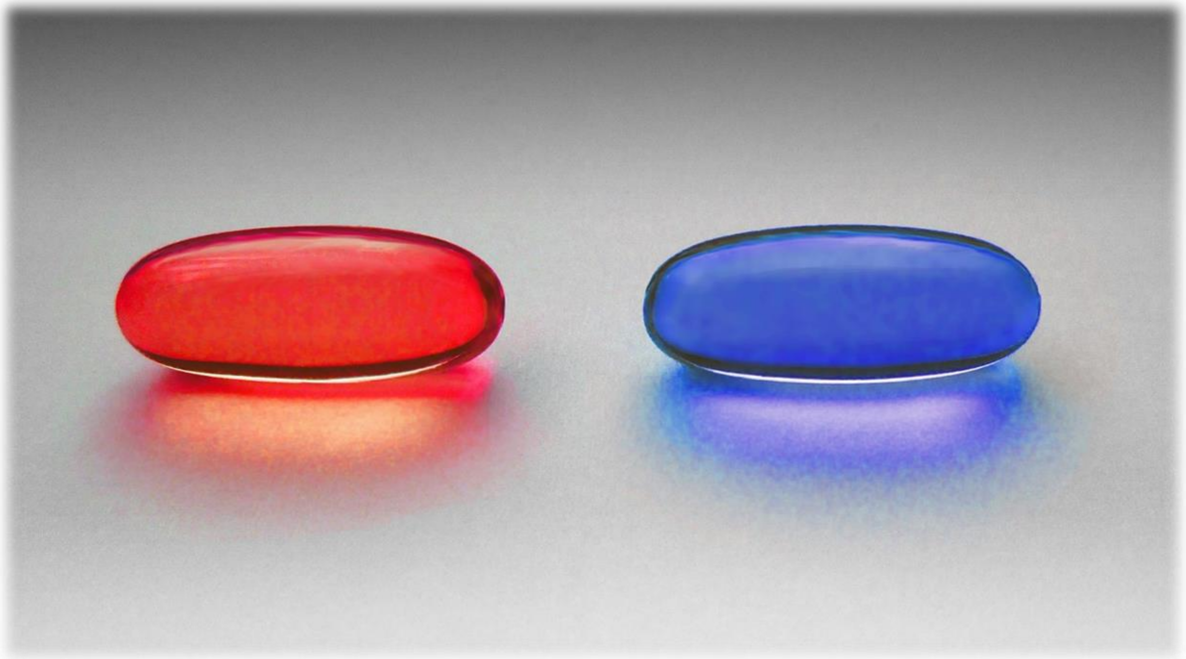
Cyberstorm & Xenowar 2020-2035: CI & Strategic Society

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 in the near future 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 really about shutting down a city's power but showing you can have an effect on 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.

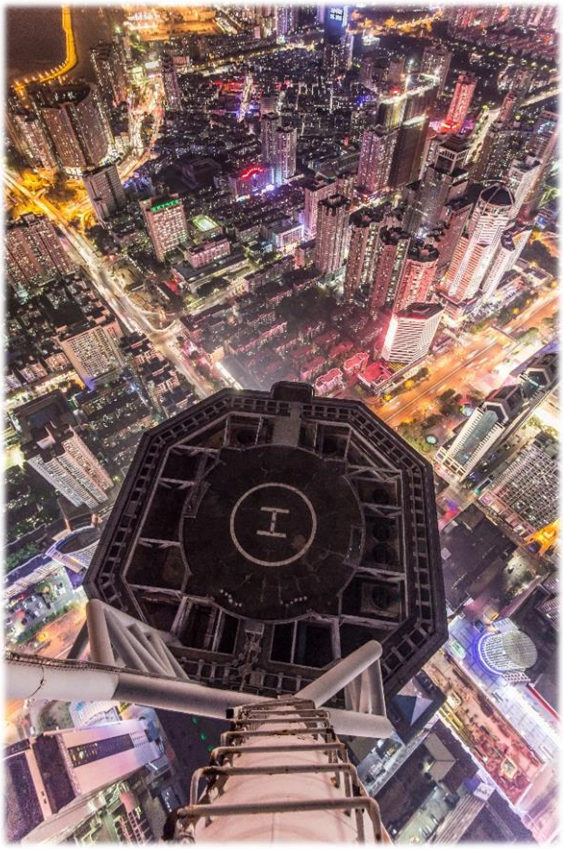
https://link.springer.com/article/10.1057/s42984-020-00019-6

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.

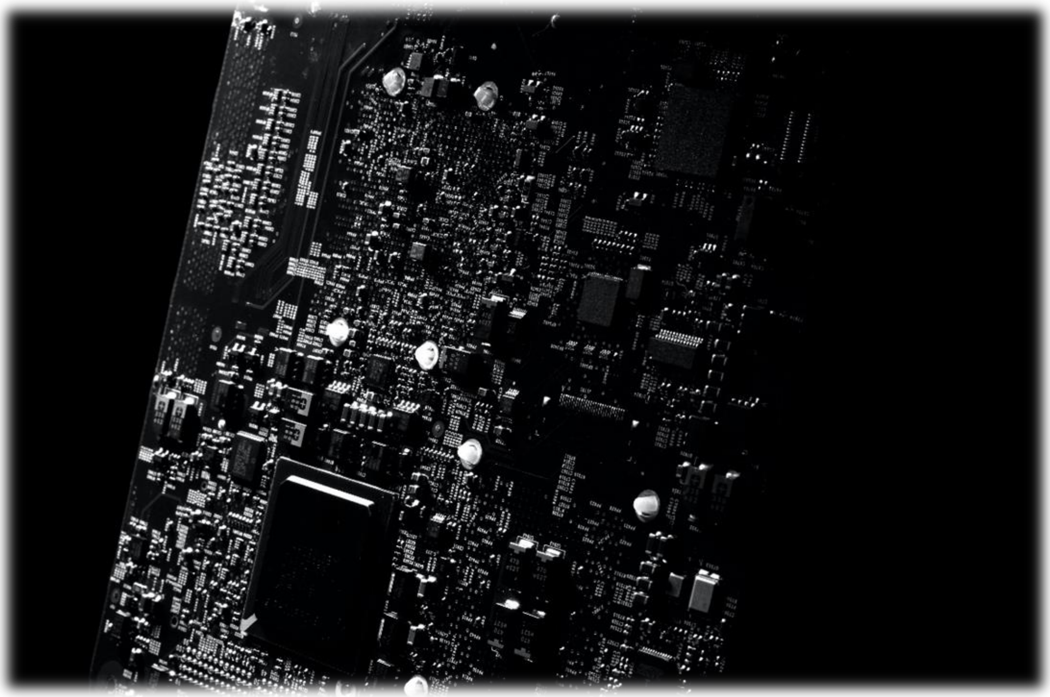
More recent existential threats provide insight to how threats might arise, but also how we can respond. For example, bushfire could be itself a terrorist threat to critical infrastructure. A small, dedicated group with transport who monitor vulnerabilities and simple technology could create widespread 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

Developing an Australian volunteer cyber response capability for critical infrastructure protection

Tom Sear, Protecting Critical Infrastructure and Systems of National Significance Consultation Paper, Submission 1.1

This year, I have been one of the few Australians involved in the COVID19 CTI League. The CTI League is the first Global Volunteer Emergency Response Community, defending and neutralizing cyber-security threats and vulnerabilities to the life-saving sectors related to the current COVID-19 pandemic. This experience has provided me with the insight to how effective volunteer expert responses to complex system emergencies can be in building and ensuring resilience.

Like the response to SARS-CovV-2, critical infrastructure protection is 'wicked problem': the social complexity and interdependencies ensure the problem is stochastic and non-linear. This 'system of systems' challenge is precisely the pivotal vulnerability and why nation state adversaries target CI in an era of strategic cyber contest.

Ensuring resilience requires considerable cooperation, knowledge, and responsibility sharing. The Consultation Paper pursues a 'collective understanding of risk within and across sectors', and a 'positive security obligation for critical infrastructure entities, supported by sector-specific requirements.' In addition, the paper recognises the most difficult challenge in ensuring resilience and security in critical infrastructure, namely: 'interconnected nature of our critical infrastructure.'

As my initial submission (1.0) indicated the internet has fundamentally changed the threat matrix to critical infrastructure for Australian society. The Australian population is immersed within digital geopolitics in an era of strategic competition and real attacks in CI networks have escalated since 2014. Now to return the conclusion of my first submission: what can we do as a society?

One other trend - which my research on digital Anzac - reveals is that across the political spectrum there has are continuities between traditional moral accountability and very new forms. One of these is volunteerism.

Based on this continuity, outlined is a proposal below. This idea is far better suited to response to a cyber storm event or attacks on critical infrastructure protection contingencies arising from protracted and complex, multi-vector, multi-wave, multi-theatre attacks against cyber assets. Such an idea raises much more serious ethical concerns when considered in relation to free and open political domains such as social media. However, in a time when providing an adequate response to such an asymmetrical threat to our society is evident, it is presented here as an idea.

Historically, throughout the 20th century and into the 21st, all sides of the political spectrum have participated in the collective defence of Australia. For urgent high-tech military threats from great powers, Australia needs to rely on flexibility, innovation, and volunteers. That is one lesson of defence of Australia and operations in New Guinea and the Pacific in WW2. For instance, the 39th Battalion soldiers of 'Maroubra Force' - responsible for the heroism of the Kokoda Track – were all militia. This project explores the relevance of that lesson as Australia confronts potential armed conflict with a great power in coming decades.

Australia faces a wide spectrum of cyber risk. In an era of planetary scale computation, the critical information structures, and data flows upon which a sovereign nation depends extend across borders and into all levels of society. Fundamental security extends beyond traditional defences and into people centric, civilian and cybercrime contexts. Critical national, state, and private infrastructure and data management is increasingly shared with business and the community. This diffuse, emergent information frontline is also rapidly changing. The Internet of things (IoT), for example, will escalate security risk in fundamentally new ways. A systemic failure or cyber-attack on critical infrastructure may be catastrophic, with widespread flow on kinetic effects. Just such a 'Cyber Storm' will create response vulnerabilities in military civil affairs arising from protracted and complex, multi-vector, multi-wave, multi-theatre attacks against cyber assets. Such assets can include critical civil infrastructure, military C4ISTAR, computerised systems in weapons platforms, and even other civilian targets of military or national security significance. Further, the increasing intrusion and manipulation of automated influence operations, and cyber propaganda efforts from adversaries in western democracies, are likely to undermine stability and increase political turbulence. Simultaneously, Australia faces a cyber-skills shortage to manage these risks. The capacity to resource and train the skills and standing capacity within just the ADF, ASD and police forces will become an impossible burden.

An urgent response to these threats is required. Auxiliary capacity forces are a novel response to remaining adaptive to unpredictable, rapidly changing threats. At least two possible responses have been articulated in Australia and within our allied partners. Some proposals include a defence-based Cyber Reserves within force structure redesign to incorporate cyber at all levels. The United Kingdom and the United States – although functioning in different ways - both have adopted Reserve units and recruitment models. In the UK, for example, the 2011 Future Reserves 2020 documents recommended the engagement of Reservists with specialist skills and the active outreach to skills in IT firms and the establishment of larger structure around the Defence Cyber Operations Group.

A second, possibly complementary, approach has a civilian focus: the creation of an Australian Cyber Civil Corps made up of volunteers. This Corps would be independent of, but linked to, the Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC), while being capable of providing a disciplined command structure to coordinate an emergency response. Such a Corp might be a government service functionally closer to ASIS or ASIO than the ADF and AFP.

This research proposal would consider the challenges, opportunities, and viabilities of both above models and any other alternatives which arise. Research would be an international comparison and review of options and their applicability to an Australian context and threat environment. Interviews and discussion with relevant areas in Australia would be pursued.

The research proposal further considers the volunteer cyber forces considering the core values and shared cultural understandings which frame the information ecosystem of Australian nationhood. An aspect of research explores how the concept of Anzac has been uploaded and incorporated by digital publics into cyberspace for the 21st century. This work explores how the notions of the past are adopted in the digital present for future cohesion and political turbulence in an international post-trust, cyber propaganda, bot context, where old school espionage is activated in new ways. Volunteer citizen Armed Forces mobilised in times of emergency are the bedrock of Australian culture. The Australian way of war was developed at Gallipoli. It involves the projection of power from a small, highly geographically isolated nation into and onto the world map. The novel deployment of this concept now needs to be reimagined for cyber. Our nation has a long history of coordinated volunteer effort to respond to national crises, whether it be the State Emergency Service or the Rural Fire Service – it needs a similar capacity within digital and cyber emergencies.

NEXT STEP OUTPUTS:

Feasibility assessment report for target group: PM+C, Home Affairs, Australian Cyber Security Centre (ACSC), ASD, Defence, and Emergency Services. The report would explore technical, legal, operational feasibility of the option/s. A website and social media marketing to locate the report and provide source for media and public. Follow up focus group towards next steps.

- Focus groups and key informant interviews conducted with project target group: Relevant Ministers, PM+C, Home affairs, Australian Cyber Security Centre (ACSC), ASD and Defence, State Emergency Services(NSW), critical infrastructure owners, private cyber security practitioners, leaders of university IT courses.
- Legal advice on legal feasibility of concept with reference to current Australian legislation.
- Extensive professional survey and analysis of the capacity in Australian and international experience. The method of this survey might be based upon SEQ and SET evaluation techniques. The survey could be provided to an experimental sample set of the target group above. This approach would provide clear evaluation of where the concerns of the above groups are, where the gaps are and how the proposed auxiliary Corps might match those opportunities and gaps.
- To support the provision of guidance to explore how gender equality and culturally diverse Australians can be incorporated into the approach to the feasibility problem.
- Data collection and analysis for inclusion in final report. Transcription of key informant interviews and focus group events.
- Development of website and marketing promoting and providing online site for the report
- Meetings, and workshops to discuss report and action following its finalisation and hard copy publication.

Tom Sear, 2018/2020.

Tom Sear, Fellow, 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