REFLECTION

Cyber: Emerging Themes and Reflections

Prof Lesley Seebeck, Inaugural Chief Executive Officer of the Cyber Institute, Professor in the Practice of Cyber Security, Australian National University.

August 2019

About the Author

Professor Lesley Seebeck started as the CEO of the Cyber Institute, Australian National University, on 30 July 2018. Most recently, she was Chief Investment and Advisory Officer at the Digital Transformation Agency, arriving there from the Bureau of Meteorology where she served as Chief Information Officer from mid 2014 to late 2017. In March 2017, she was recognised as Federal Government CIO of the Year.

Professor Seebeck has extensive experience in strategy, policy, management, budget, information technology and research roles in the Australian Public Service, industry and academia. She has worked in the Departments of Finance, Defence, and the Prime Minister and Cabinet, the Office of National Assessments, and as an IT and management consultant in private industry, and at two universities.

Professor Seebeck has a PhD in information technology, an MBA, a Masters in Defence Studies and a Bachelor's degree in Applied Science (Physics).

The following forms initial reflections of my recent visit to Berlin and Brussels, as part of an Australian delegation sponsored through the Konrad Adenauer Foundation (KAS), and the questions our discussions subsequently raised in my own mind. I am grateful to KAS for the opportunity to engage with senior counterparts in Germany and the broader European security and economic organisations.

We've come a long way in the 30 years since the Morris worm, considered the first major attack on the internet—and not in an overwhelmingly positive direction. Cyber security is now part of any conversation about national security, economic certainty and societal well-being. And in those discussions, there are a number of common themes that lead to larger questions around cyber.

The increasing pressure on—and sense of urgency within—states to increase their cyber defences is quite evident. States typically have responded as we would expect. Government is reorganised, with new agencies emerging either as new constructs or agglomerations of the old. More often than not, they are based on or around existing security organisations, and so take on much of their progenitors' culture and worldview.

Governments also rely heavily on legislation and regulation: tools of the state. Yet legislation is tedious, slow and too often a blunt instrument, especially in new fields where the nation-state has little understanding or penetration. Good legislation takes time: concepts need to be tested; the community should be engaged and diversity of views canvassed; consequences should be fully understood and appreciated; and, critically, assumptions should be tested. While such due diligence may not be possible—especially a full appreciation of unintended consequences—it's clear that legislation rushed through in a hurry, often in response to a crisis or political pressure, rarely qualifies as good law. And poor outcomes that may have otherwise been foreseen with more forethought and caution don't merely degrade capability, they undermine trust and condemn government to a 'whack-a-mole' approach to cyber- and technology-triggered issues.

Similarly, many of the programs supported by governments reflect an internal consensus view of the problems and the skills needed to resolve a problem. Moreover, they seek to stabilise and to return to a known and understood norm. In a fast-changing world, that's less than optimal. There's a reluctance to think differently about the problem, or about how technology, society, economic drivers and the geostrategic situation may all co-evolve and fundamentally change the environment.

As a result, much of government support in cyber tends to focus on a narrow technical skill base, rather than a diversity of skills and conceptual frameworks. Proposed solutions are all too quickly reduced to a technical issue, to be resolved by technical staff with generally inadequate funds. But cyber is much more than the technology.

Those conversations mentioned above rarely touch on the technology itself. And so the deep, challenging and desperately-needed discussions about adaptation and transformation are avoided.

So it's little surprise that many of the prescribed solutions and funding aren't really hitting the mark. In some cases, that's a function of time: it takes years to educate and season graduates, for example. Government itself prefers to move slowly—and the consensus provisions required by the EU and NATO underline that preference.

There is a sense, too, that the pace of technological change and social disruption is leaving governments behind. Liberal democratic states, with rules of law, democratic processes, etc, feel increasingly vulnerable.

In contrast, illiberal and authoritarian regimes have fewer concerns about accountability and fewer qualms about using—and simply taking—technology to meet their goals, sometimes recklessly. They have also grasped, quickly and ruthlessly, the use of technology for control and suppression, just as they have understood the existential threats posed by those same technologies.

The temptation for liberal, democratic governments, is to mimic behaviours of their opponents: exerting increasing controls on their populations, decreasing transparency, and increasing means of access to the private lives and communications of citizens. Often those are incremental changes. But we should not forget is that while the changes may seem incremental, the powers and intrusiveness of the technologies, and the data collected, is increasing exponentially. As this data increases, we have tools to process it that mean that a small number of data points easily identifies individuals, even when data is de-identified. Privacy—a fundamental human need, often requiring anonymity—struggles and needs to be actively bolstered.

Continental European sensibility to such matters differs somewhat to the Anglophone world, possibly reflecting closer experience with the capriciousness and harms of authoritarian regimes. European data protection and privacy provisions offer a safeguard against over-reach, but it's not inconceivable that even European governments will bow to pressure to compromise on individual rights. Indeed, despite the EU's efforts to build consensus frameworks, those same frameworks offer sufficient scope to allow a range of behaviours and approaches across the EU.

Such diversity is good, inasmuch it is proving challenging for our governments and societies, in the West, to understand, anticipate and manage the changes being wrought on our societies by technologies and social and economic disruption.

Those challenges will increase, and the nature of current information technologies—which the West is largely responsible for creating—is such that attack is easier than defence, that tracking is easier than hiding, that replication is easier than destruction, that ambiguity is easier than integrity, and that contamination is easier than purity.

Because Western governments have had difficulty coming to terms with those fundamental changes to the economy and society, their conceptual models, and means of acting on the world are misaligned. Moreover, years of focusing on efficiencies in government, and the transfer of functions to the private sector, either as a deliberate policy (for example, the privatisation of critical infrastructure, or outsourcing of technical skills) or by being overtaken (the uptake of platforms for interaction or the democratisation of, for example,

cyber tools) have weakened government's own capacity to act.

In contrast, the scope, reach, scale and ability to act on the concerns of states—their economics, societies and security—are now available to private companies—Google, Facebook, Ali Baba, Weibo, Tencent, and others.

Where does that lead us?

First, I would suggest that there remains strength in liberal, democratic values, institutions and behaviours. They should not be discarded, and indeed should be upheld and promoted even more strongly. But they will need to be re-interpreted in this new, digital, data-heavy environment. To that end, the European efforts to protect privacy and the ownership of their own data by individuals are steps in the right direction—but only first steps.

We should not mis-interpret the nature and actions of authoritarian societies as meaning that they are inherently stronger, faster or better. Certainly, a control-heavy approach may generate short-term gains. But those controls make their society, and security, more brittle, less resilient, less adaptable and less capable over the longer-term. Fear does not create or sustain creativity, nor the questioning inherent to scientific activity, nor help build the trust that underpins healthy societies, economies or institutions.

Europe has a close acquaintance with the nature and consequence of societies that can be destroyed or created by fear. So—second—Western liberal democracies need to support the open spirit of inquiry, diversity of thought, and willingness to contest opinions, assumptions and authority that are their strengths. As Henry Farrell and Bruce Schneier argue[1], we have to be smart about how we secure open information flows and manage, dynamically, political stability, so that they benefit democracy.

There is much to share between Europe and Australia. And efforts such as those promoted by the Konrad Adenauer Foundation, including the exchange of ideas and experiences, are integral to that broader effort.

A third point. States are finding themselves on the defensive—and falling further behind. That's generated considerable concern in the business community. And so interest in counter-attacks and vigilante policies such as 'hacking back' are understandable: decision-makers are running out of options and businesses are frustrated with the inability of governments to provide a safe space for operations.

Failure to address those concerns will undermine the legitimacy of government, and of economic stability. Current efforts are falling short, and the direction of many policies in terms of simply constraining activities or undermining broader security exacerbates the problem; we need to start thinking differently about how to resolve those issues.

Fourth, we need better conceptual models around cyber in the geo-strategic context. Tropes such as 'cyber as nuclear', and even 'cyber as the fifth domain', fall short of the reality of technologies densely embedded in evolving civilian contexts. They also evoke unhelpful scenarios and reactions—especially the cyber-as-nuclear analogy.

Warfare has typically been a matter for states—at least since the Peace of Westphalia. But cyber offers means of coercion, control, and disruption that may be both deniable and available to actors other than nation-states.

Just as Mahan found that few of Jomini's principles of war on land were applicable to sea, we should not expect a direct translation of existing concepts and doctrines into the cyber world. There are no heartlands here, as per Mackinder, nor rimlands, as per Spykman, at least that translate easily in the physical sense. Clausewitz's centres of gravity are diffused and changeable, though cyber is no less a political issue than any other use of force. Vauban's fortresses won't help here; counter-insurgency may offer some insights into the dynamic interplay of populations and politics. In no other—forgive the term—domain do both protagonists and bystanders constantly change the shape of the contested environment as they work, play, build, steal and corrupt.

Finally, time in Europe and more recently in Asia, has left me with some reflections specifically on Australia. Australia has the opportunity to recreate itself and its positioning in this new digital world. It has an educated and multicultural population, offering the benefits accruing to diversity, it can build on the density of its urban centres while also taking advantage of its vast distances and resources, and it has a reasonably stable political system that advocates meritocracy, transparency, accountability, the role of the individual and the rule of law.

All this means that we cannot easily reduce the challenges presented by cyber, or digital disruption, to a mere technology issue – as much as governments, perhaps understandably, would like to do so. We need to foreswear hastiness, and to move with greater deliberation: there's much to be gained from a more patient and careful response, not least a deeper understanding of the issues and greater scope to bring people on board. We need to embrace and encourage the diversity we have in our community—we know that cognitive diversity in groups yields better decisions. And we should avoid the temptation of continuously yielding to a single controlling voice. Such voices prevail by firepower. And under fire, a unit will scatter, then regroup, adaptively—just as in nature.

Nor is cyber simply about security. Cyber is about adaptiveness, and resilience. Doing cyber well means strategy, not simply security. Strategy emphasises the proactive; security the reactive. Cyber is fundamentally about the world we want to live in, the societies we want our children to grow up in, the nature of economic growth, and the nature of fundamental human rights and the values we hold dear. And that means contemplating deeply what those values are, and reflecting them through the people we educate, the institutions we shape, and the elections we run to ensure that they are, in turn, reflected by those we elect as our representatives.

Endnote

[1] https://bostonreview.net/forum-henry-farrell-bruce-schneier-democracys-dilemma

Copyright

Editor

Katja Theodorakis

Publisher

Konrad Adenauer Stiftung (Australia) Limited
Regional Programme Australia and the Pacific

11/3 Sydney Avenue
Barton, ACT 2600
Australia

Tel: +61 2 6154 9322

www.kas.de/australia

Disclaimer

All rights reserved. No part of this publication may be reprinted or reproduced or utilised in any form or by any electronic, mechanical or other means, now known or hereafter invented, including photocopyng or recording, or in any information storage or retrieval system, without permission from the publisher.

The opinions expressed in this publication rests exclusively with the authors and their interpretations do not necessarily reflect the views or the policy of the Konrad Adenauer Stiftung.

Design, Layout and Typeset

Swell Design Group

Paper

100% FSC www.fsc.org RECYCLED Paper made from recycled material FSC® C102086

ecoStar+ is an environmentally responsible paper. The fibre source is FSC Recycled certified. ecoStar+ is manufactured from 100% post consumer recycled paper in a process chlorine free environment under the ISO 14001 environmental management system.