DRAFT 24 June 2016

Proposal for an Australian Cyber Corps

Discussion Brief

A novel institutional response is needed to address emerging high technology security threats to the civil economy, the community and international interests of Australia.[1]

Main Purposes

1. To be the national authority for civil sector dependency mapping of Australia's critical information infrastructure, its data resources and its transmission flows, including international dependencies
2. To provide an auxiliary capability in a disciplined command structure for national civil and military defence response to extreme cyber emergencies
3. To develop, monitor and manage a response system for handling cyber threats to critical national or state infrastructure short of an extreme emergency
4. To develop, monitor and manage a national response system for handling serious cyber crime that may affect the national economy or social infrastructure
5. To develop appropriate international working arrangements to support these functions
6. To develop, monitor and advise on education needs for national military and civil defence of cyber space.

Ancillary Purpose

1. To provide leadership in national cyber space education for businesses and the community

Assumptions

1. Current arrangements for national critical infrastructure protection in cyber space, including for essential services, are weakly developed, with the federal government taking active responsibility only for governmental infrastructure through the ACSC
2. National policy recognises that such protection is a shared responsibility but there is no mechanism in place and no organized body of trained professionals for the unique and highly complex needs of critical infrastructure protection in cyber space, including for essential services
3. Australia will never be able to afford the cost of maintaining such capabilities in existing military and police forces
4. The pipeline for supply of skilled personnel in military and police forces is not adequate for the purpose
5. Existing priorities and mission orientation of the Australian Defence Forces and national and state police forces, including the necessary transitions for likely future operations in cyber space, are already so burdensome it may not be prudent to place national civil defence and strategic management of countering cyber crime in their hands

---

[1] These are outlined in several papers released by the Australian Centre for Cyber Security (ACCS) at the University of New South Wales Canberra in 2016: Greg Austin, "Australia Rearmed: Future Needs for Cyber-enabled War", Discussion Paper #1, January 2016; Greg Austin and Jill Slay, "Australia's Response to Advanced Technology Threats: An Agenda for the Next Government", ACCS Discussion Paper #3, May 2016; and Greg Austin and Jill Slay, "Benchmarking Australia's Cyber Security Strategy: A Future Looking Checklist", Briefing Note #1, April 2016.

6. The contours of future high technology threats to Australia in cyber space are sufficiently unpredictable to suggest that development of overly rigid standing structures supported by full-time staff with pre-determined skill sets, as in the ADF, would be the equivalent of building modern versions of the Maginot line
7. Extreme cyber emergencies in the civil sector in cyber space are of such low probability that a full-time standing response force cannot be justified, even if Australia could afford it
8. Since the overwhelming share of critical national infrastructure is in civilian hands and since an appropriately sophisticated understanding of the consequences of cyber crime is almost exclusively in the civil sector, the federal and state government must set in place an appropriate partnering structure for response because neither the government sector nor the private sector acting largely alone can develop and coordinate national response
9. A "neighbourhood watch" for cyber space (such as a set of information sharing centres) which has no response authority or response capability and is devoid of a command structure can be an important foundational element of national cyber defence but cannot address emerging circumstances appropriately.

Fundamental Capabilities

1. A highly secure and globally networked command, monitoring and operations centre independent of (but linked to) the Australian Signals Directorate and the Australian Centre for Cyber Security (ACSC)
2. Advanced knowledge of cyber dependencies in Australia's civil economy and essential services
3. Highly disciplined rapid response teams, based on the most highly qualified volunteers, specific to certain technologies, environments or sectors, on a mix and match basis appropriate to cyber emergencies in the civil sector
4. Maintain a comprehensive and current database of the key civil sector cyber defence skills in Australia and overseas
5. Effective monitoring of business and economic threats and rapid response capabilities beyond the enterprise level
6. Nation-wide preparedness for the unlikely but credible threat of a cyber emergency affecting the civil economy or national security interests (including international aspects)
7. Capacity to articulate in a consistent, coherent and authoritative manner the different domains of cyber security (crime, harassment and bullying, espionage, warfare); of the many dimensions of cyber security (technical, human, social and legal); and how different sections of the society must bear differentiated responsibilities
8. Capacity to articulate in a consistent, coherent and authoritative manner the emerging and future threat environment in each of those domains and variegated response options
9. Capacity to develop a comprehensive suite of governmental, cross-sector, private-public, professional and civil society networks active in cyber security
10. Capacity to consistently promote a national consensus on where to draw the line between sovereign capabilities and the global communities of practice (including R&D).

DRAFT 24 June 2016

Enabling Arrangements

1. Corresponding national legislation will be needed to establish the Cyber Civil Corps (CCC) as a new branch of government service in Australia closer to ASIO and ASIS in approach than to the ADF, Border Force or AFP.
2. The legislation will need to break new ground in federal state relations and in national defence arrangements around policing and Commonwealth "aid to the civil power"
3. The leadership of the cyber civil corps will need to be highly expert in the field of managing advanced cyber threats and coordinating responses to them, under Ministerial direction
4. The Director General of the cyber civil corps will report directly to a Minister, possibly the Minister of Communications or a new Minister for Civil Security in Cyber Space, not the Attorney General
5. Beyond training, exercising and educational activities, any operational action by the cyber civil corps will be authorised by the relevant Minister
6. Only the small headquarters of the cyber civil corps would be full-time permanent staff, all other personnel would be sworn officers.

Development Strategy

1. The enabling legislation and associated Cabinet decision would provide for development of the cyber civil corps in several phases over two years:
    a. Appointment of the Director General, possibly from a closely Allied country and not necessarily an Australian national (Day 1)
    b. Establishment by the Director General of the headquarters staff (complete by Day 90)
    c. Development by the Director General and headquarters staff of the operating regulations, staffing plan and initial five-year budget of the cyber civil corps, including through community consultation over one year (complete by Day 365)
    d. The public consultation phase would run in parallel with an inquiry by a special select joint committee of the federal parliament (complete by Day 365, end of Year 1)
    e. Consideration and approval of the plans by the federal Cabinet and its subsequent consideration by the Council of Australian Governments (complete middle of Year 2)
    f. Recruitment of first 100 volunteer civil corps personnel (complete by end of Year 2)

Greg Austin
Australian Centre for Cyber Security
UNSW Canberra