Research Group on
Cyber War
and Peace

AUSTRALIA NEEDS CIVIL DEFENCE AGAINST THE CYBER STORM

Policy Report

Discussion Version 31 March 2019

Executive Summary

The report[1] recommends that Australia move rapidly toward a comprehensive system of cyber civil defence that does not yet exist and which will demand paradigm-changing actions and decisive leadership by key stakeholders. The recommendation is underpinned by research over more than a decade on trends in technology, the observed activity of major powers, and their active planning for wide-ranging attack on civilian infrastructure of military significance in the event of war or hostilities.

In brief, the report canvasses:

1. The need to set up a Cyber Civil Defence Force, with a disciplined structure, led by a senior commander with military combat experience, and staffed mainly by part-time volunteers.
2. Whatever structural solution is identified, the new investment by governments and businesses country-wide required for highly effective cyber civil defence is likely to be of the order of billions of dollars over a decade.
3. Establishment of a provisional National Commission for Cyber Civil Defence led by the private sector, supported by government, and with heavy representation from a wide variety of scholars.
4. Retirement of the current national cyber security strategy of April 2016 in favour of nine separate strategies for the following, quite distinct national needs: cyber civil defence, countering cyber crime, containing cyber terrorism, countering cyber espionage and information warfare, cyber-enabled war, protecting personal privacy and human rights online, enterprise-level cybersecurity, industry policy for the ICT sector, and human capital development for the information age.
5. Commissioning of various inquiries, academic research and parliamentary hearings to identify new pathways to radical institutional reform to prepare the country for cyber civil defence crises.

The report is issued in it current form for discussion purposes. The discussion version is the result of two international workshops held at UNSW Canberra on 18 and 19 February 2019. It reflects other research by at least two of its authors over more than a decade in Australia and overseas. The report begins with some background considerations and information, it analyses policy options in brief, and offers four recommendations for action. Appendix A provides summary material that allows a comparison between Australian approaches and those in the United States.

[1] This report has been prepared for the purposes of discussion by several members of the Research group on Cyber War and Peace and does not necessarily reflect the views of all members of the group. The corresponding author is Professor Greg Austin, coordinator of the research group (G.Austin@unsw.edu.au). Notable contributions have been provided by Dr Gary Waters, Adam Henry and Karine Pontbriand.

Context: Ten Points, Twenty Years

1. On 18 February 2019, the Head of Australia's Information Warfare Division, Maj. Gen. Marcus Thompson, observed that in the event of a significant incident in Australian cyberspace, the resources needed to respond might not exist at the appropriate scale. This judgement concurs with earlier research published by UNSW Canberra and is implicit in several statements by government leaders over the past two years.
2. On 18 February 2019, Prime Minister Scott Morrison revealed that an unknown actor, presumed to be a foreign state, launched a cyber attack against the country's major political parties in its Parliament House.
3. The United Kingdom revealed in 2018 that it has plans to black-out Moscow in the event of a major crisis and exercised that during a military simulation involving kinetic and cyber operations that cost around A$200 million.
4. Russia conducted cyber attacks against the critical power infrastructure of Ukraine in 2016—in "peacetime".
5. China regularly conducts cyber reconnaissance against civil infrastructure of potential adversary countries to support its combat operations in time of war or major crisis, including against power grids.
6. The United States is planning for cyber options in all phases of military operations and at all levels of command, and according to its Law of War Manual (2015) sees it as lawful in wartime to attack targets such as dams and civil nuclear power stations, including through cyber means, if military necessity dictates—"so long as it is conducted in accordance with other applicable rules, including the rules of discrimination and proportionality".
7. The United States launched a debilitating cyber attack on Iranian nuclear enrichment facilities beginning in 2009 and Iran retaliated two and three years later by launching debilitating attacks on U.S. banks and Saudi Aramco—in "peacetime".
8. Attacks on Estonia in 2007 by Russia-based hackers demonstrated the potential for cyber attacks to cripple the economy of a small country (at least temporarily).
9. In 1999, the United States conducted cyber attacks against the electric grid of Yugoslavia, reportedly causing simultaneous blackouts in 70 per cent of the country, through combined kinetic and cyber operations. A NATO spokesman said at the time that the Alliance had its "finger on the light switch in Yugoslavia".
10. For the major powers, the primary aims of cyberspace operations in or just before the outbreak of war would be the strategic decapitation of the adversary's national command and control and/or cyber disruption of deployed forces and civil-military support mechanisms. This could include government communications to sub-national governments and authorities, and civil communications of many sorts (such as control of trains, air traffic control, civil aircraft in flight, and infrastructure in banking, energy and water)—depending on the political character of the conflict.

Background

Since 2015, researchers at the University of New South Wales Canberra have been undertaking consultations in Australia and overseas with stakeholders and specialists on a range of cyber policy issues, ranging from sovereign R&D priorities and cyber security education through to cyber warfare and critical infrastructure protection. These consultations included three research workshops (2015, 2017 and 2019) that saw participation (*inter alia*) from the U.S. Department of Homeland Security, the U.S. Army Cyber Institute, U.S. National Defense University, the

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Australia's Department of Prime Minister and Cabinet, the Defence Science and Technology Group, the Information Warfare Division of the Australian Defence Force, leading universities in the field (Oxford University, University of California Irvine, Tel Aviv University, Melbourne University, QUT and UNSW), a range of private sector thought leaders, and government representatives (United States, United Kingdom, Canada, and New Zealand). The researchers have been steadily expanding their global research networks and partnerships as well as making a significant contribution to knowledge transfer through a unique suite of Master's degrees, demonstrated best by offering the country's only degree in cyber war and peace, an educational program available in few universities in the world. In its five years of existence, UNSW Canberra Cyber has established itself as the leading hub for interdisciplinary cyber security research in Australia.

In February 2019, the third academic workshop in the series referred to above was dedicated to the "cyber storm" and the scholars participating in that are now preparing two volumes of papers arising from that work for academic publication by a globally prominent firm.[2] The academic workshop over one-day was followed by a policy workshop on the more narrow subject of Australia's preparedness for a "cyber storm" event. This workshop, involving some 80 invited participants, took on the task of teasing out policy responses to complex cyber emergencies (the "cyber storm"). This policy report reflects conclusions that its authors regard as the most important for Australia arising from both the Policy Workshop and the Research Workshop, as well as by other research undertaken by the Research Group on Cyber War and Peace at UNSW.

The challenge for the deliberations was articulated by the Australian government in November 2016 when Australia's former Minister of Cyber Security, Hon. Dan Tehran, offered the first official warning that the country needed to prepare for a cyber storm, even if it was an unlikely contingency. Mr Tehan painted a picture of such an event as the cascading consequences of a single vector cyber attack (one virus). The meteorological metaphor was repeated by former Prime Minister Turnbull in 2018 and by Home Affairs Secretary in March 2019. The government has never really spelled out in any detail and in public what precisely the country would need to do to prepare for and fight through such a crisis.

The task has become more urgent in the two and half years since the original Tehan statement. A more recent view of the cyber storm sees it as the contingencies arising from protracted and complex, multi-vector, multi-wave, multi-theatre attacks against cyber assets in a time of war or in a political crisis that may escalate to war.[3] Such assets can include critical civil infrastructure, military C4ISTAR, computerised systems in weapons platforms, and even other civilian targets of military or national significance.

The workshop addressed several questions in separate sessions:

- Who is in charge during a cyber storm? And of what? (according to the law and policy)?
- What does advanced cyber situational awareness for a cyber storm look like?

[2] Provisional titles are "Civil Defence for the Cyber Storm" and "Human Capital for Security in Cyberspace". They will be the first books on these subjects published under the leadership of Australian scholars.

[3] Greg Austin, Civil Defence Gaps under Cyber Blitzkrieg, Discussion Paper, February 2019.

- Trusted communications and information sharing systems between highly secure and unclassified domains
- Directing cyber talent and non-cyber emergency services to triage the worst local impacts. How should key stakeholders respond to these challenges of human capital formation?
- How should Australian military planners prepare for advanced technology threats?

Over the two days, the importance of these subjects was reinforced by the presentations and participation of thought leaders from government, the armed forces, industry and academia. The excellent international participation was another measure of the high relevance of the discussion, as was significant media coverage in Australia of several ideas and material presented. We would like to acknowledge the contribution of session chairs in the Policy Workshop, especially Mr Bryan Cunningham, Executive Director of the Cyber Security Policy and Research Institute at the University of California Irvine; Commander Michael Widman USN, Head of Strategy at the NATO CCDCOE; and Dr Paul Barnes, Head of the Risk and Resilience Program at the Australian Strategic Policy Institute. This report does not imply their endorsement of any part of the content.

This policy report is not a record of the discussions. It addresses top-level conclusions of relevance to Australia that in the opinion of the authors the discussion pointed towards. The report cannot be read as necessarily being endorsed by any of the participants save for the authors.

The report is intended to be non-partisan but it cannot be apolitical. Leaders in government, business and the education sector need to be accountable. The "cyber storm" challenge was first identified at least as early as 2006 by the United States government and since that time successive federal governments in Australia have been consistently slow to act compared with important international partners such as the United States and the United Kingdom. The report does not pretend to analyse the causes for the delay or for the constrained measures taken by these governments. It is clear, fortuitously, that 2016 was a turning point in Australia with the release of the Australian Cyber Security Strategy in April and the Defence White Paper in March of that year. Both documents committed the government to wide-ranging action, and the Federal Opposition offered its support to the measures, without any significant reservations to the policies therein.

Main Conclusions

The discussion over two days of presentations and workshops in February 2019 does not allow any other conclusion than this: Australia is not adequately prepared for a cyber storm. It has not yet made adequate investments in a range of capabilities and human capital that would help the country prepare appropriately. There are several mitigating circumstances: Australia is not alone (no country is well prepared), a cyber storm is a low-likelihood event (so we may appear to have a certain luxury of time), and Australia simply lacks the research base in public policy aspects of complex cyber crises to inform government policy. There is almost zero research available on the economic trade-offs Australian firms and agencies are making by maintaining current levels of investment and readiness for cyber crises.

With those competing considerations in mind (the art of the possible versus the science of the perfect), participants in the workshops nevertheless identified several worrying circumstances that they felt demanded prompt attention. Some of these would be relatively inexpensive or quick to implement, but most would require immense political will, significantly more analysis, and likely large amounts of money that could underpin the necessary paradigm shift. All of them are underpinned by the free choice of Australian students and professionals to invest in their own human capital on a scale that may begin to match the national needs. So far, according to Austcyber's 2018 Sector Competitiveness Plan Update, that transition is still happening too slowly to repair the skills deficit (even as narrowly defined by them) in the short term.

The human capital choices of Australian citizens parallel the human influences affecting the investment choices of government and the private sector. There is little national consensus and almost no structured and sustained debate on what a cyber storm might be, despite Prime Ministerial and Ministerial invocations of the threat beginning two and a half years ago. Senior leaders in Australian security policy have identified this as a major gap in the country's preparedness.

Questions that need to be resolved according to workshop participants included:

- What precisely are the responsibilities of the three different layers of government in Australia (federal, state, and local) in cyber civil defence and what will they not defend?
- What is the role of the ADF in defence of the "homeland" in cyberspace, a question complicated by the fact that key Australian information assets are outside the territory of Australia?
- How do the Australian government agencies and security forces defend civilian infrastructure in the absence of a civil defence organisation?
- How should Australia better respond to aggressive and malicious activity in cyberspace that targets civil assets but which falls short of the legal definition of armed attack?
- How do we elevate the awareness and education of the Australian population as 'combatants', albeit unwitting ones, in cyberspace?
- What is the best model from international experience for effective high intensity collaboration across government, industry and citizens in the event of a national cyber crisis?
- How do we build a full-spectrum capability across information operations, cyberspace operations and electronic warfare (including through the fusion of technology and social or political consideration)?
- How do we define and maintain sovereignty in a globalised cyberspace?
- How do we achieve information advantage through advanced technologies, like artificial intelligence, machine learning and behavioural analytics?
- How will technological, political and doctrinal changes in the coming decades affect any of the above?

In several respects, Australia is already in a cyber storm while major powers are actively planning much more intense and wide-ranging attacks, perhaps a form of cyber blitzkrieg,[4] in the event of war. The following section contains some recommended responses to begin to prepare for civil defence in such circumstances.

[4] See footnote 3.

Future Policy Directions

Separate Strategies, New Institutions

The current approach in many countries of having an omnibus national cyber security strategy seems to have been overtaken by events. They are no longer fit for purpose because they blur massive differences between important areas of policy. The judgement is well captured by the simple observation that "cyber security is not cyber war", but it is a judgement that is also strongly supported by research. It seems inevitable that Australia will need separate national level strategies to individually address nine distinct policy sets: personal privacy, enterprise-level cyber security, cyber crime, cyber-enabled terrorism, cyber espionage, cyber-enabled warfare, industry policy for the ICT sector (including export/import policy), human capital for the information age (including security aspects)—and cyber civil defence. This is a vast agenda much of which is not currently well-serviced by existing Australian institutions in government, business or academia.

It is the tragedy of cyber space affairs in Australia and globally that when the subjects are addressed by omnibus agencies or departments (such as Home Affairs at the national level or by the Department of Premier and Cabinet at state level), non-cyber agendas win out in the fight for political attention. There is no strong voting power behind these issues—and little solid economic evidence to justify escalating investment decisions beyond the clamour for "more", reminiscent of Oliver Twist.

> **Recommendation 1**: (a) Australian scholars, supported by industry and government, should develop a feasibility study for a comprehensive cyber civil defence program at national, state and local levels that brings together key stakeholders. Such a study should be developed in a twelve-month period, possibly under the auspices of the Australian Council of Learned Academies. The study should include lawyers, economists, business studies specialists, security strategists, international relations specialists, as well as technical experts—all Australian citizens. The level of funding for such a study should not be less than $3 million and should probably be closer to $5 million. (b) The study should include a review of possible new education strategies and institutions, such as a Federal Department of Information Transformation or National Cyber Civil Defence College, with costings, to stimulate rapid growth of the Australian work force with high-level specialist skills. (c) The report should reflect research on new legal regimes for cyber civil defence because existing legislative authorities fall far short of what most observers regard as appropriate. (d) In undertaking consultations for the report, scholars along with business and government leaders, and privacy advocates, should set up a provisional National Commission for Cyber Civil Defence led by the private sector, supported by government, and with heavy representation from a wide variety of scholars. The logic behind the leadership of the private sector is that civil defence activities always fall heaviest on private actors.
>
> **Recommendation 2**: (a) In parallel with the work recommended above, federal and state governments, as well as municipal authorities in larger cities, and senior executives in critical sectors should develop a national cyber incident response plan that is far more detailed than anything in existence in Australia[5] and that could be based on

[5] In December 2018, the Council of Australian governments agreed to a seven-page brochure setting out very broad arrangements, applicable only to governments, for coordination in responding to a national cyber incident that did NOT reach the threshold of a national crisis. The document noted that operational plans for national

the unclassified U.S. model. The virtue of the U.S. plan is that it identifies the many capabilities that need to be in place for cyber civil defence in a national level crisis. See Appendix A for a summary of the plan. (b) The time frame for development of the national cyber incident response plan for crisis situations should be two years so that it can take full account of the major study led by scholars that is recommended above for completion in one year. (c) The response plan should take account of: information warfare activities that might be conducted in or through cyberspace; the dynamics of offence and defence in a major cyber conflict and how that will affect civil sector assets; strategies for dealing with foreign-owned critical infrastructure (such as in the power grid or telecoms sectors); and strategies of dealing with the globalised suite of assets and expertise that many Australian agencies and enterprises currently depend on. (d) This work should not be owned by any single agency or department at the federal level, and should be led by a highly qualified person under commission from the Governor General with the powers of investigation of a Royal Commissioner. The cost of such an undertaking would need to be in the tens of millions of dollars.

Recommendation 3: (a) The Parliament's Joint Committee on Intelligence and Security should consider undertaking a year-long inquiry to parallel the work suggested in Recommendations 1 and 2, without interfering with the remit of either line of work but rather directed at questions of community impacts of such arrangements and matters. (b) The Senate Committee on Constitutional and Legal and Constitutional Affairs should consider undertaking a year-long inquiry to parallel the work suggested in Recommendations 1 and 2, without interfering with the remit of either line of work but rather directed at questions of protecting the rights and interests of the private sector and citizens as the governments develop their approach.

New Infrastructure for Cyber Civil Defence: communications, situational awareness, and exercises

Australia does not have a secure multi-dimensional and intelligent communications network in place that can deliver advanced cyber situational awareness simultaneously to key actors and stakeholders across the country in the event of a national cyber crisis. Such a capability relies on defining the capabilities needed, the tasks, and designated people, roles, assets and funding. Australia does not yet have a capability for advanced country-wide exercises appropriate for a national cyber crisis or even a national cyber incident. The Australian government indicated in December 2018 that this would be an important area for future work between it and state and territory governments for a national cyber incident.

The larger share of this set of problems has been on the national agenda since 2010 when the National Security Advisor to the Prime Minister, Duncan Lewis, put forward the "National Security Information Environment Roadmap: 2020 Vision". Recognising that the milestones would be radical but achievable with the right leadership, the plan foreshadowed by 2020:

- A harmonised policy and legislative environment that supports the smooth flow of people, ideas and activities across boundaries;

cyber incident response sill needed to be developed. For further information, see https://cyber.gov.au/government/news/cima/cima_2018_A4.pdf.

- The ability of all members of the national security community to access and share information and cooperate from their desktop with their partners across government, industry and international counterparts;
- Access to secure desktop video teleconferencing and secure mobile communications;
- Real time collaboration and coordination across the entire national security community via increasingly standardised tools and applications;
- An interoperable, secure and reliable information and communications technology among and between all classification levels;
- A single computer screen and keyboard per desktop so users can switch between classification domains with ease;
- Nationally consistent interoperability standards, supported by mutual recognition of personal security clearances, consistent identity management and access controls, and a single security classification nomenclature; and
- Focused ICT investment that is aligned with the priorities of Government, represents best value for money, and enhances interoperability domestically and internationally.

In the decade since, while we can see a more harmonised policy and legislative environment, we do not see the necessary technical capabilities foreshadowed by Lewis. It would appear to be vital for the federal government to update the 2010 roadmap for the "national information environment roadmap" ensuring that it addresses resilience during and after a cyber crisis.

It would probably be a mistake to imagine that ASD or the ACSC should provide the networks needed let alone deliver the political leadership needed for such a transition. It may be logical for ACSC to be the main hub but that should not be assumed as a given since civil defence operations in a crisis (as opposed to a "national cyber incident") are not currently part of the ACSC mission set. Citizens and businesses across the country are stakeholders in cyber civil defence. While governments set policies and regulations, the private sector (partly foreign-owned) designs, delivers and operates the capabilities. And civil defence by definition is something that falls primarily to citizens or private actors to execute—acting only in loose but effective coordination with government. We need to build trust among these actors, including with foreign corporate owners, and a common purpose for this to work. Some industry sectors and government departments have strong cyber response plans in place but only a handful would be adequate in a national cyber crisis. We need to capture and build on these at a joined up national level through a national command centre with authorities like those of the Chief of the Defence Force or the Chief of Border Force. ACSC can do this up to a point but it does not extend across all critical infrastructures nor does it have any command authority.

An essential element of a national cyber awareness capability is a system of "indicators and warnings" that is agreed nationally and which underpins not only threat analysis but which also exposes pathways for action to maximise resilience. Such indicators exist throughout the information environment in Australia and beyond, but Australia needs to improve its ability to recognise and interpret these; and it needs to be a whole-of-country effort. A cyber civil defence system is dominated by the periphery, not the hub, and this is especially the case with the development of indicators and warnings.

Most specialists in this field of policy would agree that these needs exist. One challenge is to find the appropriate institutional framework for advancing them in a timely fashion. There are three broad options: first, continue to build-out the capability of ACSC and its Critical Infrastructure Centre but with a radically increased pace and a transformed remit; second, work through the Council of Australian Governments to get relevant actors lined up and in agreement on the authorities need to monitor threats and respond defensively; or third, dig into quite recent Australian history to resurface the legislated civil defence roles of the state emergency services and to dig even deeper into our history to resurface the concept of Australian militia forces.[6]

What would a cyber civil defence force (militia) do?

1. 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. Provide an auxiliary capability in a disciplined command structure [separate from Border Force] for national civil and military defence response to extreme cyber emergencies.
3. Develop, monitor and manage a response system for handling cyber threats to critical national, state and local infrastructure.
4. Develop, monitor and manage a national response system for handling serious cyber crime that may affect the national economy or social infrastructure.

A cyber civil defence force would provide globally significant ancillary functions: it would support Australia's deterrence of extreme cyber attack; and it would provide leadership in national cyberspace education for businesses and the community that would have important ripple effects in our region and with traditional Allies (New Zealand, United States, United Kingdom and Canada).

Assumptions underpinning the choice for such a force as the best option are these:

- The cascading consequences of extreme cyber emergencies will be felt more outside cyberspace than in it, and so the response must be addressed by organised security agencies that can straddle both cyber knowledge and community resilience.
- Current arrangements for national critical infrastructure protection in cyberspace, including for essential services, are weakly developed, with the federal government taking active and direct responsibility only for governmental infrastructure through the ACSC.
- National policy recognises that such protection is a shared responsibility but there is no mechanism in place (beyond reporting obligations) 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.
- Australia will never be able to afford the cost of maintaining such capabilities in full-time roles in existing military and police forces. (Even if Australia could afford it, extreme cyber emergencies in the civil sector in cyberspace are of such low probability that a full-time standing response force cannot be justified.)

[6] The word "militia" is often identified in modern mass media with countries experiencing civil strife but in many stable democracies, including Australia, it is not only politically neutral but a cherished part of their historical fabric. In 1943, Australia's Citizen Military Force, referred to as the militia, were among the units sent to New Guinea to resist the Japanese forces. On 15 November 1939, just after the outbreak of the war, Prime Minister Menzies spoke of the forces: "we have decided to keep our Militia Forces at an adequately trained strength of not less than 75,000 men, and for this purpose compulsory military training will be reintroduced in January next. … there is, I 'believe, a growing recognition of the fact that military training for the defence of Australia should be a normal part of our civic life, and that if it is to be just and democratic, it should be made compulsory." The text is cited not to support the notion of compulsory militia service but to underscore the central place in Australia's history of civil defence premised on a militia force.

- The pipeline for supply of skilled personnel for entry into military and police forces is not adequate for the civil defence purpose.
- Existing priorities and mission orientation of the Australian Defence Force (ADF) and national and state police forces, including the necessary transitions for likely future operations in cyberspace, are already so burdensome it may not be prudent to place national civil defence in their hands.
- The contours of future high technology threats to Australia in cyberspace 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.
- 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.
- A lower level option, such as a “neighbourhood watch” for cyber space (a set of information sharing centres) would not address emerging circumstances appropriately as they would lack legal response authorities and response capability and would likely be devoid of a formal command structure.

The capabilities that a cyber civil defence force would deliver include:

- A highly secure and globally networked command, monitoring and operations centre independent of (but linked to) the ASD and ACSC.
- Advanced knowledge of cyber dependencies in Australia’s civil economy and essential services.
- 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 highly variable cyber emergencies in the civil sector.
- Maintain a comprehensive and current database of the key civil sector cyber defence skills in Australia and overseas for emergency access.
- Capacity to develop a comprehensive suite of governmental, cross-sector, private-public, professional and civil society networks active in cyber security
- Effective monitoring of business and economic threats and rapid response capabilities beyond the enterprise level but below the national security level.
- Nation-wide preparedness for the unlikely but credible threat of a cyber emergency affecting the civil economy or national security interests (including international aspects).
- 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. (Cyber security awareness programs do not match this high-level threat.)
- 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
- Capacity to consistently promote a national consensus on where to draw the line between sovereign capabilities and the global communities of practice (including for R&D).

To achieve such capabilities country-wide, the investment required may be of the order of billions of dollars, rather than millions. There are large scale requirements for new physical networks, supporting equipment, human capital, and dedicated secure buildings.

> **Recommendation 4**: Stakeholders in the private sector and state and local governments, including state emergency services, should open a national debate on Australia's emergency response management for extreme cyber emergencies with a view to deciding in a short period of time on new disciplined structures for management of such crises that go well beyond existing structures and begin to approach a Cyber Civil Defence Force.

APPENDIX A: CYBER INCIDENT RESPONSE PLAN CAPABILITIES AND TASKS

This is a summary of key points, including verbatim material, of a policy document from the U.S. Department of Homeland Security, 'National Cyber Incident Response Plan' (NCIRP), from December 2016.[7] Australia has no direct equivalent in the public domain beyond a short seven page brochure on intergovernmental coordination in the event of a national cyber incident that is not regarded as a national crisis. The U.S. policy covers both types of event. This summary reveals the breadth and depth of the cyber civil defence planning, and the scale and type of associated capabilities development, that Australia's major ally is undertaking. The purpose of including this summary as an attachment to the Policy Report is not to suggest that Australia emulate the U.S. policy in its entirety, but rather to inform discussion on which parts of it we can and should emulate, and what we might do differently. The section on capabilities development needed for comprehensive cyber civil defence helps illuminate how weakly developed Australia's capabilities are and identifies useful directions for early policy action.

Introduction

Networked technologies touch every corner of the globe and every facet of human life. They have driven innovation, nurtured freedoms, and spurred economic prosperity. Even so, the very technologies that enable these benefits offer new opportunities for malicious and unwanted cyber activities. The US has recognised that the frequency of cyber incidents is increasing, and the most significant of these incidents, those likely to result in demonstrable harm to the national security interests, foreign relations, or domestic economy or to the public confidence, civil liberties, or public health and safety of the nation's people, necessitate deliberative planning, coordination, and exercising of response activities, in order to minimise the threat and consequences to the nation, infrastructure, and way of life.

The National Cyber Incident Response Plan (NCIRP) articulates the roles and responsibilities, capabilities, and coordinating structures that support how the nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure. The NCIRP is not a tactical or operational plan; rather, it serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations.

The concurrent lines of effort are threat response, asset response, intelligence support, and the affected entity, which undertakes efforts to manage the effects of the incident on its operations, customers, and workforce. The NCIRP builds upon these lines of effort to illustrate a national commitment to strengthening the security and resilience of networked technologies and infrastructure.

Guiding Principles

The NCIRP's guiding principles are:

- *Shared Responsibility*. Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

[7] The document and an overview of where it sits in U.S. public policy architecture can be found at this website: https://www.us-cert.gov/ncirp.

- *Risk-Based Response*. The Federal Government will determine its response actions and the resources it brings to bear based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, privacy and civil liberties, or the public health and safety of the nation's people. Critical infrastructure entities also conduct risk-based response calculations during cyber incidents to ensure the most effective and efficient utilisation of resources and capabilities.
- *Respecting Affected Entities*. To the extent permitted under law, Federal Government responders will safeguard details of the incident, as well as privacy, civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event of a significant cyber incident where the Federal Government interest is served by issuing a public statement concerning an incident, federal responders will coordinate their approach with the affected entities to the extent possible.
- *Unity of Governmental Effort*. Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These entities must coordinate efforts to achieve optimal results. The first federal agency to become aware of a cyber incident will rapidly notify other relevant federal agencies to facilitate a unified federal response and ensure that the right combination of agencies responds to a particular incident. When responding to a cyber incident in the private sector, unity of effort synchronises the overall federal response, which prevents gaps in service and duplicative efforts. The transnational nature of the Internet and communications infrastructure requires the nation to coordinate with international partners, as appropriate, in managing cyber incidents.
- *Enabling Restoration and Recovery*. Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible.

Core Capabilities

Core capabilities are the distinct critical elements needed to conduct the threat response, asset response, and intelligence support activities in response to a cyber incident. Core capabilities are the activities that generally must be accomplished in cyber incident response, regardless of which levels of government are involved. They provide a common vocabulary to describe the significant functions that must be developed and executed across the whole-of-Nation to ensure preparedness.

Access Control and Identity Verification: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems, which is also referred to as Authentication and Authorisation. This capability relies on the implementation and maintenance of protocols to verify identity and authorize, grant, or deny access to specific IT systems and networks.

Cybersecurity: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorised use, and exploitation. More commonly referred to as information security, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.

Forensics and Attribution: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident. ***Forensics*** is the term for discovering and identifying information relevant to an investigation through both scientific and intelligence-based acumen. In the context of a cyber incident, forensics refers to several technical disciplines related to the duplication, extraction, and analysis of data to uncover artefacts relevant to identifying malicious cyber activity. Forensics includes several sub-disciplines, including host-based forensics, network and packet data forensics, memory analysis, data correlation, and malware analysis. During the response to a significant cyber incident, government agencies and private sector partners frequently conduct simultaneous analysis and share analytical results with each other to create a common understanding regarding the malicious cyber activity and how to defend against these or similar activity. In the days following an incident, several different threats, asset, and business response organizations may also engage in simultaneous forensic analysis. Although these lines of effort may appear to be duplicative, findings from these efforts could vary depending on the entities' varied access to particularised datasets or holdings. ***Attribution*** identifies an adversary linked to a particular incident. It is the culmination of the review of evidence and intelligence gathered during an incident which results in an assessment that identifies individuals or organisations which likely played a role in the cyber incident. Attribution occurs over the lifecycle of an investigation and may not be known at the onset of a cyber incident response. Although the development of attribution for a significant cyber incident is one of the primary functions of lead federal response agencies, other government and private sector entities have a significant role to play in determining attribution. An assessment regarding attribution for an incident is not only important for government agencies conducting criminal or national security investigations; it could also be significant to an affected entity as it considers whether to pursue additional legal or civil action against threat actors. This core capability also includes unique and technical activities that support computer network and asset analysis during an incident. These supporting activities contribute to awareness of a comprehensive picture, which ultimately helps reduce the impact of a current incident and prevent future cyber incidents from spreading across the network.

Infrastructure Systems: Stabilise critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity. Critical infrastructure and cyber networks are interdependent. In a response to a cyber incident, this capability focuses on stabilising the infrastructure assets and entities, repairing damaged assets, regaining control of remote assets, and assessing potential risks to the critical infrastructure sector at large.

Intelligence and Information Sharing: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the nation, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary. In the context of a cyber incident, this capability involves the effective implementation of the intelligence cycle and other information collection and sharing processes by federal and state/territory entities, the private sector, and international partners to develop situational awareness of potential cyber threats to the nation.

Interdiction and Disruption: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity. In the context of a cyber incident, these threats include people, software, hardware, or activities that pose a threat to the nation's cyber networks and infrastructure. This includes those interdiction and disruption activities that may be undertaken in response to specific, actionable intelligence of a cyber threat. Interdiction and disruption may include the targeting of persons, programs, or equipment or machines to stop or thwart threat activities and employing technical and other means to prevent malicious cyber activities. Interdiction and disruption capabilities help thwart emerging or developing cyber threats and neutralise operations. These capabilities should be utilised in a manner that preserves evidence and the Government's ability to prosecute those who violate the law.

Logistics and Supply Chain Management: Facilitate and assist with delivery of essential commodities, equipment, and services in support of responses to systems and networks impacted by malicious cyber activity. Synchronise logistics capabilities and enable the restoration of impacted supply chains. In the context of a cyber incident, this capability focuses on providing the logistical or operational support to achieve cyber incident response priorities established by leadership through identifying, prioritising, and coordinating immediate response resource requirements.

Operational Communications: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders. In the context of a cyber incident, this capability includes identifying federal support organisations, capabilities, and teams with internal interoperable voice, video, and data systems and networks essential for effective cyber incident response operations. In a cyber incident, this capability focuses on the timely, dynamic, and reliable movement and processing of incident information in a form that meets the needs of decision makers at all levels of government and authorised participating private sector partner organisations.

Operational Coordination: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities. This is the capability to conduct actions and activities that enable decision makers across the whole-of-nation to determine appropriate courses of action and to provide oversight for complex operations, to achieve unity of effort and effective outcomes. It coordinates the threat response, asset response, and intelligence support activities in the face of a cyber threat or in response to an act of terrorism committed in the homeland. Unity of message is included within the guiding principles. In the context of a cyber incident, this core capability includes efforts to coordinate activities across and among all levels of government and with private sector partners. This capability involves national operations centres, as well as on-scene response activities that manage and contribute to multi-agency efforts.

Planning: Conduct a systematic process engaging the whole-of-nation, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives. In the context of a cyber incident, planning includes both deliberate planning and incident action planning. Deliberate planning involves developing strategic, operational, and tactical plans to prevent, protect against, mitigate the effects of, respond to, and recover from a cyber incident. Incident action planning occurs in a time-constrained environment to develop or rapidly adapt operational and tactical plans in response to an imminent or ongoing cyber incident.

Public Information and Warning: Deliver coordinated, prompt, reliable, and actionable information to the whole-of-nation and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threats or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate. In the context of a significant cyber incident, this capability uses effective and accessible indications and warning systems to communicate significant cyber threats to involved or potentially involved operators, security officials, and the public (including alerts, detection capabilities, and other necessary and appropriate assets).

Screening, Search, and Detection: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence. In the context of a cyber incident, this capability includes the measures which may be taken in response to actionable intelligence that indicates potential targets or types of malicious cyber activity, or the threat actors planning such activity. Measures may also be taken to verify or characterise a cyber threat that has already been located. Screening relative to a cyber incident may include monitoring the status of the network, assets, sensors, and other technologies that provide information on the security posture that may determine further action as necessary.

Situational Assessment: Provide all decision makers with timely, decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response. In the context of a cyber incident, this capability focuses on rapidly processing and communicating large quantities of information from across the broader community, from the field level to the national level, to provide all decision makers with the most current and accurate information possible.

Threats and Hazards Identification: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude of those threats; and incorporate this into analysis and planning processes to clearly understand the needs of an entity. In the context of a cyber incident, this capability involves the continual process of collecting timely and accurate data on cyber threats, including accounting for the future impacts of technology advancements, to meet the needs of analysts and decision makers. Effective Threats and Hazards Identification for a cyber incident is supported by standardised data sets, platforms, methodologies, terminologies, metrics, and reporting to unify levels of effort across all layers of government and the private sector, reducing redundancies.

Critical Tasks

The NCIRP (Annex F) details the core capabilities described above, and the critical tasks needed to achieve them. The Annex is repeated below (with wording modified to suit an Australian audience).

Access Control and Identity Verification

Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems. Also referred to as Authentication and Authorisation.

Critical Tasks:

- Verify identity to authorise, grant, or deny access to cyber assets, networks, applications, and systems that could be exploited to do harm.
- Control and limit access to critical locations and systems to authorised individuals carrying out legitimate activities.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform audit activities to verify and validate security mechanisms are performing as intended.
- Conduct training to ensure staff-wide adherence to access control authorisations.

Cybersecurity

Description: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorised use, and exploitation. More commonly referred to as computer network defence, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.

Critical Tasks:

- Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited.
- Secure, to the extent possible, public and private networks and critical infrastructure (e.g., communication, financial, electricity sub-sector, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities.
- Create resilient cyber systems that allow for the uninterrupted continuation of essential functions.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Forensics and Attribution

Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.

Critical Tasks:

- Retrieve digital media and data network security and activity logs.
- Conduct digital evidence analysis, and respecting chain of custody rules.
- Conduct physical evidence collections, analysis adhere to rules of evidence collection as necessary.
- Assess capabilities of likely threat actors(s).
- Leverage the work of incident responders and technical attribution assets to identify malicious cyber actor(s).

- Interview witnesses, potential associates, and/or perpetrators if possible.
- Apply confidence levels to attribution assignments.
- Include suitable inclusion and limitation information for sharing products in attribution elements guidance.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform audit activities to verify and validate security mechanisms are performed as intended.

Infrastructure Systems

Description: Stabilise critical infrastructure functions, minimise health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.

Critical Tasks:

- Maintain a comprehensive understanding of the needs for the safe operation of control systems.
- Stabilise and regain control of infrastructure.
- Increase network isolation to reduce the risk of a malicious cyber activity propagating more widely across the enterprise or among interconnected entities.
- Stabilise infrastructure within those entities that may be affected by cascading effects of the cyber incident.
- Facilitate the restoration and sustainment of essential services (public and private) to maintain community functionality.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Maintain up-to-date data knowledge of applicable emerging and existing security research, development, and solutions.

Intelligence and Information Sharing

Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the nation, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.

Critical Tasks:

- Monitor, analyse, and assess the positive and negative impacts of changes in the operating environment as it pertains to cyber vulnerabilities and threats.
- Share analysis results through participation in the routine exchange of security information— including threat assessments, alerts, threat indications and warnings, and advisories—among partners.
- Confirm intelligence and information sharing requirements for cybersecurity stakeholders.

- Develop or identify and provide access to mechanisms and procedures for confidential intelligence and information sharing between the private sector and government cybersecurity partners.
- Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include critical infrastructure participants and partners with roles in physical response efforts.
- Share actionable cyber threat information with state and territory and international governments and private sectors to promote shared situational awareness.
- Enable collaboration via online networks that are accessible to all participants.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

Interdiction and Disruption

Description: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity.

Critical Tasks:

- Deter malicious cyber activity within the nation, its territories, and abroad.
- Interdict persons associated with a potential cyber threat or act.
- Deploy assets to interdict, deter, or disrupt cyber threats from reaching potential target(s).
- Leverage law enforcement and intelligence assets to identify, track, investigate, and disrupt malicious actors threatening the security of the nation's public and private information systems.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Logistics and Supply Chain Management

Description: Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronise logistics capabilities and enable the restoration of impacted supply chains.

Critical Tasks:

- Identify and catalogue resources needed for response, prior to mobilisation.
- Mobilise and deliver governmental, non-governmental, and private sector resources to stabilise the incident and integrate response and recovery efforts, to include moving and delivering resources and services to meet the needs of those impacted by a cyber incident.
- Facilitate and assist delivery of critical infrastructure components to rapid response and restoration of cyber systems.
- Enhance public and private resource and services support for impacted critical infrastructure entities.

- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Apply supply chain assurance principles and knowledge within all critical tasks identified above.

Operational Communications

Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.

Critical Tasks:

- Ensure the capacity to communicate with both the cyber incident response community and the affected entity.
- Establish interoperable and redundant voice, data, and broader communications pathways between state and territory entities, particularly state fusion centres, federal, and private sector cyber incident responders.
- Facilitate establishment of quickly formed ad hoc voice and data networks on a local and regional basis so critical infrastructure entities can coordinate activities even if Internet services fail.
- Coordinate with any entity established to manage physical (or non-cyber) effects of an incident. Ensure availability of appropriate secure distributed and scalable incident response communication capabilities including out-of-band communications mechanisms where traditional communications and/or systems are compromised. Adhere to appropriate mechanisms for safeguarding sensitive and classified information private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information.
- Protect individual privacy, civil rights, and civil liberties.
- Cyber threat information also is conducted through automated indicator sharing using established formats (such as the US Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII).
- Perform red team activities to verify and validate that forensics and attribution capabilities are performing as intended and have adequate visibility.

Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities.

Critical Tasks:

- Mobilise all critical resources and establish coordination structures as needed throughout the duration of an incident.
- Define and communicate clear roles and responsibilities relative to courses of action.
- Prioritise and synchronise actions to ensure unity of effort.
- Ensure clear lines and modes of communication between entities, both horizontally and vertically.
- Ensure appropriate private sector participation in operational coordination throughout the cyber incident response cycle.

- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform table-top activities to verify and validate effective and appropriate coordination between stakeholders.

Planning

Description: Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

Critical Tasks:

- Initiate a flexible planning process that builds on existing plans.
- Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities.
- Establish partnerships that coordinate information sharing between partners to restore critical infrastructure within single and across multiple jurisdictions and sectors.
- Inform risk management response priorities with critical infrastructure interdependency analysis.
- Identify and prioritise critical infrastructure and determine risk management priorities.
- Conduct cyber vulnerability assessments, perform vulnerability and consequence analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private and non-profit sectors and local, regional/metropolitan, state, territorial and federal organisations and agencies.
- Develop operational, business/service impact analysis, incident action, and incident support plans at the federal level and in the states and territories that adequately identify critical objectives based on the planning requirements; provide a complete and integrated picture of the escalation and de-escalation sequence and scope of the tasks to achieve the objectives; and are implementable within the time frame contemplated in the plan using available resources.
- Formalise partnerships such as memorandums of understanding or pre-negotiated contracts with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner.
- Formalise partnerships between communities and disciplines responsible for cybersecurity and for physical systems dependent on cybersecurity. Formalise relationships such as memorandums of understanding or pre-negotiated contracts between information communications technology and information system vendors and their customers for ongoing product cyber security, business planning, and transition to response and recovery when necessary.
- Formalise partnerships with government and private sector entities for data and threat intelligence sharing, prior to, during, and after an incident.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

Public Information and Warning

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole community and the public, as appropriate, using clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.

Critical Tasks:

- Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, faith-based organisations, non-governmental organisations, and the public.
- Share actionable information and provide situational awareness with the public, private, and non-profit sectors, and among all levels of government.
- Leverage all appropriate communication means, such as public alert and warning systems, public media, and social media sites.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect applicable information sharing and privacy protections.
- Assure availability of redundant options to achieve critical public information, threat indication, and warning outcomes.

Screening, Search, and Detection

Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.

Critical Tasks:

- Locate persons and networks associated with cyber threats.
- Develop relationships and further engage with critical infrastructure participants (private industry and state and territory partners).
- Conduct physical and electronic searches as authorised by law.
- Collect and analyse information provided.
- Detect and analyse malicious cyber activity and support mitigation activities.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Situational Assessment

Description: Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.

Critical Tasks:

- Coordinate the production and dissemination of modelling and effects analysis to inform immediate cyber incident response actions.
- Maintain standard reporting templates, information management systems, essential elements of information, and critical information requirements.

- Develop a common operational picture for relevant incident information shared by more than one organisation.
- Coordinate the structured collection and intake of information from multiple sources for inclusion into the assessment processes.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

Threats and Hazards Identification

Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes to clearly understand the needs of an entity.

Critical Tasks:

- Identify data requirements across stakeholders.
- Develop and/or gather required data in a timely and efficient manner to accurately identify cyber threats.
- Ensure that the right people receive the right data at the right time.
- Translate data into meaningful and actionable information through appropriate analysis and collection tools to aid in preparing the public.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Discover, evaluate and resolve gaps in policy, facilitate or enable technologies, partnerships, and procedures which are barriers to effective threat, vulnerability, and hazard identification for the sectors.