2
Conceptualising Security as Resilience in Cyberspace

Introduction

Many cybersecurity strategies within and beyond Europe refer to developing effective cyber resilience, but without adequately defining and deconstructing what resilience is, what it looks like at different stages, and the preconditions and governance forms required to achieve it. Approaches to cybersecurity thus far have been theoretically and conceptually eclectic – utilising traditional and critical theories of International Relations (IR) and concepts such as cyber power. This chapter will – in line with the main purpose of this book – draw on existing theorisations of cybersecurity more broadly, and add to them through interrogating resilience and security governance in order to create a holistic approach to assessing the evolution of the European Union’s (EU) ecosystem for cybersecurity governance. Moreover, it will seek to provide a frame of reference for not only understanding the ‘Internet interconnection system’ (ENISA 2011c) but more specifically the conditions that can potentially lead to cybersecurity as resilience across the European space.

Furthermore, this chapter will explore and define the concepts of resilience and security governance and delineate how they will be operationalised in analysing EU cybersecurity. The aim will be to fuse the literature on resilience and security governance in order to construct and establish a security as resilience approach. This will allow the characterisation of emerging governance in the EU Cybersecurity Strategy and more importantly, how this equates to achieving an effective security as resilience in Europe. Whilst such a frame no doubt has synergies with existing conceptual work, it will also add to such literature, not least by introducing different understandings of resilience through which cybersecurity governance can be understood and assessed.
In short, it is the aim of this chapter to provide a framework and conceptual markers for explaining the evolution of the EU governance system for cybersecurity in order to provide a deeper understanding of how the EU can construct an ecosystem of resilient security governance with regard to questions of cyber threat. Such a framework will facilitate provision of a conceptually informed answer to the central questions that this book seeks to ask: How can we characterise and understand the EU’s evolving ecosystem of cybersecurity governance? To what extent has the EU been able to construct a comprehensive and resilient approach to cybersecurity within the evolving ecosystem? What is the nature of the resilient ecosystem emerging in the EU? The implicit argument running throughout the chapter and the book is that a more socio-ecological, adaptive and flexible form of resilience should drive the EU’s approach to cybersecurity in order for it to become an influential actor in cyberspace and a leader with regards to good practice in cybersecurity and its many different dimensions.

The chapter will be structured as follows to achieve its aim. The first section will provide a contextual overview and assessment of the way in which cybersecurity is theorised and conceptualised in the literature more broadly. The second section will then draw on the specific literature that will be used to construct the framework for the book; namely, resilience and security governance, and sketch out conceptual conditions and markers that can be utilised to understand the development of the EU’s emerging ecosystem of cybersecurity. This section will also articulate the relationship between the broader literature and the security as resilience frame constructed for analysis of the EU cybersecurity ecosystem. The final section will summarise the argument made in the chapter and the implications this has for the analysis in the book.

**Approaches to analysing cybersecurity**

Theoretically informed work on cybersecurity is surprisingly sparse, although growing rapidly. What does exist is focused on the US and other geographical areas (for example, see Kshetri 2013 on the Global South), with no comprehensive, theoretically driven analysis of the EU in cybersecurity. In terms of the existing literature a variety of approaches have been used to analyse the topic, ranging from traditional national strategic and managerial approaches (Libicki 2007, 2009; Janczewski and Colarik 2007; Mehan 2008; Janczewski 2008; Clarke and Knake 2010), to historical approaches (Carr 2009) and ‘terrorist’ oriented approaches (Verton 2003; Colarik 2006; Wiemann