Routledge
Taylor & Francis Group

European Security

ISSN: 0966-2839 (Print) 1746-1545 (Online) Journal homepage: http://www.tandfonline.com/loi/feus20

Cybersecurity in the European Union. Resilience and adaptability in governance policy

Andre Barrinha

To cite this article: Andre Barrinha (2016) Cybersecurity in the European Union. Resilience and adaptability in governance policy, European Security, 25:3, 387-389, DOI: 10.1080/09662839.2016.1160892

To link to this article: http://dx.doi.org/10.1080/09662839.2016.1160892

Published online: 30 Mar 2016.

regard to maritime security (p. 193). Due to the EU's limited resources and the fact that its power depends on its member states' willingness to act and spend resources, he thinks that the Union should concentrate "on activities that end up in concrete, quantifiable results and outcomes that member states, parliamentarians, and the public opinion in Europe can empathise with" (p. 194). In particular, he thinks that the EU should further strengthen the link between maritime security and sustainable development, which would be in line with the Union's benevolent image and allow it to develop an original approach to maritime security that originates in non-security considerations and contributes to both security and non-security objectives.

Although each chapter has a great deal to offer in its own right, the book's main contribution is the creation of a framework for analysing EU maritime security. This framework will make it easier for scholars to think about the subject and build on the literature that already exists. Therefore, future research should take advantage of it and build up the literature on different aspects of EU maritime security, such as the fight against specific threats, the management of maritime resources, or the protection of the maritime environment.

The book will appeal to a broad audience of undergraduate students, graduate students, established scholars, security experts, policy-makers, and anybody who is interested in and would like to learn more about EU maritime security, geopolitics, or International Relations. However, it will undoubtedly appeal the most to those who are interested in EU maritime security because it is currently the only book on the subject available on the market. Thus, the book is almost guaranteed to become the go-to source on EU maritime security.

Niklas I.M. Nováky
University of Aberdeen
✉ niklas.novaky@gmail.com

http://dx.doi.org/10.1080/09662839.2016.1145115

Cybersecurity in the European Union. Resilience and adaptability in governance policy, by George Christou, London, Palgrave, 2015, xiii + 222 pp., £68 (hardcover), ISBN 978-1-137-40051-2

With the advent of the European Digital Single Market and the (ever) increasing presence of information and communication technologies (ICTs) in our daily lives, Europe's security is, to a large extent, its *cyber*security. The European Union (EU) is fully aware of this fact and has, particularly in the last decade, approved a number of measures in order to address the inevitable risks that come from the intensive use of ICTs. Interestingly, this seems to be an issue that has, so far, deserved limited attention of the academic community dedicated to the study of Europe and European Security. George Christou's book is, in that regard, a significant contribution to what will hopefully become a vibrant area of research in the near future.

Divided into eight chapters, *Cybersecurity in the European Union* explores the EU's developments in the three main pillars of the 2013 EU Cybersecurity Strategy: cybercrime, network and information security (NIS), and cyber defence. Before engaging in the concrete analysis of those three areas, Christou offers an overview of the global cybersecurity ecosystem and develops a conceptual framework that attempts to understand the EU efforts in cybersecurity from the prism of "security as resilience", a concept that focuses on the complexity and multi-layered character of the cybersecurity ecosystem and that comes in opposition to the more traditional approach of "security as control". According to the author, there are six necessary conditions for effective security as resilience in cyberspace: the capacity to adapt to new structures and "operating assumptions", the acceptance of complexity in governance logics, the development of trust-based partnerships between main actors, the shared acceptance of common understandings of key concepts, the adoption of a "culture of cybersecurity" among all stakeholders and, finally, the existence of coherence and consistence across levels and actors (p. 29). Put together, these six conditions constitute the basis for assessing the EU's evolution in the field.

Cybercrime is, in Christou's view, the most advanced of the three EU cybersecurity pillars, even if quite fragmented as "there is no overarching framework but rather a series of legal and regulatory instruments that overlap" (p. 102). In terms of NIS, the EU is progressively moving towards a more hands-on type of governance. The expected approval this year of the (contested) Network and Information Security Directive, which imposes significant obligations on companies and member states in terms of disclosing information related to cyber-attacks and incidents, will constitute an important landmark in the assertion of this type of cybersecurity governance.

Of the three domains, cyber defence is the least developed EU cybersecurity dimension (and the one that deserves less attention in the book), with Brussels' activities in this realm being strongly conditioned by both the member states' lack of interest in seeing this issue developed within the EU and NATO's efforts in the field. Although there is some degree of collaboration between both organisations, the room for the EU to develop an autonomous "security as resilience" in cyber defence has been very limited, with the European Defence Agency currently being the EU's best hope of influencing Europe's cyber defence agenda (p. 143).

In terms of member states, although there is some visible progress and an emerging shared understanding of the need to develop a resilient cybersecurity ecosystem, overall, member states still evince very different levels of cybersecurity maturity and "significant barriers exist" (p. 182) in that regard. The UK is presented as being among the leading European states in the field and Christou uses it as a "case study" of a national approach in chapter 4. The UK's "hands-off" approach to cybersecurity governance contrasts with the more "hands-on" approach the EU is veering towards and cultural clashes between Brussels and London have and will continue in this field, particularly in the NIS domain. Following this approach, it would have been interesting to see how the British case compared with, for instance, France's or Germany's.

Before offering some concluding remarks, the author discusses the current state of transatlantic relations in cybersecurity, mapping the progression of this relationship and problematising the effects of Edward Snowden disclosures. The EU and the USA have much in common in this field, and cooperation, particularly against cybercrime, has been very successful, but there are significant frictions in terms of data protection, internet governance and cyber defence. As the author concludes "if effective security as resilience is a real objective […] then the US and EU […] must, in the short term, have a serious conversation – and find a compromise – on the logics that underpin their respective approaches" (p. 170). Many questions could be raised regarding the normative position the author adopts here, and the book could have potentially explored it in further detail, but that would have probably taken the whole discussion in a completely different direction.

Cybersecurity in the European Union ends with some research recommendations for the future, including a more thorough analysis of the 28 member states' national cybersecurity approaches and an empirical study of how "resilience is performed in cybersecurity contexts" (p. 187), in a clear recognition by the author that there is still quite a lot to do in this field or research. Overall, this is an excellent exercise in exploring the largely uncharted territory that is the EU's approach to cybersecurity. Christou's work will hopefully help trigger the academic debate on the prospects and pitfalls of EU's actorness in this field.

Andre Barrinha
Politics and International Relations, Canterbury Christ Church University, Canterbury CT1 1QU, UK
✉ andre.barrinha@canterbury.ac.uk

http://dx.doi.org/10.1080/09662839.2016.1160892