



Regulating Security

Martin Lodge and **Andrea Mennicken** consider the growing currency of security in risk and regulation debates

Security is not a term that has enjoyed widespread currency in the field of risk and regulation. Most attention has traditionally been paid to questions of 'safety': how to ensure the mitigation of harm by controlling for deviating operating practices (such as allowing poorly maintained ships into harbours). Less attention has been paid to security: the mitigation of external threats (such as provisions for harbour screening systems). Such concerns have conventionally featured in the field of international relations.

Why, then, consider security in the context of risk and regulation? There are a number of reasons why security has become increasingly prominent in fields of study that have customarily been more interested in safety. For one, increased attention has been paid to the vulnerabilities of large critical infrastructures across countries – leading to the adoption of national risk assessment and management plans. Further, there have been changes in the field of civil protection and contingencies. The divide between the 'security state' of intelligence agencies, the police and the military, on the one side, and the 'civil protection' state, on the other, has become increasingly blurred, especially after 9/11, as evidenced by the creation of the Department of Homeland Security in the US. Similarly, the increased concern with 'societal security' has brought together agencies from the different 'security' and 'protection' fields.

To some extent, this blurring responds to changing perceptions of threat: cold-war era concerns with aerial bombardment have been supplanted by fears about attacks on critical infrastructures. The weekly siren drills to ensure that populations could be warned about an impending attack have vanished. Of course, the newness of such concerns should not be overplayed; states have been concerned with the security of energy (oil), water and food reserves to deal with potential disruptions for a long time. Similarly, announcements that individuals should stock sufficient

water and food supplies to maintain a certain degree of self-sufficiency, at least for short periods, are also nothing new, especially in areas prone to natural disasters.

However, there have also been some notable changes. Ideas about security have become more prominent and widespread. In the area of finance, reforms have sought to ringfence activities so as to make markets more secure from contagion. Ideas of food security have been revisited in the context of international production chains. Furthermore, the justification for civil protection has altered. There has been an increasing formalization of crisis infrastructures across European public administrations at all levels of government. There have also been changes in justification, for example, the German federal government's announcement of its new civil protection plan in the summer of 2016 stressed that the threat was not related to traditional warfare but stemmed, instead, from threats to critical infrastructures posed by cyber-security related attacks.

The importance of algorithms, online communication and energy infrastructures in everyday life has been widely discussed. These raise important questions for risk regulation, if alone in the context of scenario building exercises. For example, the modern classic 'Black-out' by Marc Elsberg was used as a reference point by the German Federal Minister of the Interior to justify the issuing of a new civil protection plan. In that novel, the sustained hacking into computer networks quickly destroys social and economic infrastructures across European states and the US. The awareness of growing vulnerabilities due to cyber attacks has also been noted in the context of attacks on national communications systems, voter databases, and nuclear reactors.

However, security issues do not just relate to questions of collective welfare and the protection of critical infrastructures. Algorithms are deployed by private and public organizations to

predict individual and organizational behaviours and preferences on the basis of collected data. Much of these data are collected in non-transparent ways (for example, via smartphones and other electronic devices). Generally, individuals casually consent to becoming 'quantified selves' in order to access 'convenient' online services.

The security implications of such a trend are at least twofold. The first concerns the security of the systems that gather data. These include worries with regard to the security of individuals about whom information exists that they themselves might not be aware of. Individuals are also unlikely to understand the algorithms that are being applied to target specific messages to them, whether these are links to advertisements, selected news outlets or other messages. There are also questions about the transparency and accountability of the algorithms themselves which, in turn, raises much wider issues about how to regulate artificial intelligence. Such issues become ever more problematic from a viewpoint of risk and regulation when data collection is used for granting access to public services, or to allow organizations to make discriminatory choices, such as differentiated pricing regimes in health insurance.

The security of the individual – in terms of protecting their right to privacy – often collides with broader, societal or governmental security considerations. Such concerns have given rise to various regulatory regimes dealing with phone-tapping and other extraordinary powers to invade an individual's private sphere. How such regimes are developed, how they are being held to account and with what consequences, are issues that have not enjoyed much currency in the wider risk and regulation literature.

The second major security implication relates to the security of the organizations gathering and utilizing information. The security of organizations' collected data is regularly questioned in view of high profile hacking or da-

ta-breaching incidents. Apart from concerns about firms' cyber security provisions, and suspicions about the motives of such hacking incidents, debates about how to develop regulatory standards in such a transboundary context remain largely under the surface.

This gives also rise to questions pertaining to the regulation of data-sharing across organizations. Under what conditions, for example, should private organizations be required to provide data to public organizations, if the latter claim to be acting on behalf of societal security? Indeed, as debates around Edward Snowden (and others) have shown, the public exposure of highly intrusive and extensive activities of intelligence services is seen by some as worthy whistleblowing to alarm the public about 'dangerous' activities of certain state organizations. For others, such whistleblowing activities represent attacks on the security of the state and its citizens (if not 'treason'). Others, in turn, might question whether standards are being applied to private and public organizations when it comes to data collection. Certainly, there is some qualitative difference in the case of state-based organizations that have the power to utilize information to restrict liberty directly. Nevertheless, in the case of private organizations, regulation might need to be applied against the interests of individuals and firms in order to 'defend' constitutional norms of privacy and the 'right

to forget' and to restrict data exchange between different applications. Such questions become ever more pertinent as certain online services become utility-like facilities – without access to such services, individuals are unable to fully integrate into social and economic life. In other words, the world of non-state cyber-security has reached a degree of publicness that calls for the development of regulatory regimes to protect individuals.

Harold Laswell in his classic 'The garrison state' of 1941 painted a picture of a future in which specialists of violence had replaced the specialists of bargaining (business). A modern-day Laswell (as arguably depicted in David Egger's *The Circle*) would most likely put his emphasis on data science specialists who enjoy considerable power through their knowledge, their capacity to identify individual preferences and lifestyles, and their ability

to deliver tailored messages to bespoke publics. In our contemporary world, critical questions therefore relate to the balance between individual and societal security and how national and regional organizations can seek to regulate such transboundary activities. This is not to say that all national power to regulate has vanished, as can be seen by the particular security arrangements regarding the data protection applicable to EU-funded proposals.

But security-related questions should also be more generally at the centre of debates about risk and regulation. Security assumes the existence of a threat. This threat is directed at a certain state of the world that is seen as desirable. The identification of threats (or 'the other') is a highly political process as is the definition of desirable states of the world deemed worth protecting. This raises questions as to what or who is being threatened, such as individuals or collectives. It also questions about 'who' is causing a threat, whether these are state or non-state, national or international organizations or individuals. Regulating security links to a world in which emergency powers exist and where private organizations are tied closely to state powers in order to allow for the continued functioning of critical infrastructures. It links to questions as to how much security an individual should be granted in view of potentially opposing interests by the security state. This hidden world that seeks to provide security requires more interrogation. The tensions that emerge in the regulation of security go to the heart of constitutional democracy. They are therefore of fundamental relevance to the study and practice of risk and regulation.

Martin Lodge is Director and **Andrea Mennicken** is Deputy Director of **carr**.

