Ukraine war a wake-up call for Australia's digital chasm

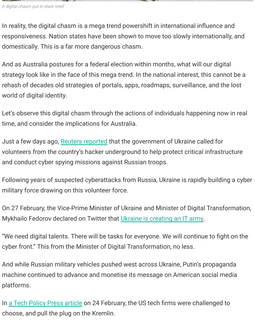
Marie Johnson
Contributor
18 February 2022

In the third decade of the 21st century, the digital chasm has been crossed. But not as anticipated or predicted.

The Ukraine crisis is a demonstration of the power of the individual in democracy, and the circumstances of the individual. But this time, 'digital' has become a flashpoint of individual action, individual expertise, and individual power. Who is this individual?

For decades, organisations such as the UN, and the International Monetary Fund have become increasingly concerned about the deepening digital divide within nations, and between developed and developing nations. The digital divide within society has been called the digital chasm.

But this is not the digital chasm that has erupted in Ukraine.



A digital chasm put in stark relief

In reality, the digital chasm is a mega trend powershift in international influence and responsiveness. Nation states have been shown to move too slowly internationally, and domestically. This is a far more dangerous chasm.

And as Australia postures for a federal election within months, what will our digital strategy look like in the face of this mega trend. In the national interest, this cannot be a rehash of decades old strategies of portals, apps, roadmaps, surveillance, and the lost world of digital identity.

Let's observe this digital chasm through the actions of individuals happening now in real time, and consider the implications for Australia.

Just a few days ago, Reuters reported that the government of Ukraine called for volunteers from the country's hacker underground to help protect critical infrastructure and conduct cyber spying missions against Russian troops.

Following years of suspected cyberattacks from Russia, Ukraine is rapidly building a cyber military force drawing on this volunteer force.

On 27 February, the Vice-Prime Minister of Ukraine and Minister of Digital Transformation, Mykhailo Fedorov declared on Twitter that Ukraine is creating an IT army.

"We need digital talents. There will be tasks for everyone. We will continue to fight on the cyber front." This from the Minister of Digital Transformation, no less.

And while Russian military vehicles pushed west across Ukraine, Putin's propaganda machine continued to advance and monetise its message on American social media platforms.

In a Tech Policy Press article on 24 February, the US tech firms were challenged to choose, and pull the plug on the Kremlin.

"The apps they operate are not fun and games. Their platforms are not an abstract realm of ideas and debate. They are vehicles for the exercise of power."

Also on 27 February, the Vice-Prime Minister of Ukraine and Minister of Digital Transformation, Mykhailo Fedorov wrote directly to Mark Zuckerberg appealing for Zuckerberg to block access to Facebook and Instagram from Russia.

Letters were also written to CEOs of Apple and PayPal, with all letters published on Twitter.

What is extraordinary about this is that one individual – Zuckerberg – has amassed so much power, accountable to no one, with world leaders appealing to his humanity during a time of war.

Does a country or entity have to face an existential threat before realising that digital transformation has in fact happened, and the levers are different.

Effectively, the Ukraine Minister of Digital Transformation was asking the CEO of a company not based in his country, to ban the citizens of a third country.

Fedorov also appealed directly to Elon Musk, another individual who has amassed power and capability:

"...while you try to colonize Mars – Russia try to occupy Ukraine! While your rockets successfully land from space – Russian rockets attack Ukrainian civil people! We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand."

Just one day later – not weeks, months, or years – Musk responded that the Starlink service was active in Ukraine, with more terminals en route.

Also on 27 February, Fedorov reported on Twitter that YouTube had disabled the monetisation of Russia Today channels.

It turns out that powerful individuals like Zuckerberg and Musk can act faster than NATO, UN, and 'global' powers. But so can a collective of skilled individuals.

The hacker collective, Anonymous – a decentralised collective of individuals without hierarchy or leadership – announced they had launched cyber operations that took down RT.com, the propaganda outlet for the Russian government, other Russian websites including the Russian Ministry of Foreign Affairs, and banks in Belarus and Russia.

This is cyber activism. A war like no other being fought with 1's and 0's. And the arsenal is not just – or rather, no longer – within the control of governments.

Similarly, volunteer editors on Wikipedia have been documenting the Russian invasion of Ukraine as it unfolds. The Wikipedia article on the invasion has been edited 2100+ times by 500+ editors, with 340+ references, in 77 languages. It's received 2 million pageviews, making it currently the most popular article on the site.

As the conflict between Russia and Ukraine unfolds, much of the world continues to watch via social media. Australia's government funded ABC, cannot keep up this pace and is often 12-24 hours behind what's happening on social media – often not reporting at all.

Like the DTA, the ABC strategy appears lost in the old world of portals, forcing viewers to create an account and hand over personal data in exchange for access. Many people like me will just stop watching ABC altogether, knowing the cyber security landscape.

And unlike the ABC, the Twitter account 'IT Army of Ukraine' and Wikipedia provide a constant update on what is happening, including the cyber activism.

Thankfully, Australia does have an active cyber, academic and privacy community that has worked together to expose cyber flaws and risks to civil liberties in a vast range of Australian government digital policies, strategies, and services.

Most recently, RoboDebt, RoboNDIS, the COVIDSafe app, the digital identity and even the ABC iView.

But in a bureaucracy bereft of cyber skills, there is an increasingly antagonistic relationship with this outstanding Australian ecosystem of cyber activists and cyber professionals. And yet, the bureaucracy maintains a captive dependency on consultants.

Why is it that Commonwealth and state audits continue to show a swiss cheese of cyber vulnerabilities: Australian and state government agencies; ANU; Service NSW; heath organisations; the Australian Parliament; and of course, the COVIDSafe data "incidentally" collected by intelligence agencies.

In many instances, vulnerabilities and massive actual breaches that are either not fixed, or the remediation so slow as to be ineffectual. One has to wonder if this level of vulnerability would be tolerated by Elon Musk.

The swiftness of the Ukrainian cyber activism 'for good' serves to highlight the power asymmetry of the digital chasm and the vulnerability of institutionalised slowness.

And in the era of decision-based algorithms and AI, these risks are even more extreme. Why is it that funding for Australia's AI Action Plan remains locked up in the Industry department nearly a year after it was announced? Announceables do not build capability.

In the midst of this fog of war and as we start to emerge from the pandemic, Australian governments and businesses have been warned that they face their greatest hacking threat yet, with the Australian Cyber Security Centre warning of possible widespread systems failure.

This includes advisory warnings to boards and directors. With a worst-case scenario being the collapse of the Centrelink payment system.

The good people at Services Australia, are challenged on many fronts. I was the Department of Human Services portfolio Chief Technology Architect responsible for Access Card and the architecture and technology business cases bringing together Centrelink, Medicare, and Child Support – so I appreciate better than many the complexity of these mega systems.

But the Services Australia response to the Privacy Act review is troubling, highlighting its "significant concern" over the lead time, cost, and wholesale changes to critical whole-of-government IT systems that would be needed to accommodate proposed privacy reforms.

Effectively, what the Services Australia submission appears to be saying, is that the 7-year multi-billion-dollar transformation program has taken it from one rigid system incapable of change, to another.

The Ukraine crisis has revealed the flashpoint of the digital chasm. Transformation is often driven by catastrophic failure and existential threat rather than long term transitional planning.

And the challenge for Australia is not how we responds to the Ukraine crisis – which we must – but how we protect ourselves and advance our well-being in the digital decades ahead.

We are not far away – but seconds away.

The chasm has been crossed. There is no going back.

Do you know more? Contact James Riley via Email.

Related: COVIDSafe app | Cybersecurity | digital | Marie Johnson | RoboDebt | robotNDIS | Ukraine | Ukraine war

← Previous post
Forrest buys $3b renewables farm, FFI hydrogen hub gets underway

Next post →
SA lands first major federal manufacturing grant in lead up to state election

Your email address will not be published.

Name* Email* Website

Save my name, email, and website in this browser for the next time I comment.

Comment*

POST COMMENT

Related stories

Big Tech media bargaining code passes
14 February 2021 | by Denham Sadler

Games industry weathers COVID-19 ahead of tax relief
14 June 2021 | by Joseph Brookes

Liberal Senators' Big Tech inquiry gets knocked back
18 March 2021 | by Denham Sadler

Deloitte lands another big federal platform fix
17 December 2020 | by Denham Sadler