

Australian cyber Light Horse must prepare for a new charge2

FINANCIAL REVIEW

Opinion

Australian cyber Light Horse must prepare for a new charge

Rory **Medcalf** and Elanor Huntington Professor Rory **Medcalf** is head of the National Security College and Professor Elanor Huntington is dean of the College of Engineering and Computer Science at the Australian National University.

920 words

31 October 2017

The Australian Financial Review

AFNR

First

51

English

Copyright 2017. Fairfax Media Management Pty Limited.

Anniversary

Australia's past success at Beersheba - now Israel's Silicon Valley - has valuable lessons to teach us about cyber security.

The charge of the Australian Light Horse at the Battle of Beersheba precisely 100 years ago offers surprising lessons for the nation's security today.

In the desert sands of Israel, Australia's mounted military past is in step with our nation's cyber security future.

For Australians, Beersheba is where a young nation won a key battle of the First World War. Eight hundred men of the Light Horse made the last successful cavalry charge in history.

They captured the strategically important town and its wells - vital infrastructure in a desert campaign. The bold action was a turning point in the defeat of Germany's Turkish allies.

For Israelis, the place is something else entirely. The city of Be'er Sheva has risen from the sands to be Israel's Silicon Valley, where tech start-ups work with universities and government to make this small nation a global cyber technology leader.

This week, a new cavalcade of Australians has descended on Be'er Sheva to honour the memory of the Light Horsemen but also learn from Israel's innovation story.

One side effect of the domestic political crisis over dual nationality is that Prime Minister Malcolm Turnbull is abbreviating his visit to Israel, where he has sought to build strategic links in cyber. But the march goes on.

Today's commemoration of the 1917 charge will punctuate a week of cyber security consultations convened by the Australian National University with Israeli counterparts. These talks involve the Minister assisting the Prime Minister for Cyber Security, Dan Tehan, as well as officials, academics and entrepreneurs.

The Australians are here to learn from Israel's extraordinary success in combining its national security experience with cyber expertise, enterprise and international networks. But we could also learn from our own history.

Beersheba has been easy to mythologise, marked by the speed, victory and decisiveness so missing from so much of the horrific First World War.

The charge called for courage and inventiveness. Australia's mounted infantry surprised their Turkish and German opponents by fighting as cavalry - making a sudden headlong charge using bayonets as swords, too unexpectedly for the defenders to bring firepower to bear.

The counter-intuitive use of this tactic underlines the resourcefulness, agility and risk-taking we will need as a nation to handle the treacherous terrain of cyberspace. The government last year made a significant start, with a cyber security strategy focused on joining up the efforts of industry, academia, society and security agencies. This

means co-ordinating finite resources to protect the nation from the full spectrum of cyber risks. These include the criminal denizens of the so-called dark web as well as terrorists and their propagandists - but also states.

The solution is not just to dig cyber trenches but to equip Australian business to go forth, to innovate and compete in a fast-evolving global landscape.

Yet government alone cannot secure the nation's cyber future. Now industry and universities are starting to step up.

For its part, the Australian National University has just announced a cyber institute that will combine expertise across technical and social science disciplines - because cyber is ultimately about people - to foster the talent, research and innovation the nation will need.

This will expand the nation's cyber security workforce to take in more of the creative and the curious, beyond the regular ranks of IT specialists.

This skills element is crucial. Australians face a bewildering array of cyber security threats, from IP theft, compromise of financial data and ransomware through to espionage, misinformation, the sabotage of critical infrastructure and the criminal misuse of devices connected to the fast-arriving Internet of Things.

At present, our security agencies and businesses have far from all the personnel and skills they need to hold the line of national cyber resilience, or seize all the opportunities for prosperity.

Again, history is illuminating. Part of the myth of the men who charged at Beersheba is that, though they had volunteered to be soldiers, they were at heart individualists and civilians from many walks of life.

This may be so. Their horses were of motley breeds. Their untidy battledress, topped by an emu plume, was more personalised than uniform, a bushman's precursor to the cyber geek's T-shirt.

But what is often forgotten is they had honed their skills for years. Their effectiveness was a result of a national system of compulsory military training that began in 1911.

The Light Horse were no amateurs but an elite citizen force born of preparedness in peacetime. Their numbers were reinforced by Australia's ability to attract and refine talent from many places.

If written today, their job description would include creative problem-solving involving deep expertise, divergent thinking, confidence and motivation - very much the qualities the nation needs in its cyber talent pool.

In the new and constant battleground of cyber, Australia would do well to study its own past as well as Israel's present, and start skilling more people to protect its interests.

It's time to imagine a new Light Horse for security and prosperity in the information age.

Document AFNR000020171030edav0004w