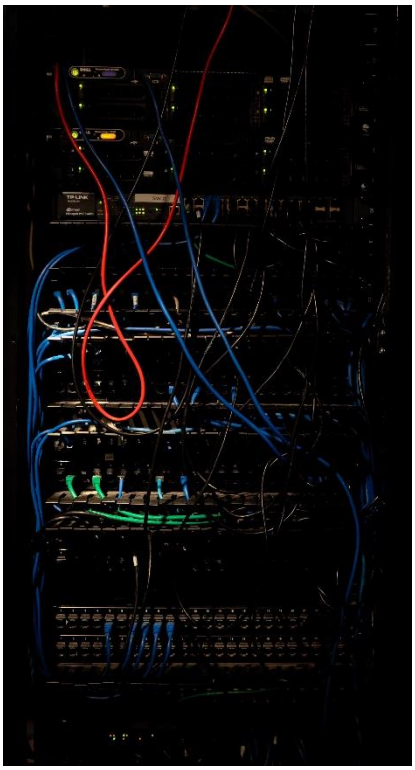
Digital Platform Services Inquiry – September 2021 Report on market dynamics and consumer choice screens in search services and web browsers

Issues Paper| Submission in response to the interim report | A Provocation |

Computational Data Markets



Tom Sear, UNSW Canberra Cyber at the Australian Defence Force Academy

Anzac Day, 2021.

Master Sun said:

In War,

Better take

A state

Intact

Than destroy it.

Ultimate excellence lies.

Not in winning

Every battle

But in defeating the enemy

Without ever fighting.

The highest form of warfare

Is to attack

Strategy itself;

Sun-Tzu, *The Art of War*, Penguin, London, 2002. p. 12.

Welcome to your life
There's no turning back
Even while we sleep
We will find you
Acting on your best behaviour
Turn your back on mother nature
Everybody wants to rule the world

It's my own design
It's my own remorse
Help me to decide
Help me make the
Most of freedom and of pleasure
Nothing ever lasts forever
Everybody wants to rule the world

Tears for Fears, song, *'Everybody Wants to Rule the World'.*

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it.

Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf p.3.

Instead of the chain of determining representation flowing from a legal declaration, which is then reflected in the form of a technical apparatus, perhaps the sovereign that emerges from the emergency and is created by the emergency will look more like a technical apparatus, one which is subsequently indexed in legal symbolization as another new normal takes shape.

Benjamin H. Bratton. *The Terraforming*, Strelka, 2021. p.33

Strategic Overview

We are alive in an era of planetary emergency. Digital advertising distorts the capture of data we must collect - and apply - to computation if we are to survive as species [See APPENDIX A].

In response to the Interim Report of the *Digital Advertising Services Inquiry*, Google states:

'Any regulatory intervention must not reduce the innovation and competition that has driven so many benefits.'

I agree with Google.

I suggest the ACCC go further. The ACCC should lead Australian whole of Government measures to *accelerate* innovation. Even use Ad Tech to amplify and deliver an innovation outcome.

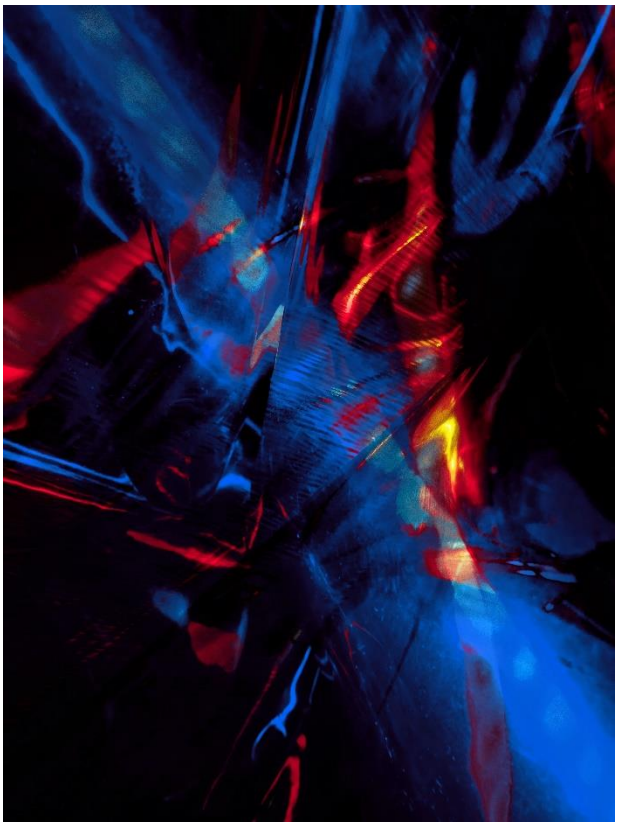
The Australian Government should regulate data to replace current arrangements with a wholesale data market-based model.

Data streams are abstractions of flow like telecommunications and energy utilities. Data streams can be priced like commodities. Like utility markets, the ACCC should split the backend and frontend of the data market into two parts: wholesale and retail. Indexing data then effectively becomes a pricing/bidding system for those markets. That way, there is not just a transaction in between but that data system can be easily taxed by Government. Currently Government cannot effectively tax these flows and Big Tech can take profit offshore.

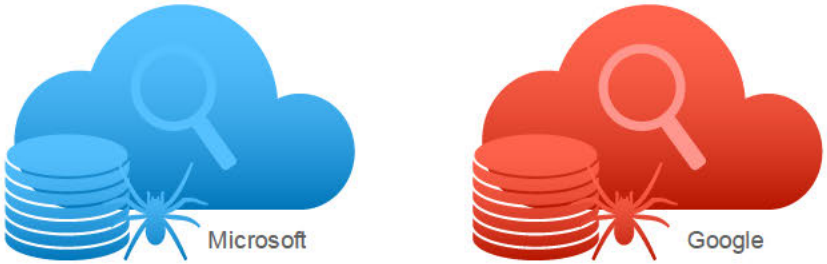
The consumer will also benefit from a wholesale data market, in a perhaps unexpected way. Big Tech *wants* the ACCC to focus on personal privacy solely - because what it really fears is regulation of commercial data. Big Tech can more easily pivot than smaller or new entry competitors to regulation. Big Tech can easily make a system 'safe' in response to ACCC regs, thereby maintaining, even amplifying separation and monopoly.

The interface war has been raging longer than the Afghanistan conflict. The interface war is made up of battles for the customer attention to collect human data which has already been curated for free by homo sapiens, training the Algos and AI. There is another way: Ad Tech Systems could combine forces like a Marvel franchise, working together to use their selling superpowers to be a force for good rather than evil. Pricing personal information collected when an upper hominid puts in a search query effectively acts as a cash equivalent. Right now, humans are a kind of retailer for Big Tech Machines. There is a transaction at the browser level that the ACCC simply cannot regulate now. So, do not – instead: break all the rules.

The ACCC can lead Australia into a Brave New World of disruption, not control. The ACCC should explore the separation of monopoly from contestable competitive areas. A wholesale market for data could operate under a Participation Code overseen by a market regulator, to be named the Australian Data Authority. Data trade could then take place at State Capital nodes across Australia. That would enable a Jane or Joe Blow to set up their own interface to retail data and content. Then competition would exist – genuine data flow competition enabled for proverbial Jane and Joe Blows.



Current State

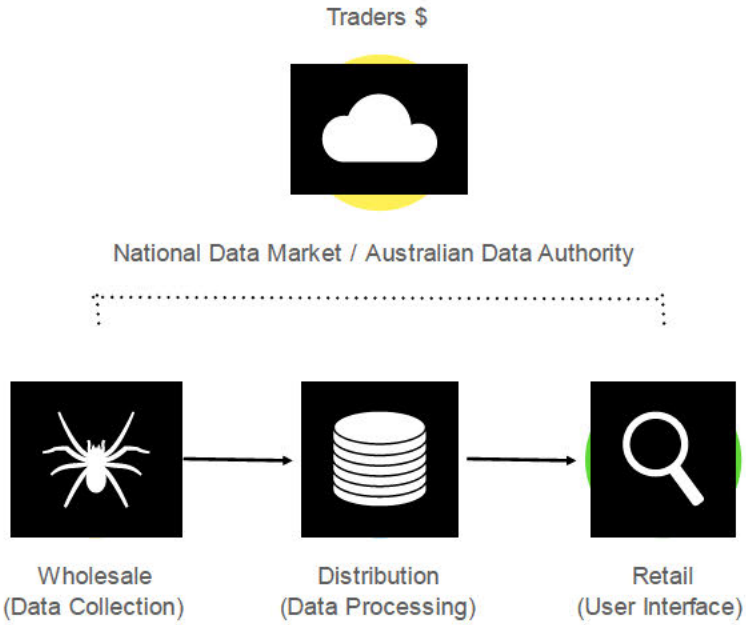


Currently users choose between a small number of vertically integrated search service providers who provide web crawling, indexing, and front-end user experience as part of a single ad-funded service.

Consumers have very little choice not just between providers, but between the quality of services they receive from each competitor.

For instance, there is no such thing as a 'business' or 'enterprise' account as we see in energy and broadband markets

Future State



Unbundling the “wholesale”, “distribution”, and “retail” aspects of the data market in a way that mirrors the National Electricity Market would enable more intense competition between infrastructure and data service providers while opening up innovation on the retail side and making costs more transparent to end users. Startups could create interfaces tailored for different languages, disabilities, industries, etc.

By treating different aspects of cloud data services into a mix of wholesale and retail, transactions between the two could be taxed, audited or subsidised as necessary.

Necro Nepho - Crypto Eco | The Emergent Era of Competitive Computational Data Markets

Competitive computational data markets are a distributed alternative to Cloud forms. The Cloud characterises markets as multi-level or vertical. Digital information instead requires a price ecosystem which encodes context and value into canonical data identifiers to displace the ad-based ranking recommender systems of Facebook and Google. Attention integrated with proof of work creates a genuine capital light data supply chain without the need to collect personally identifiable information. Instead of pooling data in sky reservoirs, computational data markets deploy cryptography whereby start-ups, content creators and developers and citizens can compete equally in real time cost effectively.

The current problem is one of scale not monopoly. Big Tech is based on a business model of capture to keep customers on a platform. In contrast, 'proof of work' models enables markets to rank and categorise information via cryptographic content IDs in context. Such models can be practically rolled out now – with the very same tools Big Tech search engines and social networks use locating info – except proof of work models would work on metadata rather than raw content.

Big Tech Algos (BTAs) distort the marketplace. BTA based platforms each have proprietary way to measure value – the context of which is selling ads. Such pricing is inefficient. All the BTA does is create a floor price. This sucks for content creators as they have no price ceiling. Rather than control the square peg in the round hole of tech via monopoly, the ACCC and Government should regulate for a standardised way to differentiate content. The ACCC could adopt a Schumpeterian instead of Ricardian rent competition policy for data markets [See APPENDIX A for how this submission syncs with the Ad Tech Inquiry]. That would have the structural effect of ensuring that not only would users own more of their data they could own their relationships as well.

The flow on effect of such a universalised price system for data is not only that it is more capitalist in the Adam Smith sense of political economy as exchange, but also support the way, democracy creates laws which ensures as much equality as possible between citizens. Automated negotiation systems proposed here signal value in an open market undermining the bias BTAs create in a marketplace. Such a system would be immutable, inherently monetizable and enhance niche data not the utilitarian cookie cutter lowest common denominator necessity of BTAs.

Local first web interfaces to search the index can replace legacy engines while also sharing peer to peer via traditional web servers. Local web clients, browsers C++ articulated APIs could facilitate the license that the ACCC would regulate. Data on the IP supply chain could then handle via 'Platform as a Service' the transition out of the legacy BTA model the ACCC is struggling with.

The Australian economy has long relied on primary industry sectors such as mining. There is no need to give those up. Australia would instead create world leading regulatory model to mine the new resource: Data. Instead of mining engineering deploying technologies of material drilling, hauling, and crushing; that industry could pivot their model to future exploration of data resources. The mining sector could pivot to Turing tunnels and crypto mining in distributed hash shafts digging for the ores of valid checksums in global address cyberspaces. The Australian economy has often been categorised as overly reliant on primary industries such as mining, and agriculture. Aussie high tech Ag systems can also be applied. As the twenty first century planetary economy shifts into renewable energy, human biotech and information, the initiative suggested in this submission pivots the Australian resource base into a human capital centred multi-species economy - from the proverbial metaphor of 'Riding on the Sheep's Back' to the new tertiary axiom of 'Riding on the Leet's Back'.

Sovereign Data Infrastructure |

The ACCC and the Australian Government can simultaneously address systemic data market issues and build supply chain security within critical infrastructure protection and the IoT sensor future. Ideas in this submission enable an anti-fragile strategic society. Control of our own national data would facilitate the current dependencies of our status as an information colony of larger states and economies of our trading or military partners.

In the planetary size accidental megastructure that is the internet Australian data – in all its forms and flows – is a form of critical infrastructure that the Australian Government is responsible to ensure is secure. This ACCC submission syncs with those I have outlined to Home Affairs and Defence as requirements to respond to the challenges of the twenty first century. Interdependence of supply chain, borders, biosecurity, and data are now indivisible from secure sovereignty. [See APPENDIX B for a submission to Home Affairs which links with and informs this submission to the ACCC]. Government is responsible for secure supply chains for itself, Defence and the Intelligence community, trade of dual use military technology, electricity, ports, airports and water infrastructure, systemically important financial institutions and market infrastructure, media entities which impact plurality - and increasingly - social media as the fulcrum of democratic speech. Data infrastructure is now not only integral to the function of all the above, but necessary for sovereignty and protection of citizens. Competitive Computational Data Markets regulated by an Australian Data Authority would integrate these efforts.

While the proposal suggested here does not require data centres to operate, it is possible that Australian Government could cheaply and easily operate the data market on secure data centres that form part of Australian critical infrastructure protection. Open academic, ASD interrogated and verified crypto protocols could ensure citizen privacy and safety.

It is even feasible now. The federal government will invest $64.4 million to establish a centre in Perth to process and analyse data from the Square Kilometre Array (SKA) radio telescope. An international network of SKA Regional Centres will support the global flow of data and processing needed for the telescope. The data flow and processing volumes would make Shannon's eyes water. Approximately 7 terabits of data will travel from Australia's SKA antennas to supercomputers in Perth every second. Your weird techy uncle might be proud of his data speed, but the SKA rate will 100,000 times faster than average Australian broadband - processing 600 petabytes annually. Storage will be 10,000 times more data year on year than the *entire* capacity of Netflix.

That means that should Australians continue to use Google, Facebook and Tencent as providers no interruptions will take place.

It is even feasible that just like we will increasingly exist in regional trading markets like the AUS/NZ COVID bubble, we could AnzaCyber Data Spheres of automated regulation – expanding our interaction and tradition as Anzac Cyber Sovereignty. This could even be an Strategic Society Anzac AI Defence System as what is proposed grows a market for AI recommender systems since its not just data on a sociometric, limited network but its every packet everywhere in the infrastructure.

APPENDIX A

Ad Tech Inquiry| Submission in response to the interim report

Tom Sear, UNSW Canberra Cyber at the Australian Defence Force Academy

Strategic Overview

2020 marked a hard reboot for sapience on planet Earth. The period from late 2019 and throughout 2020 simultaneously saw a maturation of the 1989 global factory reset and a transition into a new century. The impact of climate change and pandemic focussed humanity's attention upon the marketplace of global supply chains. These challenges exist at a planetary scale. The scale of these challenges is important. The period also marked the maturation of another form of planetary social infrastructure: the internet. Planetary-scale computation has ensured a cybernetic human society but has also restructured nation state sovereignties borders and economies.

Advertising supports the social infrastructure of the internet. This has a flow on effect. The internet has shifted how humanity governs itself. The political economic intersection of these factors is what makes the Digital Platform Services Inquiry important, and specifically what makes the Digital Advertising Services Inquiry important.

The internet has carved up planetary political economies into Stacks. For the Australian continent, two stacks predominate: the Anglospherical Stack GAFA and the Chinese based BAT [PRC/CCP] Stack of Baidu, Alibaba, Tencent. Both these Stacks intercede in Australia. While GAFA predominates, BAT is also important. For Australian governance, this has significance for the polity. Citizens now participate in a global economy directly, and the defence of the state depends upon secure value and supply chains.

A new informational political economy is immanent of the internet. Planetary computation geopolitics is an armature of data. Ad Tech spirals within this armature. It is not capitalism or communism anymore in dipoles: it is vectoralism. US-based Big Tech platforms don't function like old firms by owning capital, just as the CCP does not redistribute like the era of Mao or Deng. Instead, they both control the vectors which move materialism around with information. Data is now vital to both economic activity and political organisation.

This is a long way to say: the ACCC has a special problem – competition has changed, but the tools at the disposal of government are products of earlier forms of production and governance. The old rules of competition and anti-trust will not work to control broad spectrum competition in an era of Big Tech.

Time is now the key resource. The last decade has shown that we exist in a governance via the curve and the temporal: paranoia and power laws predominate, while the polity is recursive. This means the ACCC must operate on two-time scales – the immediate present and the long term – and has to provide policy options for both.

More accurately, conventional competition policy has focused on static competition, but dynamic competition policy will create much larger long-term gains in the digital economy. Just as previous anti-trust and competition policy is tuned for the industrial economy where markets and innovation are contained and relatively static, it is for an era of restaurants and cafes, not ghost kitchens and mopeds.

Tactical Note: Digital advertising services inquiry: Interim report

While not technically incorrect, the ACCC approach methodologically puts the cart before the horse. The ACCC Chicago style static micro theory-based competition policy excludes innovation. The ACCC is entirely correct, in that competition drives innovation, but innovation also drives competition, and focusing upon one side of the equation may misunderstand the way Big Tech works. Much of current anti-trust policy is tuned for the old industrial era. The ACCC responses are broadly resource driven, not innovation driven. Monopoly power, predatory mergers and models of market power are no longer sufficient to understand competition in the digital economy of Big Tech. The ACCC's measures may seem to consumers and firms to be of benefit – while some of these are real effects – they are short term only and will distort dynamic competition and reduce consumer welfare in the long term.

- ACCC Proposal 1 – Measures to improve data portability and interoperability.

This proposal is in spirit an important first step in ensuring against tech industry magical thinking around consumer consent. However, data portability measures and common user IDs may not increase benefit for consumers. Consent is considered a lawful way to trade consumer data, however, this measure is dependent upon anonymisation. Such controls on data are well known to be weak and insecure.

- ACCC Proposal 2 – Data separation mechanisms.

While consumers may have concerns about data being utilised in vertical integration, this is not where competition regulation could have the best effect. On the contrary, vertical non-market use of data should be encouraged. It is structural diversification which should be targeted for regulation and control.

- ACCC Proposal 3 – Rules to manage conflicts of interest and self-preferencing in the supply of ad tech services.

Please see response to ACCC Proposal 2 above.

- ACCC Proposal 4 – Implementation of a voluntary industry standard to enable full, independent verification of DSP services.

If the ACCC is serious about this proposal, they need to develop a structure for and pursue rigorous prosecution for the regulation. Voluntary codes are prone to exploitation.

Alternatively, rather than pursue demand side codes, the ACCC could encourage, amplify and even develop regulation which encourages innovation in this space to improve consumer welfare.

The reason for this is simple. The current proposal overstates market power and understates the importance of innovation in Big Tech competition. Focus on demand side, and Google in particular, might not fully comprehend the role stress of maintaining innovation in such a Big Tech firm. A focus on market power alone at any point in time avoids the reality that uncertainty is the key competition determinant in digital economies. For example, the massive rise in Zoom during the pandemic – at the exclusion of Google - is an example of how uncertainty leads and Big Tech bleeds.

ACCC Proposal 5 – Implementation of a common transaction ID.

Putting a price on data alone may not affectively ameliorate the key urgent concern of consumers that data privacy is being breached.

- ACCC Proposal 6 – Implementation of a common user ID to allow tracking of attribution activity in a way which protects consumers' privacy.

Close examination of cryptographic protocols and human cyber weakness indicates that while this proposal is a positive measure to prevent fictional and false consent it is not a cure all in the medium to long term.

In addition, very recent developments in econometrics mean that unbounded dynamic programming via the Q-Transform and competitive equilibria can be recovered as solutions to dynamic programs. This means that non-linear dynamic competition may not just be captured but programmable at macroeconomic scales.

Temporary Conclusion

In conclusion, the ACCC might consider broader proposals for trade-offs between short term and long-term consumer welfare. On the one hand all regulation benefits big players because they can easily pivot faster than small competitors. On the other hand, static competition undervalues just how much innovation is required by Big Tech to compete. Rather than pricing consumer data, harder restrictions on IP control would encourage Big Tech innovation investment. One example demonstrates how this focus skews the broader market. The ACCC has focussed upon Google due to market share. However, People's Republic of China based Big Tech companies Tencent/WeChat have also adopted a Google style model. At minimum 600,000 Ethnic Chinese Australians and up to a 1.2 million people sized market in Australia cannot operate within this defined market without ascribing to the market power of Tencent in Australia. Ascribing to the Tencent platform requires political affinity with the Communist Party of China. Tencent's domination of the market in Australia is near 100% and is also tied (unlike Google) to authoritarian non rule of law controls. There are zero references to Tencent in the report.

I would suggest the ACCC support innovation instead of just controlling competition. All regulation will favour the big players and reduce diversity. There will be unintended outcomes for consumers and forms. Regulation to control so called 'monopoly' in tech spaces may ironically discourage new entrants. Arguably, Big Tech giants like Google are not even monopolists in the old sense, perhaps not even at all. While they may look and feel they do, on closer inspection, Big Tech firms do not have the market power of traditional monopolist at all. In a Big Tech based economy, demand and supply curves go the opposite way of old school economics. Market share does not equal power in a linear fashion.

This is both a problem and new opportunity for a regulator. The ACCC has an entrepreneurial flair for courageous global intervention. A concern may be enforcement fatigue and resourcing deficits leading to paper tigers. The ACCC needs to be a disruptor. But an innovative one: The ACCC needs to go harder on enforcement of intellectual property infringements, intrusions into new markets, while also encouraging new forms of consumer demand.

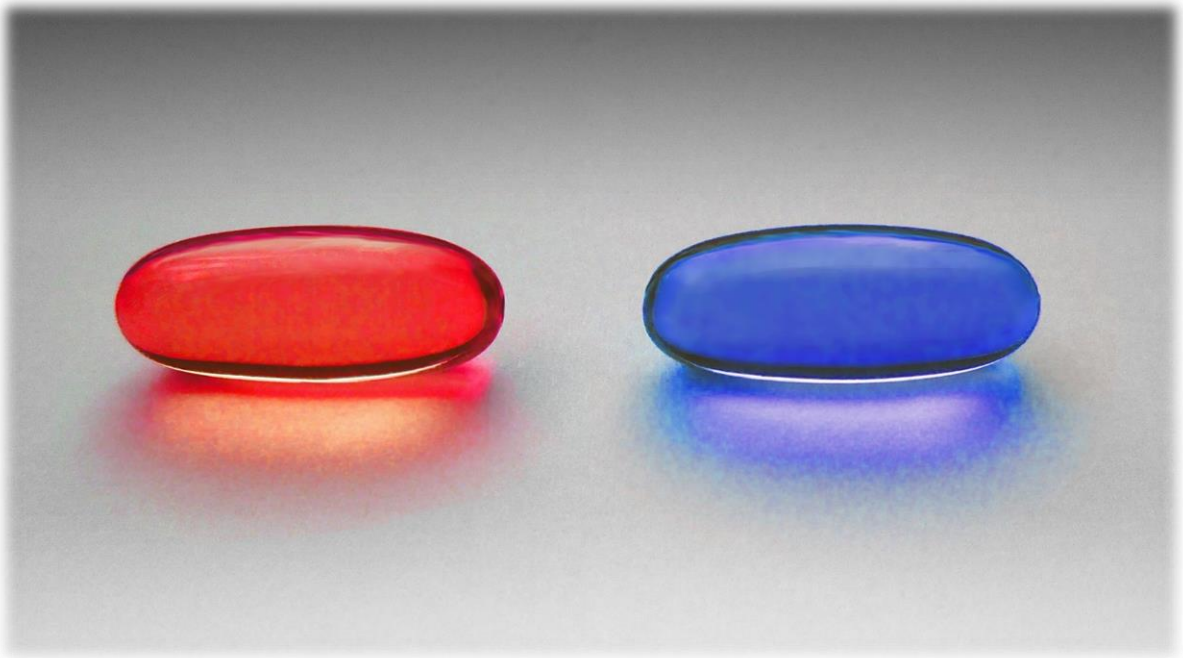
Overall, as a society we need to decide which data to ascribe regulation - not all data. We need to develop innovative ecosystems at least as much as control market power. Much of the data collected in advertising is an issue not just because of market dominance, but because it is the wrong sort of data to tackle our continental and planetary problems. Schumpeterian rents and innovation pressures to free up the use of that data may be in long run be more important than short term Ricardian rent competition policy.

Tom Sear, UNSW Canberra Cyber at the Australian Defence Force Academy. 31/03/21

APPENDIX B

Cyberstorm & Xenowar 2020-2035: CI & Strategic Society

Tom Sear, Protecting Critical Infrastructure and Systems of National Significance Consultation Paper, Submission 1.0



The importance of context: locating critical infrastructure

This submission argues that to protect critical infrastructure and systems we must fundamentally understand how they exist and operate within a new kind of digital society and rapidly changing planetary systems, including the biosphere and the infosphere. In this world, attacks on infrastructure are as much aimed at destabilising social cohesion and trust in democratic civil society as they are at interrupting flows of power, communication, services and resources on which that society depends.

The pressures of a planetary polity is gradually overtaking geographically and historically defined globalism. In the twenty first century 'planetary' forces and information flows are reorienting society. Familiar binaries of conflict are breaking down and existential threats are often within our national borders.

The digital has revolutionised Australian democratic society. Information and Communication Technologies (ICTs), through the Turing revolution, have created the present era. In this epoch, not only is the mode of production informational, but society exists within this 'infosphere'. Infosphere-dependent western societies exist in a constant state of Cyber-Enabled Information/Influence Warfare and Manipulation (IIWAM) in an era of post-Westphalia (polis-State) computational 'Stack sovereignty.' The institutional rules of cyber space – where nation states are forced to cooperate while avoiding outright cyber conflict, compounds the motivation of adversaries to undermine societies, with critical infrastructure operations combined with the new sociotechnical and social media dependent form of disinformation embedded within ICTs.

Climate change is also now affecting critical infrastructures. Impacts from the increasing size and intensities of climate disasters have and will continue to affect Australian society and ecologies. In 2019-20 many Australians felt that we are fighting a frontline of an overwhelming but uncontrollable existential threat. Smoke occluded our cities, firestorms engulf our homes, biomes and animal life were eliminated. Apocalyptic panic and a sense of threat exuded the air.

Australia's response to Black Saturday meant a revision of fire ratings and how to most effectively manage and education public and industry's response to risk. We will see an immediate future in which these sorts of conceptual revisions occur across multiple new areas and scales. Even within Federal Government accountability and risk assessment is distributed across overlap with Attorney General, Home Affairs, Defence, Environment, Climate, Disaster recovery to name just a few. Greater interagency cooperation and integration will be inevitably required. The expansion and consolidation of Home Affairs has gone some way to dealing with these wicked systems of systems problems.

We will see an escalation, acceleration, and convergence of risk. The division between the 'natural' and 'information' environment will experience convergence.

2020 has demonstrated the portents of constant change and rapid response that will mark this century. The impact of the SARS-Cov-2 and the COVID-19 pandemic stretched public health and Governmental resources to respond. Simultaneously, health systems had to be defended against ransomware and cyber security threats.

2020 feels like a moment of decision in choosing a *Strategic Society*.

This means there is an increased need for government to focus at a strategic level on building resilience in society against internal and external threats. For CI this means Government needs to lead, but support legal frameworks, interagency cooperation, volunteer resources and connections across industry and government, confronting contest even below the level of, but not discounting combined with outright kinetic conflict.

In the 20th century compartmentalised silos were the best way to respond to organising information around thematic threats. Now not just Government must change – we need a *Strategic Society*. The response will have to be whole of society to be truly effective.

In this submission, I will initially use the classic metaphor of the red and blue pills from *The Matrix* to explain some of the complex choices we face in relation to critical infrastructure.

The Matrix has become a cliché for awareness: red and blue pills as a metaphor for consciousness. But its also now a comfortable pharmaceutics of choice. Thought experiments and platonic binary choices are now also behind us. We are now immersed in the clinical human trials of a new form of governance – governance by the curve: flattening the curve, the Gartner Hyper Cycle's Trough of Disillusionment of Post-Truth, trashed economies, and the recursive 'Eternity politics' of social media Power Law curve.

Commensurately, critical infrastructure resilience protection is now beyond the effect of 'tactical surprise' and required at the level of the 'Strategic Society.' What Home Affairs and the Critical infrastructure Centre are developing in this plan for protecting critical infrastructure will likely be adapted and applied soon to areas that neither Home Affairs nor society will expect. Systems of National Significance requiring such strategic protection will necessarily expand. Rather than providing feedback by looking inward on the *Consultation Paper*, I argue here an outward expansion *from* the *Consultation Paper*.

Red Pill

Life in Australia exists within an internet-enabled era of strategic competition. The result is a Vulnerability-Threat Matrix of cyber measure vectors. Geopolitical cyber power is constantly contested at just below the threshold of outright conflict within and through planetary scale internet infrastructure where sovereign borders may be unclear. Equally, the threat of outright kinetic conflict from a large-scale multi-vector pre-kinetic military incident is also present danger.

Two concurrent infrastructure challenges confronts Australian society: a current persistent and ongoing threat which, within the infosphere on which society depends for existential survival, occurs across a binary around which society has been constructed and enforcement can operate - the private enterprise/ government split. At the same time, the infrastructure itself is largely dependent upon a Global Value Chain (GVC) of supply which may contain security threats and has a continuing future dependency upon those via IoT. The threat to that environment is a cyberstorm/blitzkrieg event ahead of any kinetic action.

In addition, the critical infrastructure of the socio-economic-political function and primary communication now operates in platforms that are subject to the legislation of domains managed by other governments, some of which Australia is entangled with in an interaction that might be described as 'cooperating to compete'. Australia has committed hundreds of billions of dollars to buy weapons platforms for the contingency of major war between 2030 and 2060. But it is inadequately prepared to respond to the reality of current internet competition, nor to generate the shared societal resilience required to create and implement the policies, processes, and procedures needed for identifying and responding to a multi-sector cyberattack targeting critical infrastructure.

The *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper* is a welcome initial response to these concerns. A positive start which challenges the many Bridges of Königsberg the Australian government will need to build with industry. There is more to be done, however.

Here I allude primarily to the larger scale challenge, which involves making additions to the plan outlined in the *Consultation Paper*.

There is no escape and evasion map to be developed, as Australian society and the continent itself ***is*** both the map and the ground, which makes scaling from models profoundly difficult.

Overall, the *Consultation Paper* and Home Affairs are exploring and taking responsibility for the existential requirement of protecting critical infrastructure. However, the critical functions of everyday social life take place in areas largely not managed by them or spread across other areas of government (social media, the economy for example).

So, those areas the operational plan and tactical planning that the *Consultation Paper* targets are just one form of cyberspace where cyberwar and cyber warfare is, and will, take place. Typically, we focus on the 'necessary' existential areas of critical infrastructure such energy, water, food, transport. However, as it is becoming increasingly clear the social environments such as communications and the climate change impacted environments of the natural world might also be considered spheres of Critical Infrastructure. To defend a systemic conflict requires even more systemic thinking and unthinking. This is because critical infrastructure attacks do and will target both the functional *and* social systems.

In this reality, everyday conflict and sequenced cyberblitzkrieg would take place across these areas deliberately, and all future war is taking place in them *today*. I call this a State of Xenowar.

So, in my view the plan is insufficiently focused on wider contexts such as society and the environment and should expand into considering the development of an Australian strategic society in cyberspace.

Blue Pill

The blue pill looks increasingly attractive: the information environment has decayed even faster than our planetary climate. Awareness of our biological fragility has become apparent just as in last five years the involvement of nation-state adversaries blatantly intruding within critical infrastructure has been made clear. Even living in knowledge and truth - even supposed rational inquiry and 'knowledge' implicit in the fin di siècle red pill in a contemporary era of social media promises an informational disintegration into the perspectives of crackpots and conspiracy theorists.

However, the scale of the *Consultation Paper* and Home Affairs remaining unaware or silent on how society is incorporated into the threat matrix and just accepting the positive steps of the paper into outreach and collaboration will not prove sufficient. Ignorance will not prove bliss.

This is because the binary choice of ignorant bliss or painful awareness has itself been deconstructed.

The red and blue pills of *The Matrix* - just as much as Donald Rumsfeld's famous aphorism - have located the nexus of this challenge in epistemology. There is a lot of focus in current security conversation on knowledge, but very little on thought. Or, rather, there is little *sharing* of that thought in providing the security of a society's critical infrastructure across our institutions and interactions, not just in government or even in the military, but across society and corporations. The *Consultation Paper* and Home Affairs approach is the start of balance towards a capability that functions as an output and towards multi-focal temporal frames in the era of non-linear chaos that already marks the twenty first century. The fluid dynamics of an emergent, chaotically turbulent century will necessitate the aperture dilation for this vision, open to strategic scenarios.

Influence, not interference, is the real goal.

The reason why we must take this approach to resilience with some resoluteness is apparent from the nature of the geopolitical strategic environment. We worry a lot about means, how would we defend a power grid for example, but little why it would be attacked. It is not about shutting down a city's power but showing you can influence a whole population. This is where information attacks and critical infrastructure measures intersect and merge with strategic competition. The strategic goals are higher than the means. A 'hack and leak' operation has the same objective as shutting down a critical infrastructure. Increasingly we will se them deployed din consort. 'Sandworm' or sewage farm, social media or the electoral division of Sandgate, billion-dollar submarines in the South China Sea or the supply of 'battered savs' to South Australia – the ends are more important than the means.

Neo has been hacked: the strategy is to ***influence***.

As we have learned from studying the intrusions of nation-state actors, the primary goal is not to shut down infrastructure. It is to undermine trust and confidence in the structures and relationships that hold our society together: cultural and social cohesion, the public/private partnership, and the idea of government itself.

Speculations and Provocations

In this submission I offer some speculations and provocations to shift the conversation into this new territory, where the endgame is not only to protect infrastructure but the bonds within society itself. They include:

- How do we build national resilience towards malign influence and activities in the New Information Environment?
- How do we have a meaningful conversation with the public about a contested environment they may know very little about?
- What is the role of the ADF?
- How should middle powers plan for defence of the home front against the contingency of cyber blitzkrieg and mass information war of the kind that great powers seem determined to be prepared to fight in the medium- and long-term future?
- Total cyber security of critical infrastructure is not possible, and State is not the complete sum of the parts of like cyber security in a business enterprise -
- How would Australia confront an attack on air traffic control? Or *MyHealth* record? The stock exchange?
- How might data collected via *TikTok*, *Fortnite* and *WeChat* on October 1, 2020 in South Western Sydney be used in a geopolitical conflict in 2035?
- How might attacks on critical infrastructure effect a local storm system – say a cyber flood in Townsville along with a cyber drought in Canberra? At the same time? What does local and national mean? How to define scale from the size of virus to the scale of the atmosphere? Where to intervene and build bridges? How do Cyberlaneways of Melbourne differ from the Cyberlong-grass of Darwin?

The coming cyber storm

A cyber storm would involve multi-vector, multi-wave, multi-theatre sustained cyber-attacks and information warfare meaning:

- Multi-vector (cyber arsenals, hundreds of “tools”)
- Polymorphic malware (APTs)
- Multi-wave (sustained)
- Multi-theatre
- Civil and military targets
- Strategic targets and accidental targets
- Social influencing (information campaigns)
- How would be define and measure resilience? What is a dependency?
- AU has supported international efforts (APEC, ARF, APCERT, GGE) but these remain quasi-conceptual.
- AU does have a national CI strategy, but with little attention to CII compared with USA and UK: We are not prepared yet to ride-out a cyber storm.

A new kind of war: Xenowar

Future AI will use social media data generated, manipulated, and captured now to train systems and target people in 2035.

Not only will data be a military objective in the future, it already is. Rather than war being a human activity, all human activity is now war. Cyber influence/information operations (CIO) with lethal effects will warp and extend the LOAC (Article 52) via access to civilian data.

The 'speculative fiction' section at the start of this article (quoted below) may be useful in explaining how it might work:

Tom Sear, 'Xenowar dreams of itself', *Digital War*, July 2020.

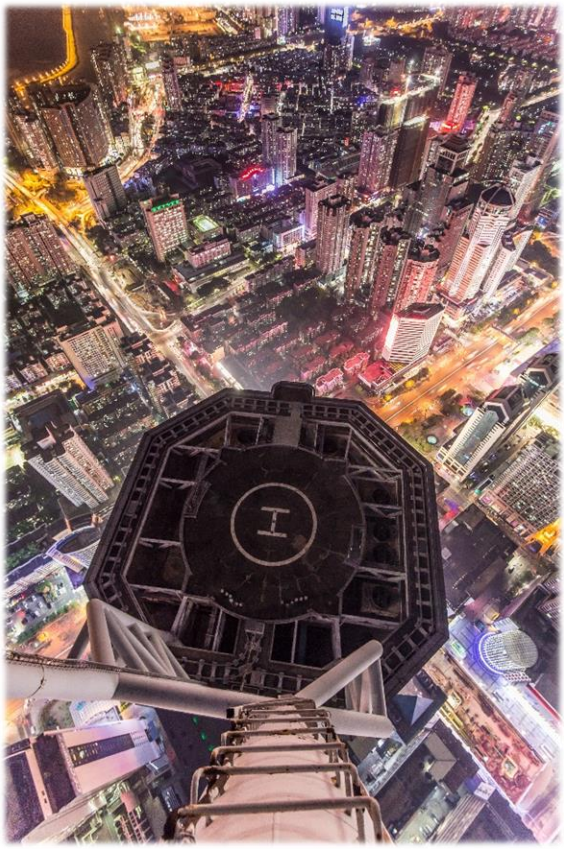
https://link.springer.com/article/10.1057/s42984-020-00019-6

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7376277/

Xenowar dreams of itself (excerpt)

"October 1, 2020. Western Sydney, Australia. Still in a semi 'Rona Iso' 10-year-old Australian Chloe Yingchao is playing *Fortnite*. Eliminated, exasperated, she posts an ironic emote parody on *TikTok*. Her mother turns from her own PC and suggests—in Australian Mandarin/Dialect hybrid—Chloe's social time is up. Time for homework. Briefly distracted, Chloe's mum takes a photograph of her daughter and shares it to a chat group in Chinese-owned social media app *WeChat*.

On the same day, 20-year-old junior engineer Xiang Kairan from Shenzhen is among a group that sits down to tea with Provincial Communications Administration officials and a local leader from the telecom company China Unicom. Ostensibly, the men are meeting to discuss the role of 5G within Tencent intercity mobility predictions for 'nowcasting' the epidemiological data for the spread of COVID-19 from Wuhan into Shenzhen since January. But the central concern of their get together involves different forecasting. Xiang is a junior city official from the industry and information technology bureau overseeing the planned installation of 45,000 5G base stations in Shenzhen, achieving full 5G network coverage by October 2020. COVID-19 had impacted the speed of the rollout, and they are behind schedule. The men are talking how fast they can catch up.



Flash forward to the year 2035, Chloe has just crossed over into Shenzhen with the help of the Hong Kong Republican Army (HKRA). A climate-change-induced weather event has helped Chloe slip in undetected via a port. Her arrival coincides with a spiral of geopolitical escalation. 2028 legislation in the EU led the US Congress and the UN to reconsider the nature of sovereignty itself. The unexpected death of Chairman Xi Jinping in 2033 led to a power struggle in the CCP. US President Ivanka Trump continues to affirm a policy of minimal intervention but elevates readiness to a state just below outright declaration of war. Over the previous seven years, critical infrastructure, energy, and logistical organisations required enhanced physical and digital defence from state adversaries and environmental protesters alike. Information has increasingly become central to production, the functions of civic identity and service delivery. A new breed of corporate warriors emerged as a cyber-military services industry to defend the ICT infrastructure and data, and as civil-military relations blurred, investment in the infrastructure of satellites and space and even the law of war began to change. Chloe is one of these operators.

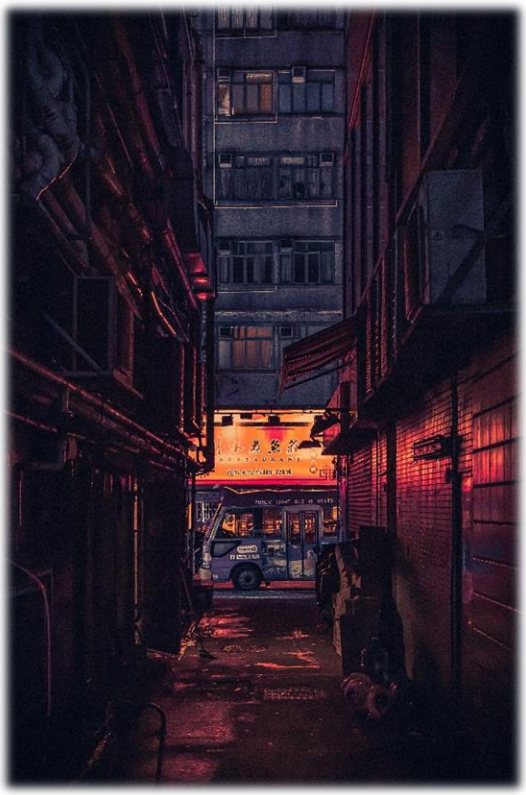
The flow on effects of all these events has resulted in an escalation of the previously grey-zone digital integrations of Taiwan into mainland political systems and destabilisation across the Indo-Pacific. A series of rolling multi-vector, multi-wave, pre-emptive and sustained cyber campaigns across global cities ensues. In response, former state official and tech entrepreneur—now regional warlord—Liu Yongfu has deployed a swarm of robot devices to control the City of Shenzhen. Whether this is to benefit China or himself in an internecine conflict is not clear. But the city is the base for many global cyberstorm events in other parts of the planet.

This cyberstorm generating system is dependent upon the now ageing 5G network backbone that engineer Xiang Kairan has control of as the chief technological official in the city. The global attacks also require the use of submarine cables near to where Chloe has come ashore, and their sabotage is one of the reasons she is there.

Chloe is now a cyber mercenary commanding a four-person team and a small swarm of air and water deployable sensor and offensive capable automated UAVs or 'Drones'. Jokingly codenamed *Operation Above the Neck* (脖子以上'改革) the Op has a human target. Chloe's target is Xiang Kairan. He is now a senior Internet of Things (IoT) engineer in Shenzhen. Xiang Kairan's biometrics are critical to the team's objective of sequencing a Cyber Typhoon - an event designed to create friction in the hub of China's information economy and military power.

Right now, Chloe has a more immediate problem—her own ability to see. In the shift to littoral city, Chloe's facemask fogs up. She is forced to remove the Australian-made mask. A flurry of metabolite creates a sensor wake.

The Australian adversarial AI — named *Maratus Vultus* — streams in response. Despite her electronic camouflage, facial exposure triggers the Shenzhen (电子对抗旅) Targeting AI - known as 'Assassin's Mace' (AM)/(杀手锏) – which deploys. Archival information is extracted from Chinese-owned data centres. Facial and gait recognition technology identify Chloe. The snapshot her mother uploaded onto *WeChat*, and the walking gait from the *TikTok* post in 2020 became part of matched and merged datasets. In 2035 the AI predicts her next tactical move. Assassin's Mace integrates five years of *Fortnite* data to predict behaviour, decision-making and mobility in Close Quarter Battle (CQB). Her own sensor swarm picks up the compromise and provides options."



Broad Implications

The article in *Digital War* that follows this piece of speculation looks back from 2035 to the discussions and decisions of 2020 and how they shape a world where social media impacts extend far beyond current definitions of influence and misinformation. Social media and foreign interference have become a means through which power can be exerted not only in the present, but towards future geostrategic goals. The issue for democracies is to maintain cyber security and digital sovereignty in a time where boundaries degrade, legal parameters are blurred, and policy constraints lag. In those times, technological knowledge, digital literacy, and social and cultural identity will need become fused into cohesive principles with national objectives to ensure the safety of a strategic society and a nation's digital sovereignty.

Democracies play by the rules, they work within mutually agreed resource, moral and environmental constraints, but corporations and other kinds of states do not. Government needs to understand how its management of all these domains at the broadest scale plays a significant role in ensuring we take an integrated approach to social cohesion, economic stability, defence, and security. Persistence and consistency need to be applied across the whole of government, not within siloed departments that are a relic of the sovereignty and security frameworks of the 20th Century.

As one of the few in the public gallery, I sat through days of the Lindt Café Siege Inquest relating to the deployment and use of highly trained ADF Special Forces and snipers with extensive Middle East experience. SOF operatives at Holsworthy as soon as they had heard the siege was on immediately recreated the Café in flatpack and drilled and drilled practicing the assault over and over, while elite snipers were on site and their advice was never sought Subsequently, calls for lowering the threshold of call out for the ADF to respond to domestic terrorism took place. As a result, the Defence Act 1903 was amended. Lindt was tragic and such direct comparison may be incorrect, but death tolls from critical infrastructure incidents may in future equate with the existential threat of terrorism. Some in the ADF will be annoyed with me suggesting that, while others will be frustrated as they stand by unable even to deploy specialists who have the skills and readiness to serve.

More recent existential threats provide insight to how threats might arise, but also how we can respond. For example, bushfire could be itself a terrorist threat to critical infrastructure. A small, dedicated group with transport who monitor vulnerabilities and simple technology could create widespread havoc, or even simply claim attacks which were not theirs. Our intelligence and security agencies would have combined skillsets and new data sets to respond to potentially explore in an emergency.

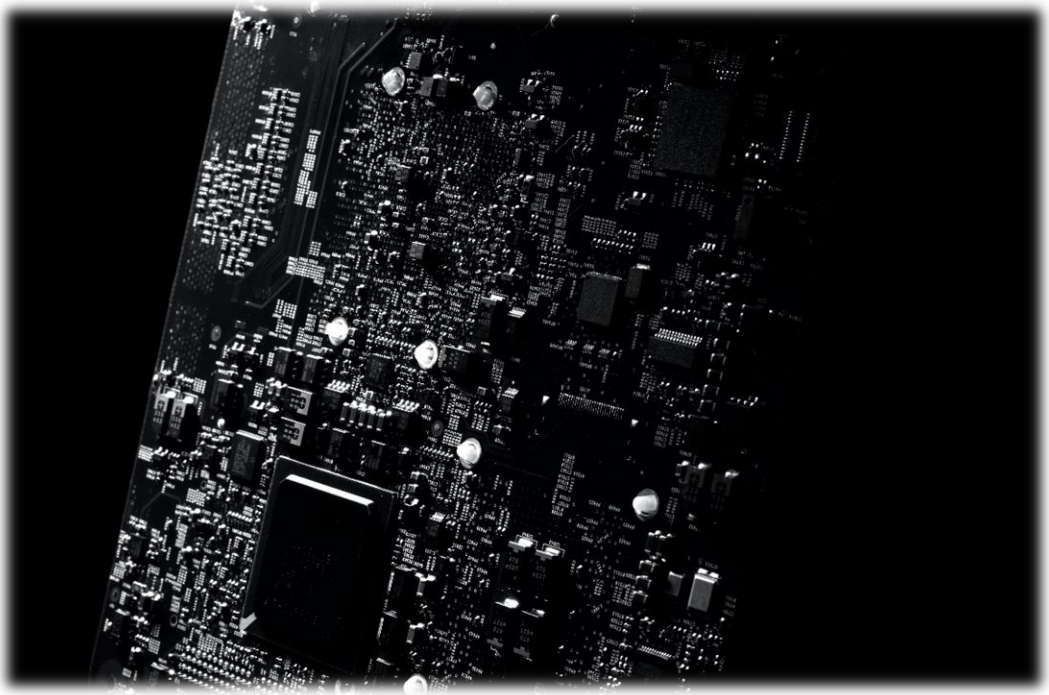
In cyber we worry about cyberstorm events – a series of rolling multi-vector, multi-wave, pre-emptive cyber-attacks sequenced in a way to create complete social chaos – cutting Eftpos, wiping Centrelink's databases, cutting power, water, energy, deep fakes, and disinformation. We got a taste of this during the fires with lines for one old hardwired old Telstra phone booth, lines to wait for supermarkets, crashed communication systems. Almost certainly our global adversaries will have closely followed the breakdown and where the gaps and failures where and how sequencing mattered, as model for how to sequence civil cyber-attacks.

In cyber some have been arguing for a Australian Cyber Civil Corps connected with ADF but centred on responding to cyber emergencies in the civil sector. At the height of the Bushfire crisis MP Mike Kelly called for something similar in response to future fires. Some wonder why it is ex-military leaders who often think of these ideas or are asked to head up response organisations – it's because they think in the larger strategic, and logistically integrated way needed to truly tackle complex

problems. For example, one of the most productive discussion I've had is when scoping how a city like Sydney might respond a large-scale cyber-attack discussion with Mark Smethurst - one the most brilliant Special Forces Commanders of the recent era – who best understood the larger threat matrix.

Security threats have in the last 30 years turned back into the Homeland. Home Affairs restructures have been sensibly in some ways closer to the US Homeland model, but insufficiently evolved in others.

Australia might consider exploring steps to develop a US style Federal Emergency Management Agency (FEMA) to respond to coordinate disasters which overwhelm the resources and borders of states. Historically many of these type organisations arose from civil defence legislation as the cold war tension eased. In Australia for example this is how the SES was created.



Recommendations

There are multiple implications and recommendations that might flow from thinking about protecting infrastructure within a larger societal frame. Some are included below, with multiple options offered to allow for diverse responses at different scales and to fluid, evolving situations:

- Define the cyber power of Australian Government and enforcement within a defined and critical infrastructure of cyberspace.
- Include all social media within the definition of cyberspace and cyber power and enforcement.
- Map what is civil Australian cyberspace.
- Map and locate interdependencies in relation to maintain that cyber border security.
- Know what resilience is and have a measure for it that is understood across industry.
- Understand what insider threat is and integrate with agencies which have jurisdiction for those in Australia.
- Define what a cyber offensive response is when it is considered proportional and justified.
- Empower initiative and action in government and industry to risk assess and act towards secure supply chains in the GVC.
- Map how current legislative Acts intersect and directs response to emergencies: are they fit for purpose?
- Explore steps to develop a US style Federal Emergency Management Agency (FEMA) to respond to and coordinate disasters which overwhelm the resources and borders of states.
- No active measure now, or future storm or sequenced coordinated significant cyber incident which precedes a kinetic attack on Australia or other place, or space, will involve just the 'base' of existential infrastructure, so therefore: include the superstructures of social media and its regulation, consumer privacy and protection within a wider framework.
- Ensure that shared responsibility for CI requires Federal agencies to adopt concurrent lines of effort: threat response; asset response; and intelligence support and related activities. This means the development of a centralised CI leadership group - a Cyber Directorate (CD) - which functions in support of the National Security Committee (NSC) and is accountable to the Minister for Home Affairs and explores the possible access for rapid deployment of domestic forces for counterterrorism in the AFP, and State and Territory Police forces. With the Attorney's General Department and advice from the Cyber Security Strategy Industry Advisory Panel should actively explore the security of the Global Supply Chain for Government and advise industry.
- Develop a cyber Unified Government Group (UGG) and a Business Operations Organisation Taskforce (BOOT) operating in consort to insulate against future threats (perhaps with a less 'warm & fuzzy' acronym).
- The UGG BOOT to develop and revise a National Cyber Incident Response Plan (NCIRP) Federal Interagency Operational Plan (FIOP) in coordination with the Cyber Directorate (CD) composed with DFAT, ASIO, ASD and the ADF, but with secretariat functions arising from Attorney's General Department. Cyber Security Strategy Industry Advisory Panel to be able to brief and direct the CD.
- Develop a National Security Telecommunications Advisory Committee whose goal is equivalent to leading science that supports infrastructure for cyberspace equivalent to the cultural values that were depicted in Working Dog film *The Dish*.
- Develop a 'Cyber *Castle* Committee'(CCC) dedicated to educating and advising Australians on the 'Cyber Vibe'(CV) of citizen critical infrastructure protection.

- Develop an interagency government subcommittee and Information Directorate (ID) to report disinformation campaigns and misinformation operations in social media. Integrate that Directorate into any relevant government committees and defence organisations developing a significant incident response.
- In recognising that Australian society operates in an Infosphere, dependent upon critical social infrastructures, perhaps in lieu of the above *Dish*/*Castle* initiatives, explore the development of a joint Government/Defence Agency Strategic Society Communication Directorate to ensure not only unified communication, but also integrated assessments.
- The Government should consider a fundamental strategic reorientation of Joint Chiefs to acknowledge the reality of cyberspace operation within sovereign borders and manoeuvres in relation that cyberspace.
- Government (and potentially with industry) should encourage the ADF to develop and wargame a unique, combined and streamlined Special Operations Command/Information Warfare Division/Australian Signals Directorate *Storm Command* to operate in emergency cyberstorm events. This leadership group should have in emergency situations, command and control of time-sensitive cyberspace operations to be actioned in any large-scale critical infrastructure or significant cyber incident by consolidating them under a single commander with authorities commensurate with the importance of such operations that may occur in Australia. Prime Minister and Cabinet should lead a paradigm shift for leadership to understand strategic relationships in a spectrum.
- Develop and conduct a large scale biannual cyberstorm exercise.
- Impose swift and costly consequences on actors who undertake malicious cyber activities against critical infrastructure. Both specifically, and in a widespread re-examination of offensive action. For example, ransomware attacks are a serious risk to critical infrastructure day to day, during emergency events and would be part of any sequenced cyber storm attack. The categorisation of these actors needs to be reconsidered to become subject to action from appropriate agencies and forces in day to day operations.
- Explore how CI relates to differing authorities in the ADF (and in government and industry) between intel/MISO and attribution requirements. This includes how definitions and authorities drive the IT infrastructures for response.

Further listening

For a podcast exploring how to build scenarios on this topic: https://soundcloud.com/unsw-canberra-podcasts/s1e8-cyber-war-with-breakfast-burritos-new-fiction-with-john-birmingham-password123

How would a cyberblitzkrieg start a war in twenty first century? John Birmingham discusses on his new book 'Zero Day Code.'

20 October 2020

APPENDIX C

Tom Sear, UNSW Canberra Cyber at Australian Defence Force Academy.

[redacted]

[redacted]

Tom Sear is an Industry Fellow in Cyber Security, UNSW Canberra Cyber at the Australian Defence Force Academy (ADFA). He has advised parliaments and industry on social media manipulation, counter influence initiatives, IoT and 5G policy, and worked as a cyber security practitioner in government. His research concerns how to build resilient national computational cultures to defend against active measures, manipulation, and cyber storm. Tom led data analysis projects to analyse cross platform nation-state social media propaganda influence operations during elections, including cross lingual work with *WeChat*. Tom has a long association with the international Special Operations network, including a current collaboration with Joint Special Operations University (JSOU), USSOCOM, MacDill. During the current COVID-19 pandemic he has contributed to the Global Volunteer Emergency Response Community as part of the CTI League. During the bushfire crisis contributed to the community mis/disinfo response, OSINT mapping and public work supporting and exploring the role of the ADF: https://ab.co/3dt6cfu & https://bit.ly/3jX7TUQ

Profile: https://bit.ly/2wj2KSM

Academic journalism: https://bit.ly/2CUkDrV & https://bit.ly/2FhEAdh

Podcast: https://bit.ly/2l4Crec