and 'fuzzy boundaries' of these interdependencies. The weakest link in the infrastructure is identified as the joint ownership by public and private stakeholders whose interests and responsibilities overlap to such an extent that the whole public-private 'partnership' is characterised by ambiguities. The frightening reality is that, driven by the neoliberal logic of the market, stakeholders fail to coordinate and invest in the kind of ‘failsafe’ mechanisms that could guarantee security in a failure or breach of any part of the system.

The work is planned around the levels of ‘target-victim’ of cybercrime as defined by the network’s structure and principal stakeholders, namely: nation-states, infrastructures (owners and stakeholders) and the individual users of cyberspace. This analytical ‘triad’ translates as two sections in the book, one on the national/state level of target analysis and one linking the infrastructural and individual concerns. Nevertheless, the inherent complexity of the subject area is never glossed over and case-studies typically incorporate elements of all three analytical levels, if from a more specific standpoint.

Stand-out chapters include Mattioli’s conceptual engagement with cybersecurity as a ‘paradigm in progress’. She examines how the nature of cyberspace and organised efforts to respond to threats in this sphere are redrawing the parameters of security. Kang’s chapter on the Chinese perspective draws attention to the challenges of cybersecurity in a developing country and also of the relevance of cultural predispositions in understanding state-stakeholder relationships. Within the infrastructure/individual ‘target-victim’ section, Giacomini and Cordani’s examination of the technical-legal dimension of cybersecurity helps to clarify the blurred distinction between legitimate and illegitimate usage of cyberspace and offer an insight into the implications of usage practices for human rights.

The book would really benefit from an analytical conclusion to draw together some of the suggestions put forward in the separate chapters, to work on an elaboration of the framing PAT approach and to more clearly identify future avenues for research. Over the course of the volume, the promising PAT approach rather fizzles out. A work on cybersecurity might perhaps be expected to incorporate a more rigorous exposition of ‘risk’. The book could also use a more explicit elaboration of the relevance of ‘semantic’ security for diplomatic purposes. The work is best suited as a launchpad for ideas and debate on the new governance challenges arising from the rapid and ubiquitous potential of cyberspace activities. The brief introductory guide to the literature of cybersecurity will be particularly useful to undergraduate and graduate students.

Patricia Hogwood is Reader is European Politics at the University of Westminster. She has published on UK devolution and EU policy-making in a comparative context. Her other research interests include EU immigration policy and the externalisation of internal security and the impacts of German unification on German identity, democracy and public policy.

-