PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

PARLIAMENTARY LIBRARY
INFORMATION ANALYSIS ADVICE
QUICK GUIDE

RESEARCH PAPER SERIES, 2018–19 1 APRIL 2019

Cybersecurity, cybercrime and cybersafety: a quick guide to key internet links

Produced by members of the Parliamentary Library's Cyber and Digital Research Group
Cat Barker, Monica Biddington, Nicole Brangwin, Helen Portillo-Castro and Tyson Wils

Background

This Quick Guide provides some brief background information on national measures to build cybersecurity and cybersafety and combat cybercrime, and includes links to relevant websites.

Cybersecurity

Development of Australia's cybersecurity framework

Vulnerabilities in online environments are discovered every day. Cybersecurity involves preventing the technical exploitation of such vulnerabilities and mitigating the risk of such exploits occurring. The extent of the cyber threat is vast, traversing many jurisdictions (domestically and internationally), and stems from a myriad of sources. As such, it is not just a technical ICT (information, communication and technology) issue.

According to the Government's Australian Cyber Security Centre (ACSC), some of the threats to Australia's cybersecurity include cyber espionage that gathers intelligence in support of state-sponsored activities; cyber attacks that aim to destroy critical infrastructure; and criminals using online environments to defraud, or steal individual identities.

As a government policy issue, concerns about Australia's cyber resilience were initially raised in the Howard Government's 2000 Defence White Paper, *Defence 2000: Our Future Defence Force*. A number of initiatives flowed from this policy, including cooperation among key national security agencies to assess and deal with emerging threats. In the 2009 Defence White Paper, *Defending Australia in the Asia Pacific Century: Force 2030*, the Rudd Government elevated investment in cyber capabilities to a national security priority, and in 2010, established the Cyber Security Operations Centre (CSOC) within the Defence Signals Directorate (now the Australian Signals Directorate—ASD).

In September 2011, the Gillard Government announced the development of a cyber white paper, which was meant to address a broad range of cyber issues including safety, crime, consumer protection, as well as broader issues such as national security and defence. However, the concept of a cyber white paper lost its impetus and eventually morphed into an overarching update of the *National Digital Economy Strategy*, which was released in June 2013.

ISSN 2203-5249

In January 2013, prior to the strategy's release, the CSOC had evolved into the ACSC as 'the hub of the government's cyber security efforts' and in May the *Defence White Paper 2013* was released, which highlighted cybersecurity as an 'important national capability'.

Following the 2013 election, cybersecurity was not part of the Abbott Government's public focus on national security issues until the cybersecurity review was announced in November 2014. The review was originally intended to take six months but it was 17 months later, under the Turnbull Government, when Australia's new cybersecurity strategy was announced—effectively replacing the 2009 *Cyber Security Strategy*.

While the Turnbull Government's *Cyber Security Strategy* (released in April 2016) recognised that cybersecurity is a strategic issue for Australia's economy and national security, there was less emphasis placed on national security than in 2009 when cybersecurity was considered 'one of Australia's top tier national security priorities'. However, the Turnbull Government's *2016 Defence White Paper* (released in February) acknowledged the importance of cybersecurity in that cyber attacks directly threaten the Australian Defence Force's (ADF) warfighting ability.

Under the 2016 *Cyber Security Strategy*, the Turnbull Government established the positions of Australian Ambassador for Cyber Affairs (Tobias Feakin), Special Advisor to the Prime Minister on Cyber Security (Alastair MacGibbon—now Deputy Secretary National Cyber Security Adviser under the Home Affairs portfolio and Head, ACSC) and Minister Assisting the Prime Minister on Cyber Security (originally Dan Tehan, then Angus Taylor as the Minister for Law Enforcement and Cyber Security). The latter position has since been subsumed by the Minister for Home Affairs, Peter Dutton, under the Morrison Government.

In the defence environment, debate continues to surround the exact nature of cyberwarfare as a sole undertaking. The *2016 Defence White Paper* highlights the 'complex non-geographic threats' in cyberspace and space, and how military capabilities can be adversely affected. The Australia – United States alliance also acknowledged the seriousness of these threats during ministerial talks in 2011 (AUSMIN) where it was agreed that the ANZUS Treaty could be invoked in response to a cyber attack. Cybersecurity has featured in each AUSMIN discussion since.

The threshold for an armed response to a cyber attack is not entirely clear nor is it publicly discussed by Australian or US officials. The Trump Administration declared in its September 2018 *National Cyber Strategy* that 'all instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States', including military force. The Australian Strategic Policy Institute (ASPI), however, suggests that offensive cyber operations are being deliberately conducted 'below the threshold of armed attack' because 'no cyber operation thus far has been classified as an armed attack', which might prompt an overt military response.

Key internet links

National—government

- **Australian Signals Directorate** (ASD)—an independent statutory agency within the Defence portfolio, ASD is Australia's signals intelligence and information security agency and provides services to the ADF and the Australian Government. On 30 January 2018 the Defence Signals-Intelligence (SIGINT) and Cyber Command was established within ASD as the military component. ASD is also home to the ACSC.
- **Australian Cyber Security Centre** (ACSC)—established in November 2014 and formally part of ASD since July 2018, the ACSC incorporates cyber expertise from the Defence Intelligence Organisation, Australian Security Intelligence Organisation, Australian Federal Police and the Australian Criminal Intelligence Commission. The ACSC maintains the Australian Government

Information Security Manual (ISM) that contains advice to businesses, industry and government about best-practice cybersecurity measures. The ACSC also maintains cyber.gov.au, which is designed to be a 'central hub for cyber security information, advice and assistance to all Australians'. This resource includes ACSC updates and reports on cyber threats targeting Australia (see the 2015, 2016 and 2017 threat reports).

- **Critical Infrastructure Centre**—assists owners and operators of critical infrastructure facilities to identify and manage national security risks such as sabotage, espionage and coercion. Given the increase of cyber connectivity in this sector, the *Security of Critical Infrastructure Act 2018* was passed to, among other things, support cybersecurity efforts.
- **Department of Home Affairs**—the lead department for national security policy. The department's cybersecurity webpage links to relevant resources and initiatives, such as *Australia's Cyber Security Strategy*.
- **Data61**—Australia's main digital research network within the Commonwealth Scientific and Industrial Research Organisation (CSIRO). In the cybersecurity sphere, Data61 is working to build more trustworthy and resilient systems that have military applications, developing knowledge-based risk management, automating cybersecurity and expanding partnering opportunities through initiatives such as SINET61 (security innovation network).
- Under the **Joint Cyber Security Centre Program**, a number of Joint Cyber Security Centres (JCSC) are being established across Australia. The first JCSC was opened in Brisbane in February 2017, and others have since opened in Melbourne, Sydney, Perth and Adelaide.
- **Defence Science and Technology** (DST)—the ADF's research and development arm, which aims to enhance military and national security capabilities, including cyber. DST also has responsibility for the National Security Science and Technology Centre, which includes cybersecurity as one of six national security science and technology priority areas.
- **Information Warfare Division** (IWD)—formed in July 2017 as part of the Joint Capabilities Group within the ADF. The IWD has four branches: the 'Information Warfare Capability, C4 and Battle Management Capability, Capability Support Directorate and the Joint Cyber Unit'. In January 2018 the IWD released the Information Warfare Strategy, which identifies four areas of capability: 'self-defence, passive defence, active defence and offence'.

National—non-government

- **Australian Strategic Policy Institute International Cyber Policy Centre**—regularly publishes research on cyber-related issues in Australia and the Asia-Pacific that have a bearing on strategic policy. Each year from 2014 to 2017, the International Cyber Policy Centre has published a cyber maturity in the Asia-Pacific region report.
- **UNSW Canberra Cyber**—based at the Australian Defence Force Academy, it offers students (military and civilian) professional and postgraduate courses specifically related to cyber. UNSW Canberra Cyber also hosts a research group on cyber war and peace and covers research themes such as complex systems security, offensive security, and useable security and value sensitive design.
- **ANU Cyber Institute**—launched in October 2017 and jointly managed by the College of Engineering and Computer Science and the National Security College. The Institute received funding from ASD to 'strengthen collaboration between ASD and ANU students and researchers in the crucial area of data analytics' and cybersecurity.

- **AustCyber**—a government-backed, industry-led initiative that brings businesses and researchers together to promote the cybersecurity sector in Australia and its links to international markets.

International

- **International Telecommunications Union—Cybersecurity**—ITU members can access tools, advice, assessments and technical assistance to increase cybersecurity capabilities and build trust in information, communication and technologies.
- **World Economic Forum Centre for Cybersecurity**—aims to 'establish, activate and coordinate global public-private partnerships to encourage intelligence sharing and the development of cyber norms'.
- **Organization for Security and Co-operation in Europe (OSCE)**—details initiatives that OSCE member states are taking to reduce the risks of conflict stemming from the offensive use of cyber capabilities through devising confidence-building measures.
- **New America Cybersecurity Initiative**—publishes reports and blog posts on cybersecurity issues, including translations of official Chinese-language materials on cyber and information policy through its DigiChina project.
- **The RAND blog**—hosts commentary, essays and articles on issues intersecting with cyber and data sciences, including cybersecurity. A 2017 research paper, *Exploring Cyber Security Policy Options in Australia*, presents recommendations based on an exploratory exercise held in December 2016 with participants drawn from the public and private sectors, academia, think-tanks, industry associations and the media at the Australian National University's National Security College in Canberra.
- **Cybersecurity Capacity Portal**—developed by the Global Cyber Security Capacity Centre, this resource maps projects, programs and initiatives aimed at capacity building to achieve cybersecurity objectives. It also publishes cybersecurity capacity maturity model assessments as either regional studies or country reports.
- **North Atlantic Treaty Organization** (NATO)—established a number of Cyber Defence mechanisms as part of NATO members' overall collective defence. This includes the 2016 Cyber Defence Pledge to prioritise cyber defence and the formation of NATO Cyber Rapid Reaction teams. In 2018, NATO allies agreed to 'set up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure'. NATO and the European Union also cooperate via a Technical Arrangement on cyber defence, which was signed in February 2016. Cooperation with industry is being advanced though the NATO Industry Cyber Partnership.
- **NATO Cooperative Cyber Defence Centre of Excellence** (CCDCOE)—formally established in 2008 to 'enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation'. The CCDCOE maintains the *Tallinn Manual*, which is considered the 'most comprehensive analysis on how existing international law applies to cyberspace'.
- **UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security**—considers the application of international law and norms on the activities of UN member states in cyberspace. The GGE maintains a 'trends in cyber-armament' map that illustrates member states' increasing investment in offensive cyber capabilities.

Cybercrime

Cybercrime is criminal activity where a computer or network is integral to, or the target of, an offence. It will often target individuals, their data or their reputation. Cybercrime can encompass conduct such as cyberbullying, hacking, unauthorised modification or destruction of data, distributed denial of service attacks, online child pornography, online fraud and scams, 'trolling', and image-based abuse.

The Commonwealth first enacted specific computer-related offences in 1989, after such offences were recommended by the Review of Commonwealth Criminal Law Committee. The *Cybercrime Act 2001* modernised Commonwealth computer offences, inserting Part 10.7 into the *Criminal Code Act 1995* (*Criminal Code*). The key offences cover unauthorised access to and modification or impairment of data held in a computer or other device, and unauthorised impairment of electronic communications.

The *Cybercrime Act* also updated search powers in the *Crimes Act 1914* and the *Customs Act 1901* in response to technological developments. These provisions have been regularly updated to ensure that law enforcement officers have the powers necessary to search for and obtain electronic evidence. Most recently, the *Telecommunications and Other Legislation Amendment Act 2018* (*TOLA Act*) amended search powers in the *Crimes Act* and the *Customs Act* so that officers may access data remotely for the duration of a search warrant. The *TOLA Act* also introduced several other measures to assist law enforcement agencies to better deal with challenges posed by the increasing use of encryption, including an industry assistance regime (Part 15 of the *Telecommunications Act 1997*) and new computer access warrants (Division 4 of Part 2 of the *Surveillance Devices Act 2004*).

Australia acceded to the Council of Europe's *Convention on Cybercrime* (sometimes referred to as the Budapest Convention) in 2012. The Convention is the first international treaty on crimes committed against or using computer networks, and requires parties to criminalise relevant conduct, have certain investigative powers in place, and to cooperate with each other to the widest extent possible on cybercrime investigations.

The Australian Government and state and territory governments agreed to the first National Plan to Combat Cybercrime in 2013. The plan committed governments to actions against six key priorities: community education; partnering with industry; fostering an intelligence-led approach and sharing information; improving law enforcement capacity and capability; improving international cooperation; and ensuring the criminal justice framework is effective. In May 2017 relevant federal, state and territory ministers agreed to develop an updated national plan, but as at the date of publication of this Quick Guide, a revised plan had not been released.

Australia's International Cyber Engagement Strategy, released in 2017, included commitments aimed at raising cybercrime awareness in the Indo-Pacific region; assisting countries in the region to strengthen their cybercrime legislation; building cybercrime investigation and prosecutorial capacity in the region; and enhancing diplomatic dialogue and international information sharing on cybercrime.

Two parliamentary committee inquiries have focused specifically on cybercrime. The then Parliamentary Joint Committee on the Australian Crime Commission reported on its inquiry in March 2004, and the House of Representatives Standing Committee on Communications reported on its inquiry in June 2010.

Key internet links

- **Department of Home Affairs**—the lead Australian Government agency for cybercrime and identity security policy. The department's cybercrime and identity security page provides

information on relevant policies and initiatives, including the National Plan to Combat Cybercrime.

- **Australian Cybercrime Online Reporting Network** (ACORN)—a national online system for reporting cybercrime and helping people recognise and avoid common types of cybercrime, such as online scams. An initiative of the National Plan to Combat Cybercrime, ACORN was designed to 'make it easier to report cybercrime and help develop a better understanding of the cybercrime affecting Australians'. ACORN publishes quarterly statistical overviews of the reports it receives about cybercrime. It was evaluated by the Australian Institute of Criminology in 2016.
- **Australian Federal Police's cybercrime page**—provides links to further information on relevant offences, issues and initiatives, including high-tech crime, digital forensics and the Virtual Global Taskforce.
- **Scamwatch**—provides information aimed at helping consumers and small businesses to recognise and avoid scams, and a means of reporting scams to the Australian Competition and Consumer Commission.
- **Cybercrime Observatory**—a centre at the Australian National University that aims to 'identify the patterns, methods and causes of Internet based crime and to better understand the impact on victims and society'. The publications page lists publications by researchers at the centre.
- **The Conversation's cybercrime page**—has links to articles on cybercrime by Australian and overseas academics.
- **Cybercrime repository**—the United Nations Office on Drugs and Crime's central data repository linking to cybercrime case law; legislative provisions on cybercrime and electronic evidence; and national practices and strategies in preventing and combating cybercrime.
- **RAND Corporation's cybercrime page**—has links to relevant reports, articles and commentary.

Many of the resources listed above under 'Cybersecurity' are also relevant to cybercrime. In that context, it is worth noting that:

- the Australian Cyber Security Centre includes staff from the Australian Federal Police and the Australian Criminal Intelligence Commission and
- the Australian Signals Directorate's functions were expanded in 2018 to include preventing and disrupting (by electronic or similar means) cybercrime undertaken by people or organisations outside Australia.

Cybersafety

Cybersafety is the term used to describe initiatives and resources to help an individual manage their online behaviour and information. A number of Commonwealth offences to punish and deter offensive online behaviour exist, and there are offences at the state level that address cyber harassment, cyberstalking and cyberbullying, which carry prison sentences. However, the focus of cybersafety is on education and an individual's capacity to monitor their online presence and online risks, including cyberbullying and image-based harm.

Discussion in parliament about online safety for children can be traced back to at least 2010 with the creation of the Joint Select Committee on Cyber-Safety by the then Labor Government, which released the reports *High Wire Act: Cybersafety and the Young* in June 2011 and *Issues Surrounding Cyber-Safety for Indigenous Australians* in June 2013. This latter report focuses on young Indigenous people in remote and rural communities.

In January 2014 the Department of Communications and the Arts released a discussion paper seeking views about a range of policy proposals by the Abbott Government, including the establishment of a Children's e-Safety Commissioner and possible legislative changes to create a new, simplified cyberbullying offence. In December 2014 the Enhancing Online Safety for Children Bill 2014 was introduced to establish the Children's e-Safety Commissioner, within the Australian Communications and Media Authority (ACMA). The Enhancing Online Safety for Children Bill provided for a complaints system for cyberbullying material aimed at Australian children and a two-tiered scheme for rapid removal of that material from large social media services. It also set out the functions of the Children's e-Safety Commissioner to include promoting and supporting online safety for children. Both Bills were referred to the Environment and Communications Legislation Committee in December 2014 and a report was published in March 2015. The Act came into force that same month.

Since 2015 additional amendments have been introduced to the *Enhancing Online Safety for Children Act 2015*. This includes the *Enhancing Online Safety for Children Amendment Act 2017*, which changed the title of the Act to the *Enhancing Online Safety Act* and the Children's e-Safety Commissioner to the Office of the eSafety Commissioner (eSafety Commissioner). It also expanded the functions of the eSafety Commissioner to include promoting online safety for all Australians.

The *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* amended the *Enhancing Online Safety Act*, the *Broadcasting Services Act 1992* and the *Criminal Code* to establish a complaints and objections system for the sharing of intimate images without the consent of the person depicted in those images—what is commonly referred to as 'revenge porn'. This legislation also made it illegal to share an intimate image of another person on social media, the Internet or other electronic service.

In 2017 the Senate Legal and Constitutional Affairs Committee inquired into the adequacy of existing offences in the *Criminal Code* and of state and territory criminal laws to capture cyberbullying. This included consideration of the adequacy of the policies, procedures and practices of social media platforms in preventing and addressing cyberbullying. In 2018 the Committee made recommendations that included increasing the maximum penalty for the current Commonwealth cyberbullying offence from three years to five years imprisonment. The Government had not responded to the Committee's recommendations as at the date of publication of this Quick Guide.

The eSafety Commissioner also administers the Online Content Scheme (Schedules 5 and 7 of the *Broadcasting Services Act 1992*). The Online Content Scheme regulates the internet industry and the content services industry through Codes of Practice and a complaints mechanism, which aims to protect the public from 'prohibited and potentially prohibited content'. The National Classification Code sets out the principles under which classification decisions are made. There are also guidelines for the classification of films, computer games and publications. In June 2018 the Government commenced a review into the *Enhancing Online Safety Act* and the Online Content Scheme. The report of that review was published on 15 February 2019 and made five recommendations, including that the Government introduce 'significant and wide ranging changes to the online safety system', which will 'set out the new norms and standards for the online world, and establish new regulatory arrangements to put them into practice'.

Cybersafety can also be seen as something for groups and organisations to consider in their day-to-day practices as well as in their broader planning. Increasingly, organisations are forced to consider cybersafety in their values, risk assessments, capacity and their everyday communications and transactions. Australia has focused on the cybersafety of the individual (or groups of individuals such as children and the elderly) and emphasised the importance of managing one's online behaviour. However, there is an increasing awareness of the need to assist

small and medium enterprises to protect themselves from malicious online activity that can affect their reputation or financial security.

Australian cybersafety resources include:

- **bullyingnoway.gov.au**—provides information and ideas for students, parents and teachers. Bullying. No Way! and the National Day of Action against Bullying and Violence are managed by the Safe and Supportive School Communities (SSSC) Working Group. The SSSC includes representatives from the Commonwealth and all states and territories, as well as the national Catholic and independent schools sector.
- **childwise.org.au**—provides education and resources for people to actively prevent child abuse and exploitation, including online exploitation.
- **eSafety.gov.au**—the Office of the eSafety Commissioner's website provides a reporting portal for cyberbullying, illegal content and image-based abuse, as well as resources for schools, parents and children.
- **ThinkUKnow**—a partnership between the Australian Federal Police, Commonwealth Bank, Microsoft and Datacom, and delivered in partnership with all state and territory police and Neighbourhood Watch Australasia. ThinkUKnow presents to schools and parents about what young people see, say and do online, and the risks of online activity.
- **IDCare**—a not-for-profit initiative, serving Australian and New Zealand communities, which provides specialist counselling and information resources to support victims of cybercrime and members of the public with cybersecurity concerns. It also offers subscription services for private and public sector organisations to promote cyber resilience and awareness.