TIM STEVENS, KINGS COLLEGE LONDON

CYBER SECURITY AND THE POLITICS OF TIME

Tempus fugit, the Roman poet Virgil reminded us, an observation that seems more apt with every passing year. We are living through the 'Great Acceleration' in human activity, precipitated by the 18th-century industrial revolution and catalysed by the information revolution of the present. Caught up in the webs of globalisation and computerised high-technology, we feel more than ever that 'time flies', as we struggle to keep up with the pace and scale of change. Few feel this more acutely than policy-makers and legislators confronted with the practical challenges of managing societal change in the national and global interest.

Cyber security is one field in which those charged with protecting populations are seemingly always playing 'catch-up' to the global information environment. Such is the dynamic evolution of malicious software, the diversification of cyber crime, and the proliferation of state cyber espionage and cyber warfare capabilities. Any attempt to regulate these phenomena appears a thankless and impossible task. And yet, against this backdrop, there is ample time for reflection and deliberation on what cyber security policy and strategy is required. There is no need to panic or to pursue ill-judged policies in response to the rapidity of global change. Indeed, being seduced by this speed and acceleration is the worst possible basis for drafting and implementing policy in pursuit of positive cyber security gains.

To understand this, we must appreciate there is no single time at work in the world but many. Multiple actors and processes operate at varying speeds and on different time scales and therefore make political and practical calculations at variance with those of others. In cyber security, for instance, computers work at fractions of time incomprehensible to humans, which is why we delegate tasks that require split-second responses to machines physically capable of making them. This automated software and hardware, and 'smart' systems, learn and adapt to stimuli and situations but are essentially 'dumb'. Cyber security specialists act as interfaces between these systems and the environment. They need to make rapid decisions, for sure, but their human temporality is a time for shaping the rules by which these technological systems act, not for interfering directly with the millisecond decision-loops of computers themselves.

At another temporal level again are policy and strategy. In democracies, policy-making occurs in institutional contexts of more attenuated deliberation and negotiation. While this might seemingly frustrate progress on key issues, such as public-private information sharing, there is no evidence policy made in haste is any better than policy crafted by slower means. The opposite is true: such is the significance of contemporary developments that we should be thinking longer and more carefully about how we tackle cyber security. Instead of rushing to keep up and being captured by narratives of the 'tomorrow is too late' variety, we need to think longer-term about the role that cyber security should play in our future. This might take two principal forms, one facilitating the other.

Societies need to determine what cyber security is for in the short- to medium-term and enable it in intelligible and socially productive ways. This requires a recalibration of what is of social value, not necessarily only what is of immediate national security or corporate interest. At present, we give too little consideration to the needs and rights of citizens, and too much to the demands of security agencies and big business. These constituencies are essential cyber security actors but the public good should be the principle that guides the allocation and investment of resources and the ethics and practices of cyber security professionals both public and private.

Building on this, our second concern must be with what cyber security will do in the long term. What sort of future world do we want? How do we secure a hyper-connected population and economy? What does security mean in the 'Internet of Things' or in 'smart cities'? How is privacy being reconfigured and what does this mean for society? Must we prioritise cyber-enabled surveillance as means of regulation and control, or can we imagine ways of enabling citizens to pursue their legitimate desires and goals? It would be incorrect and unjust to say that governments are not beginning to think through and consult on these issues, but much more needs to be done.

This much may seem obvious but the value of thinking about the temporal aspects of the politics of cyber security is twofold. It is essential to recognise that there are different time scales for the different actors in cyber security, from computers to citizens to government and international organisations. We should, of course, seek to reduce bureaucratic torpor and institutional inefficiency, but some distance between action and reaction can be a resource for improvement, not despair. For example, in the case of a major cyber attack causing infrastructural degradation and human harm, a rapid reaction should be reserved for responders not foisted on policy-makers. They must be encouraged and allowed to form policy that addresses the future, not over-reacts to the past.

Another valuable aspect of a more temporally sensitive approach is the recognition that neither time nor policy stands still. The politics and practices of security are constantly changing and we should embrace that instead of lamenting it. There is no perfect cyber security solution now, nor will there ever be, but there is a place for well-thought out policy. This will require courage on the part of policy-makers and no small degree of bipartisanship. The obstacle to good policy is not the speed or acceleration of the information age but the willingness of humans to work together for the public good. If politics is about visions of the future, there can be few more pertinent illustrations of this than cyber security.