Capabilities, competition and communication

Why the West needs a strategy for technology

Mike Rogers
About the author

Admiral Michael S Rogers retired from the US Navy in 2018 after nearly 37 years of naval service, rising to the rank of four-star admiral. He culminated his career with a four-year tour as Commander, US Cyber Command, and Director, National Security Agency. In those roles, he worked with the leadership of the US Government, the Department of Defense and the US intelligence community as well as their international counterparts in the conduct of cyber and intelligence activity across the globe. He is a Senior Fellow and Adjunct Professor with Northwestern University’s Kellogg School of Management’s Public Private Initiative and a member of the advisory board of Auburn University’s McCrory Institute for Cyber and Critical Infrastructure Security. Admiral Rogers is a member of the Australian American Leadership Dialogue’s US advisory board.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia’s defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre’s mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia–Pacific.

The work of ICPC would be impossible without the financial support of our partners and sponsors across government, industry and civil society.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
www.aspi.org.au/icpc/home
facebook.com/ASPI.org
@ASPI_ICPC
© The Australian Strategic Policy Institute Limited 2019

This publication is subject to copyright. Except as permitted under the Copyright Act 1968, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, educational institutions (including schools, independent colleges, universities and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published July 2019

Cover image: Illustration by Wes Mountain. ASPI ICPC and Wes Mountain allow this image to be republished under the Creative Commons License Attribution-Share Alike. Users of the image should use the following sentence for image attribution: ‘Illustration by Wes Mountain, commissioned by the Australian Strategic Policy Institute’s International Cyber Policy Centre.’
Capabilities, competition and communication

Why the West needs a strategy for technology

Mike Rogers
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>03</td>
</tr>
<tr>
<td>Seeing technology as a capability, not a product</td>
<td>03</td>
</tr>
<tr>
<td>Rethinking technological competition</td>
<td>04</td>
</tr>
<tr>
<td>Developing a strategy</td>
<td>05</td>
</tr>
<tr>
<td>Strengthening our alliances</td>
<td>06</td>
</tr>
<tr>
<td>Communicating with broader audiences about cyber strategy</td>
<td>07</td>
</tr>
</tbody>
</table>
Introduction

At the conclusion of his time as a Distinguished Visiting Fellow with ASPI’s International Cyber Policy Centre, Admiral Rogers shares five factors that government and policymakers should consider as they prepare for the next wave of disruptive technologies.

Seeing technology as a capability, not a product

Technology is going to be a core aspect of the future for us, and it’s not just cyber technology. It’s going to be technology writ large. I believe that we can assimilate this. Game-changing technologies with social implications have been a part of human history during our entire existence as a species. We tend to think that the time we’re living in is the most different or somehow the toughest, but it’s not. There have been game-changing technologies with potential negative second- and third-order effects throughout the history of humanity. We’ve dealt with this before. I believe we can deal with it now. But we’ve got to be willing to sit down and think about this. And we really need to ask ourselves what’s the way forward.

One of my concerns as I left government was, quite frankly, that I didn’t think we fully understood the implications of technology in national security. I thought that in many ways we were still organised and focused along very industrial lines, that we tended to think of ‘technology’ through the prism of something that’s produced. It might be a particular good. It might be a particular service. It might be a particular product. On the other hand, the idea of technology as an underpinning that powers a broader set of activities—I didn’t think we were working our way through this enough.

What’s the right answer for the implementation of a technology that will be a fundamental building block for a nation’s economic competitiveness in this digital world that we’re living in?

I would argue 5G is emblematic of this, because 5G is not just about, ‘Well, I’m going to get a better phone service,’ right? That’s not the heart of it. 5G is going to enable us to address latency issues. We’re going to be able to move massive, increased amounts of data at incredible, stable rates that will turn our handheld digital devices into the kinds of capabilities and functionality that we take for granted today in our laptops and our mainframes.

5G is going to underpin all of that, and it’s only one of many foundational technologies that are being developed right now. As I used to say about 5G in our system, ‘Hey, it’s just the wolf closest to the sled.’ It’s emblematic of a broader set of challenges that we’re going to have to deal with over time.
Rethinking technological competition

In the US, our theory had always been that the edge for us is the innovative power of our private sector. And as long as the government largely stayed out of that, we could compete head to head, and compete very well.

I would argue that for 1G, 2G, 3G, 4G, that worked perfectly. But the dynamics we’re seeing now with 5G are prompting the question of how that strategy works when the competition isn’t a single foreign company. The competition now is an integrated national strategy in which that foreign company is just one component. How does a single private company compete against the integrated efforts and resources of an entire nation-state?

I think we have to be asking ourselves how we need to change our model, because if we think it’s bad now with 5G, I would argue it’ll be even worse when 6G comes along in about three years. It’ll be even worse with artificial intelligence, quantum computing and other new technologies coming down the pipeline right now. We’re going to have a series of technological changes coming up. They’re going to be so foundational that if we don’t change the dynamic, we’re going to have this conversation over and over again.

This is not about stopping any particular nation. This is not about contesting a particular company. This is about ensuring our own and our partners’ competitive ability in the 21st-century digital age. Because, again, you’re going to have to deal with this with other countries and other companies over time. Right now, that happens to be China, Huawei and 5G, but it’ll be something different in the future.

To me, China is not an enemy. They aren’t an adversary. They’re a competitor, and we need to ask ourselves, ‘How do we compete with them?’

Let’s not waste our time trying to figure out how we stop the growth of China, how we contain China. My view is that is a losing strategy. I think a much smarter strategy is that, given that growth, given that rise, how can we work together collaboratively to ensure that the growth is done in a way in which it becomes a part of the greater, broader world order? And that it’s done in a way that optimises outcomes both for China and for its neighbours, including the US.

We shouldn’t approach this as a zero-sum game; I never believe that. I think that for Australia and the US our respective relationships with China are going to be fundamental to our competitiveness and our economic performance in this century. You can’t pretend otherwise.

I think the goal is to make sure that the playing field is level. Once we have a level playing field, then it’s up to our private sector. But the challenge right now is that the playing field is not level, and it’s really difficult for the West’s firms to compete. And I just don’t think it’s realistic to expect them to do this on their own. Levelling the playing field is going to take work. It’s also about ensuring agreements are adhered to and there are consequences for clear breaches.
Developing a strategy

In the end, to me it’s all about developing a strategy. I’m watching other nations develop strategies, and I’m saying to myself, ‘Where’s ours? How did we get ourselves into this situation? And what are we going to do so that we can compete?’

So, let’s think about the strategy we’re going to develop. Let’s think about how we’re going to compete. Let’s think about how we’re going to ensure our continued strong economic performance, our strong technological edge. How are we going to retain that? And at the same time as we’re retaining that, how are we going to retain the values of the societies that we’re a part of?

Our number one competitive advantage, I argue, is our values: the idea of freedom, the idea of the choice of the individual, the idea of the private sector’s ability to compete without the constraint of the government. I also argue that the power of innovation is one of our competitive edges, and we should be doing more to support and protect that innovative edge. So I think, again, if we can get to a level playing field, then our inherent advantages—that structure, those values, that ability to innovate—will enable us to compete with anybody.

I think we have to acknowledge that our structures and our processes aren’t really optimised for this world. I also think we have to acknowledge that it all starts from recognition and acknowledgment of the problems, so we’ve got to be willing to do that. You can’t fix anything if you don’t acknowledge that you have an issue.

I think there’s an element of changing structures and changing process in the way we do things. Part of that model which needs to change, at least in the US, is the kind of wall we build between the functions of the government and the private sector. We really need to step back and ask ourselves—given this world of technological change, given technology’s impact on national security and economic competitiveness, given the speed with which this is happening, given the geopolitical applications of some of this technology—some really fundamental questions like, ‘So, what’s the role of the private sector in this world? What’s the role of the government in this world? Are there ways they could team together?’

It doesn’t mean control. A lot of times I hear people say, ‘You’re just arguing that the government should control everything.’ That isn’t what I’m saying. That hasn’t tended to work out so well in many areas, and it’s not a model that I would default to. On the other end, I think there are some things we can do in partnership with each other. I just think we have to be open to the fundamental idea that in this digital age we’ve got to be willing to look at very different approaches to how we do things.
Strengthening our alliances

I think if we’re honest with ourselves, we have tended to take the US–Australia relationship for granted for some time, and that just isn’t going to work for us anymore. We’ve been together in every major conflict in the past century. In the post-9/11 environment, we’ve worked and fought together. Everywhere I’ve been, on the battlefields in Afghanistan and Iraq, in my professional career, I’ve loved hearing the sound of an Australian accent in the middle of nowhere. In some really tough circumstances, hearing that cheery, ‘G’day, mate,’—I just really like that. I think there’s something really powerful about that. But we can’t take this relationship for granted.

The ability to bring like-minded nations together to work on tough problems is a great thing. Five like-minded nations with a broadly common set of values and a willingness to address not only their own national interests but to support others in the execution of theirs, all with the view of ensuring that we’re helping to make the world a better place: that’s a pretty powerful fundamental idea.

I think that’s still very relevant. It doesn’t pretend for one minute that we don’t have national interests and that those interests never differ. It doesn’t pretend that we don’t have respective national interests that we want to make sure are addressed. But I still think that within that framework we can do powerful things together.

One of my concerns is that, if we don’t get this right, if we don’t think about national security, economic competitiveness and the implications of technology, then we’re individually going to make decisions that potentially increase the risk for other partners in the Five Eyes, or which potentially force other members of the Five Eyes to make some really tough choices that might not be in the interest of all five. If we’re not careful, we could start to go down the road where Five Eyes starts to splinter. If that happens, it should be a conscious decision, not something that kind of happens as an afterthought of other choices. We have to work at maintaining those alliances, and we have to be able to articulate their value. The Five Eyes structure is so important, and one of its strengths has been that we’re willing to have a discussion with each other on those kinds of issues.
Communicating with broader audiences about cyber strategy

As policymakers and as leaders, we’ve got to think about how to articulate the challenge of technology in a way that non-technical people can understand and relate to. I don’t think we’re particularly effective at this at times. One point I would make is, ‘Hey, look, we got to articulate these important topics in ways that non-technical people can understand.’

The second point I would make is this. We need to try to provide meaningful, concrete, specific examples, not an apocalyptic, cyber-could-destroy-the-world-around-us story, because what happens with that is you cry wolf too many times and people just tune you out. Instead, we should be trying to break these big, complex problems down into smaller, more understandable, more digestible components that enable us to build a comprehensive strategy.

Speaking only for the US, we have publicly started talking about how cyber is a tool within the toolkit which we will consider using in an appropriate manner, with a legal basis, for various measurable and proportionate responses to other activity.

For example, you saw us acknowledge in congressional testimony that for the November 2018 election cycle in the US, the US Government authorised and executed a strategy designed to preclude the Russians’ ability to do some of the things against US election infrastructure which they did in 2016. That’s significant: firstly, the fact that we did it; secondly, the fact that we’re willing to publicly talk about it.

What this indicates to me is a kind of evolution in strategy and policy which says, ‘Look, we need to acknowledge that being passive and responding quietly has not really gotten us to where we want to be or where we feel we need to be. Therefore, we need to try to do something different.’

The difference is that we need to start publicly talking about cyber as a tool: the fact that we have capabilities, the fact that we’re willing to use them, and then showing our willingness to use them—again, for very specific purposes, under a very specific legal regime and with a very specific sense of proportionality.
Some previous ICPC publications

- Technological entanglement
  - Cooperation, competition and the dual-use dilemma in artificial intelligence
  - Elkeinde

- Hacking for ca$h
  - Is China still stealing Western IP?
  - Dr. Adem Aksu, Dr. Samantha Poh, Eugene Haines, and Tianshun

- Preventing another Australia Card fail
  - Unlocking the potential of digital identity
  - Ferguson/Hansen

- Picking flowers, making honey
  - The Chinese military’s collaboration with foreign universities
  - Alex Zubi

- Introducing integrated e-government in Australia
  - Anu-Oria, Ferguson Hansen, and Alyssa Trupin

- Identity of a nation
  - Protecting the digital evidence of who we are
  - Arno Lysen

- Australia’s cybersecurity future(s)
  - It’s January 2034. Does Australia still have the Internet?
  - Footnote: AM Cybercast, Right to Left, Centre Link, Australian Strategic Policy Institute

- Taking Australian diplomacy digital
  - Davide Shimko

- Mapping China’s technology giants
  - Andrew Gourley, Constance Hui, and Ryan Maclean