Australian Alert Service dossier

Five Eyes and NATO upgrade cyber warfare

The articles in this dossier appeared in the *Australian Alert Service*, weekly publication of the Citizens Electoral Council of Australia, in 2018.

This page is intentionally blank

London pushes for Article 5 changes at July NATO conference

By Richard Bardon

Hysterical British-led denunciations of Russia are growing ever louder in the lead-up to the 11-12 July North Atlantic Treaty Organisation (NATO) Heads of State summit in Brussels, Belgium. Desperate to keep Western Europe in the Anglo-American orbit post-Brexit, the British establishment has renewed its efforts to set up a confrontation with Russia by broadening the scope of the NATO Charter's Article 5, which mandates collective defence by all alliance members, to include cyber attacks and other forms of "hybrid warfare" as triggers for a military response. The British government or its "Five Eyes" allies (the USA, Australia, Canada and New Zealand) could then provoke a conflict at will via a false-flag attack using their own formidable cyber-warfare capabilities.

Britain's efforts to re-write Article 5 go back at least to 2014. In July of that year, to set the agenda for the NATO Heads of State summit in Wales the following month, the British Parliament's House of Commons Defence Select Committee issued a report entitled "Towards the Next Defence and Security Review: Part Two—NATO", which asserted without proof that Russia had been deploying "asymmetric", "ambiguous", or "deniable" acts of war, such as "information" or "cyber" war, as well as irregular units of "little green men", which were insufficient to trigger Article 5 as presently written.[1] As a result of British browbeating, the NATO heads of state agreed at the summit that "A decision as to when a cyber attack would lead to the invocation of Article V would be taken by the North Atlantic Council on a case-by-case basis". In June 2016, NATO Secretary General Jens Stoltenberg, after a meeting of the alliance's defence ministers, proclaimed that cyberspace would henceforth be considered an "official operational domain of warfare" alongside air, sea, and land. To date, however, the NATO members have not agreed to alter the wording of Article 5, which at present allows a response only to an "armed attack". Also lacking is a formal doctrine of what constitutes "hybrid warfare".

The British elites are as usual manoeuvring to write those rules themselves. Former UK Foreign Secretary William Hague (now Baron Hague of Richmond), in a 19 March column for City of London organ *The Telegraph* headlined "NATO must confront Putin's stealth attacks with a new doctrine of war of its own", wrote that hybrid warfare will be a subject of discussion at the July NATO summit in Brussels. Incredibly, Hague argued that NATO should be prepared to go to war with Russia purely on suspicion: "Collective attribution and identification of cyber attacks, or of secret positioning to launch them in future, is a crucial step to a common strategy", he wrote. "So is the agreement that NATO is the right vehicle for this" rather than the European Union, a greater role for which would "dilute, confuse and weaken the Western response, divorcing it from the USA and Canada"—and Britain itself post-Brexit, he failed to add. With that decision made, he continues, "NATO leaders should be instructing their experts to evolve a new doctrine of hybrid warfare and contemplate reinforcing the NATO treaty of 1945 to accommodate it." The scenario which Hague says prompted NATO's "new thinking" on the subject of hybrid warfare is Russia's alleged "coordination of social media and armed groups [in eastern Ukraine] as a way of invading a country without saying so". By that logic Syria's allies, including Russia, would have been within their rights to declare war on Britain, France and the USA in 2011.

At the same time it foams at the mouth over imaginary Russian cyber attacks, Britain is expanding its own offensive cyber-warfare capabilities with the creation of a "joint cyberforce [which] will comprise more than 1,000 GCHQ [Government Communications Headquarters, Britain's signals intelligence agency] and military personnel as well as contractors", *The Times* reported 14 March. Ostensibly formed to combat hostile states and terrorist groups, the new unit could just as easily—especially given the use of deniable "contractors"—be used in false-flag actions against allies, to kick-start a war with Russia. In a 7 March 2017 press release, WikiLeaks exposed that the US Central Intelligence Agency had "lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponised 'zero day' exploits, malware remote control systems and associated documentation."[2] As WikiLeaks noted, "This extraordinary collection … [including] a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation", had been circulated among current and former CIA contractors in an uncontrolled manner, making attribution of future cyber attacks practically impossible. But it makes Russia even easier to blame.

1. "British oligarchy planning new 9/11 to trigger WWIII?", *The New Citizen* Vol. 8 No. 1, Nov.-Dec. 2014.

2. R. Bardon, "'UMBRAGE': WikiLeaks burns down CIA false-flag factory", *AAS* 15 Mar. 2017.

British Intelligence is preparing a cyber attack on the UK, to be blamed on Russia

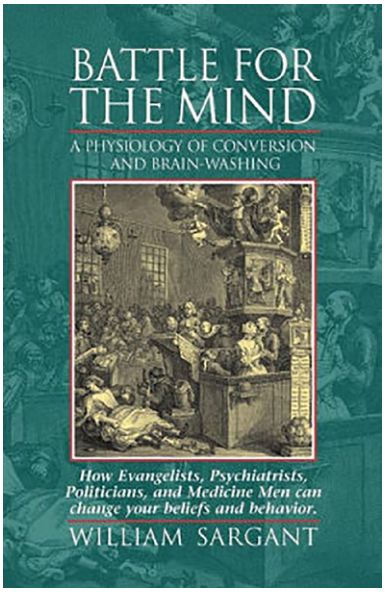
By Richard Bardon

> "Various types of belief can be implanted in many people, after brain function has been sufficiently disturbed by accidentally or deliberately induced fear, anger or excitement. Of the results caused by such disturbances, the most common one is temporarily impaired judgment and heightened suggestibility. Its various group manifestations are sometimes classed under the heading of 'herd instinct', and appear most spectacularly in wartime, during severe epidemics, and in all similar periods of common danger, which increase anxiety and so individual suggestibility."
>
> —*The Battle for the Mind: A Physiology of Conversion and Brainwashing,* Dr William Sargant (consultant to MI5), 1957.

24 April—When in the near future there is a crippling cyber attack on one or more of the UK's business sectors or essential services, the place to look for the culprit will not be Russia, but rather the Government Communications Headquarters (GCHQ), Britain's signals intelligence agency. Just as MI5, the British Security Service, has repeatedly enabled and even orchestrated terrorist attacks on British soil[1] to advance the Establishment's political agenda, GCHQ—headed since March 2017 by Jeremy Fleming, immediate past deputy director-general of MI5 since 2013—is preparing to plant "Kremlin" fingerprints on a false-flag cyber attack that will both stampede the UK's allies into confrontation with Russia under the principle of collective self-defence enshrined in Article 5 of the North Atlantic Treaty Organisation (NATO) charter, and provide a pretext for a police-state power-grab at home.

Already in 2014, the NATO heads of state, under British pressure, agreed to include cyber attacks and other forms of "hybrid warfare" as triggers for a military response "on a case-by-case basis". The British are angling to formally rewrite Article 5 at the NATO Heads of State summit in Brussels, Belgium this July,[2] while the 53 nations of the British Commonwealth were pressured into signing a digital security pact, the "Commonwealth Cyber Declaration", at the 19-20 April Commonwealth Heads of Government Meeting in London—in effect signing over control of their signals intelligence to the "Five Eyes" apparatus dominated by GCHQ and the US National Security Agency (NSA), whose other members are Australia, Canada and New Zealand. At a bilateral meeting on the sidelines, Prime Ministers Malcolm Turnbull and Theresa May issued an "Australia-UK Cyber Statement", pledging "a new era of practical co-operation" between the Australian Signals Directorate and the UK National Cyber Security Centre (NCSC), a division of GCHQ.

Many countries' governments have already proven themselves easily led, having been induced into rash actions against Russia by British Intelligence's previous frauds such as the 4 March poisoning of Sergei and Yulia Skripal in England,[3] which led to the expulsion of almost 150 Russian diplomats from 27 countries; and the hoax of a chemical weapons attack in Douma, Syria on 7 April,[4] which a week later saw Britain, the United States and France risk a direct military clash with Russia by launching missiles at Syrian government targets. An invocation of Article 5 could be expected to sweep aside all remaining opposition to war with Russia—"cold" at best, thermonuclear-hot at worst.



Sargant (1907-1988) and his collaborator, WWII British psychological warfare expert Brig. Gen. J.R. Rees, advocated the use of psychological "mass shocks" to control restive populations, both throughout the Empire and at home. In particular the use of terror, they emphasised, could change an entire population's beliefs overnight.

Propaganda drumbeat

The Establishment press has been working for the past month to whip up public fears with tales of impending Russian cyber attacks against the UK's essential infrastructure and services. The 18 March *Sunday Times*, for example, reported that the operators of the national electricity grid, along with "gas and water firms, the Sellafield nuclear power plant, Whitehall [government] departments and NHS [National Health Service] hospitals have all been warned to prepare for a state-sponsored assault ordered by the Kremlin". More recent reports have stated that Russian cyber attacks are already under way. The *Daily Mail* on 13 April cited remarks by Ciaran Martin, chief executive of the NCSC, that Moscow was attempting to hack into "critical infrastructure" such as water supplies, electricity and gas systems, hospitals, banks and transport, as "part of a wider campaign to destabilise" the country. Most hysterical has been the ultra-Establishment *Telegraph*, which asserted 16 April that Russia had "launched a 'dirty tricks' campaign against Britain and the US … [which] could be a precursor to a campaign of cyber attacks by the Kremlin" in retaliation for the illegal US-UK-French 14 April missile strike on Syria. Another *Telegraph* article the same day blared that "Russia is targeting the home internet of tens of thousands of British households", while yet another quoted a security expert's opinion that Britain's electricity network and manufacturing industries were already "definitely under massive cyber attack".

As is usual in such cases, these allegations along with others sourced either to unnamed government officials or to former police, military and intelligence officers now in the private sector, are being repeated as fact throughout the mainstream-media echo chamber—a never-ending drumbeat designed

1. *Stop MI5/MI6-run Terrorism!*, Citizens Electoral Council, 18 June 2017.
2. "London pushes for Article 5 changes at July NATO conference", *AAS* 28 Mar. 2018.
3. "Desperation drives British escalation against Russia" and "Zero evidence for May's 'Novichok' accusation vs Russia", *AAS* 21 Mar. 2018.
4. *AAS*, 18 Apr. 2018, pp 1, 5-12.

so that, as political analyst Phil Butler wrote 23 April in the online magazine *New Eastern Outlook*, "any time a light flickers in London or Edinburgh citizens will think it was Putin".

Top GCHQ figures are publicly taking point in fanning expectations of Russian attacks. At CYBERUK 2018, an event held by the NCSC 10-12 April in Manchester, GCHQ Director Fleming made what *Guardian* journalist Ewen Mac-Askill identified as "his first public appearance after more than two decades as an intelligence officer". According to MacAskill's 12 April article, Fleming "was more emphatic in attributing for the Salisbury [alleged nerve-agent poisoning] attack than Theresa May", and dropped the qualifiers such as "alleged" or "highly likely", used by the prime minister. Fleming's main topic was Russia, including the Salisbury affair, unverified chemical weapons use in Syria, and the Russian cyber attacks he claimed were sure to come. "To stay ahead", he promised, "…we are investing in deploying our own cyber toolkit", which "combines offensive and defensive cyber capabilities".

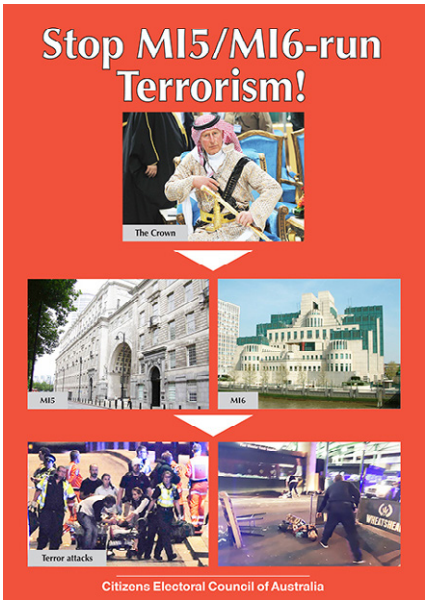
Not content only to be quoted in the media, NCSC head Ciaran Martin, who is also GCHQ Director General for Government and Industry Cyber Security, chimed in with an article under his own by-line in the *Telegraph* of 21 April, headlined "A serious cyber attack on Britain is a matter of 'if', not 'when'". An accompanying article in the newspaper reported that executives from utilities, transport and internet companies, as well as the National Health Services, have been brought in for NCSC briefings "on the specific methods—known as 'attack vectors'—being used by Russia to target Britain's critical national infrastructure", as if this were an already established fact.

Yet another dodgy dossier

Look past the hype, however, and one sees that the media reports never describe specific incidents, nor identify the targets of the alleged attacks. The only official "evidence" cited is a Joint Technical Alert (JTA) issued 16 April by the NCSC and the USA's Department of Homeland Security and Federal Bureau of Investigation (FBI). The JTA is reminiscent of the 6 January 2017 report "Assessing Russian Activities and Intentions in Recent US Elections", wherein the US Central Intelligence Agency (CIA), the FBI, and the NSA alleged that Russia had hacked the Democratic Party's servers to influence the 2016 presidential election in favour of Donald Trump,[5] in that it mainly comprises generic cybersecurity advice, combined with a lot of innuendo and a smattering of "evidence" that is convincing only to the extent that one already believes in Russia's guilt.

Yet the one piece of intelligence presented as hard fact, on the sixth of the JTA's thirteen pages, fatally undermines its whole case: On 18 November 2016, it states, "a Smart Install Exploitation Tool (SIET) was *uploaded to the internet*. … Of concern, *any actor may leverage this capability* to overwrite files to modify the device configurations, or upload maliciously modified OS [operating system files] or firmware to enable persistence [of access to compromised devices]." (Emphasis added.)

In other words, the supposed smoking gun implicating Russia is an open-source tool potentially available to every hacker in the world for over a year! Attribution of its use to Russia is sourced to "commercial and government security organisations", but since none of these are named, their testimony cannot be verified, nor do the NCSC and FBI claim to have done so. They state only that they "have high confidence that Russian state-sponsored cyber actors are using compromised routers to conduct man-in-the-middle attacks to support espionage … and potentially lay a foundation for future offensive operations." As the January 2017 FBI-CIA-NSA report itself disclaimed, however, "High confidence … does not imply that the assessment is a fact or a certainty; such judgments might be wrong. … Judgments are not intended to imply that we have proof that shows something to be a fact."



The CEC's June 2017 pamphlet, circulated widely in the UK, emphasised that the rash of terror attacks by MI5/MI6 assets during the preceding months' national election campaign in which Jeremy Corbyn soared in the polls, were invariably preceded by authoritative forecasts that such attacks were "inevitable".

The good news is that the Crown/City of London Establishment's willingness to go out on such narrow limbs betrays that it is operating from a position of weakness. With its economic system teetering on the edge of a new blowout far worse than that of 2008, blaming Russia for a false-flag attack on the UK may be the Establishment's last chance to divide the world once more into warring camps, thus forestalling the "multi-polar" order of cooperation among sovereign nations, exemplified by China's Belt and Road Initiative, in which Russia is an important partner.

Should its ploy fail, however, the Establishment will have destroyed what remains of its credibility, both abroad and, just as importantly, at home. Absent a manufactured emergency that would justify such totalitarian measures as the cancellation of elections, it faces the prospect that its puppet Tory regime will be swept from power at every level of government by the City of London's worst nightmare: a Labour Party government led by Jeremy Corbyn, who has pledged to break up the City of London's too-big-to-fail banks, end Britain's orchestration of regime-change wars abroad, and work with Russia at the UN instead of escalating towards nuclear war.

5. "Obama's 'Russian hacking' lie unravels", *AAS* 12 Jan. 2017.

Five Eyes plan global police state

By Elisa Barwick

20 Aug.—At the end of August representatives of the Five Eyes intelligence alliance—the USA, UK, Canada, New Zealand and Australia—will meet in Sydney. Not much is known about the upcoming summit and may not be even after it occurs, but fortunately—at least for the purpose of understanding what the top-secret alliance is planning—Australia's Home Affairs Secretary Michael Pezzullo is a bit of a windbag. Pezzullo has asserted that "trail-blazing" initiatives would emerge from the consultations, and in a number of speeches has foreshadowed a new era of globalisation in the realm of security.

In a 26 June parliamentary speech about the Turnbull government's foreign interference bills, MP and Iraq WMD whistleblower Andrew Wilkie said, "I will go so far as to say that Australia is a pre police state". The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*, which passed the federal parliament on 28 June, established an unprecedented state-secrecy regime smothering freedom of speech, association and political communication, in the name of curbing so-called foreign influence. ("Resistance builds to Turnbull's totalitarian 'national security' laws", *AAS* 7 Feb.; "Officials warn 'foreign influence' laws undermine parliamentary privilege", *AAS* 4 April.) London's *Financial Times* revealed on 27 June, in "Australia leads 'Five Eyes' charge against foreign interference", that the push for foreign interference laws was occurring under the Five Eyes umbrella. All Five Eyes members, bar New Zealand—whose ongoing membership the article queried—are implementing measures ostensibly to prevent hostile foreign powers, a.k.a. Russia and China, manipulating elections or policies. In reality the Anglo-American financial establishment behind the Five Eyes is trying to prevent Western collaboration with nations seeking to establish a new fair and just economic and security architecture based on peaceful collaboration for development.

Security overhaul

According to Pezzullo's pontifications, what is being planned is far worse than Wilkie foreshadowed—*global police state laws* dictated by the Five Eyes. The new scheme has emerged following the dramatic shakeup of Australia's security framework which began with last year's review of the Australian Intelligence Community, and which effectively puts Five Eyes in charge of domestic security. The Australian Security Intelligence Organisation (ASIO) and Australian Secret Intelligence Service (ASIS) have always functionally been branches of their British counterparts MI5 and MI6, but Pezzullo now heads a super-ministry, modelled on the UK Home Office. The new Department of Home Affairs was created to oversee operations, strategic planning and coordination of the response to security threats, as conducted by ASIO, the Australian Federal Police, the Australian Border Force, the Australian Criminal Intelligence Commission, the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Office of Transport Security—agencies which currently operate under the purview of a number of ministerial portfolios. Pezzullo had pushed for such a super-ministry since he was Opposition Leader Kim Beazley's deputy chief of staff in 2001; he pushed it as Secretary of the Department of Immigration and Border Protection under the Abbott government, which considered such a move; and when the Turnbull government adopted it in December 2017, Pezzullo scored the top job under Minister Peter Dutton.

Home Affairs Secretary Michael Pezzullo testifying at a Senate hearing.
Photo: Screenshot

In addition, a new Office of National Intelligence is to be established, likely taking over the operations of peak intelligence body the Office of National Assessments, but assuming a broader role coordinating and directing Australia's five spy agencies—ASIO, ASIS, the Defence Intelligence Organisation (DIO), Australian Geospatial-Intelligence Organisation (AGO) and Australian Signals Directorate (ASD). The independent statutory body will operate within the Prime Minister's portfolio and report directly to the PM.

The bill to establish the Office of National Intelligence was introduced into the House of Representatives on 28 June following examination by two parliamentary committees. When Turnbull announced the Office on 18 July 2017, he stressed that all other Five Eyes partners have a "single point of coordination" for intelligence, and that "Australia doing the same will ensure even better collaboration with our Five Eyes partners". At the Commonwealth Heads of Government Meeting (CHOGM) in London on 19-20 April, Turnbull signed Australia up to a new cyber security pact forged by the 53 member nations, extending the collaborative relationship between the Five Eyes spy alliance (four of which are Commonwealth countries) into a broader network. On the sidelines of the meeting, Australia and the UK signed up to a new joint strategy to work together at the operational level to target cyber crime, piloting "new tactics, techniques and capabilities" and coordinating "global responses" to attacks.

Pezzullo reveals all

Delivering the keynote address at the International Summit on Borders in Washington, DC on 19 June, "Rethinking the Security Role of the State in a Complex and Connected World", Mr Pezzullo demanded that security mechanisms keep up with the advance of globalisation. Along with its benefits, he observed, globalisation has also brought a "dark side" as criminal networks and terrorists take advantage of global connectivity and less rigid borders, typified by cyberspace.

Pezzullo noted that the Five Eyes grouping has taken up the need for transnational collaboration on domestic security and law enforcement. "[F]or decades these issues were

seen as matters to be dealt with 'within jurisdiction', ... this is no longer the view held by the Five Eyes partners, ... the meeting in Australia in August will be a trail-blazing one in terms of significantly advancing transnational security collaboration across a broad range of functional problems and mission areas."

Calling for the integration of "all of our tools of national power, including the cloak and the dagger, the data scientist and the detective, the border officer and the diplomat", Pezzullo spelt out how we must rethink the function and structures of government itself. While "we tended to think of the state as possessing 'majestic power'" following the rise of the modern nation-state in Europe in the 17th century, with today's erosion of sovereignty "nothing less than the transformation of the state itself will be required. Still under the rule of law, and consistent with our fundamental constitutional arrangements, the state will in future need to become at times less visible, more deeply embedded in sectors and vectors, and ever-vigilant. We will have to reorganise how government works in order to achieve this and we will have to factor in a transnational model of security."

In a subsequent, 17 July speech to the 4th Australian Security Summit in Canberra, Pezzullo elaborated on the envisioned new global security architecture: "Ironically—and somewhat paradoxically—in the networked and connected world that I have described, *unity of command, clarity of authority, and singularity of purpose* need to be hardwired into our security architecture lest our agility and flexibility to respond be compromised. [Emphasis added.] We certainly need to *re-think the paradigm that domestic security and law enforcement can be exclusively executed within national jurisdictions*. [Emphasis in original.] This is, of course, the prevailing paradigm—and understandably so in a world of nation states; the world that emerged in that same 17th century after the Peace of Westphalia."

New "values, norms and legal constructs" are required, he said, to fill regulatory and compliance gaps created by the globalised world, which is outpacing national laws and rules. The argument is that criminal syndicates can "operate in the gaps and seams created through those jurisdictional boundaries" of traditional, national jurisdictions, i.e. sovereign nations. New models of decision-making are required, incorporating sophisticated data models, analytics, powerful computational capabilities, and even artificial intelligence, to accurately assess risk and secure borders, vital infrastructure and the integrity of elections.

Given the history of the Five Eyes network, transparency on exactly what this will mean shall definitely not be forthcoming. Only a survey of existing police-state laws in Australia and the UK provides an indication of the direction that will be taken. (The latest proposals before the UK parliament have been denounced by former MI5 officer Annie Machon as "a potentially dangerous blueprint for a techno-Stasi state", *AAS* 27 June.) Originally set up by Britain in 1946 as the UKUSA Agreement, to leverage its influence over the United States after World War II, the existence of the broader Five Eyes alliance was unacknowledged for thirty years. Even thereafter it did not gain wide public attention until 2013, when documents released by Edward Snowden revealed the group's extensive monitoring of each other's citizens to get around domestic surveillance laws. US National Security Agency (NSA) whistleblower Thomas Drake called the Five Eyes and its extensions "a hidden empire". Is this the institution we want in charge of our "security"?

Turnbull: Assange broke no Australian law

In a 31 July article for *Consortium News*, Virginia State Senator Richard Black urged a sovereign state to step forward and offer WikiLeaks founder Julian Assange asylum.

Black argued that "Government 'of the People' cannot flourish beneath a suffocating cloak of secrecy. And secrecy is often aimed, not at protecting us from enemies abroad, but at deceiving us about the dark machinations of our own government. …

"Before Assange, those who 'broke the code' and detected the Deep State's patterns of misbehaviour were labelled 'conspiracy theorists' or worse." Black points out that Assange's information, with the advent of WikiLeaks, produced "original, unchallenged source documents that have proven our arguments, and revealed the truth to citizens".

Since the election of US President Donald Trump, which "sent shock waves through the Deep State", there is a new, more intense "coordinated effort to reimpose information control", said Black. In that context Assange's life may even be at risk, he continued, as "Julian Assange and WikiLeaks are among the censors' prized targets".

"I realise that Julian Assange is controversial", Black concluded, "but I'd be pleased if some courageous nation granted him permanent asylum. Let him continue giving citizens an honest peek at the inner workings of their governments. That seems to be our best hope for peace."

It is a no-brainer that as Assange is an Australian citizen, Australia should be that country, and our Prime Minister has more reason than most to consider it. Former senior MI5 officer Peter Wright, whose book *Spycatcher* breached the UK's *Official Secrets Act*, was defended in his late 1980s court case by then up-and-coming lawyer Malcolm Turnbull. Wright's right to publish his book in Australia was upheld, a victory for free speech. Sky News *Outsiders* program host and former Liberal MP Ross Cameron revealed on 16 August an audio clip of then Shadow Minister for Communications reflecting on this case, and on Assange's plight, in front of some of the country's most eminent lawyers at the Sydney University Law School on 31 March 2011. Turnbull said:

"The High Court was very clear in declaring that an Australian Court should not act to protect the intelligence secrets and confidential political information of a foreign government, even one which was a very friendly one, and even in circumstances where the Australian government requested the court to do so. Now I stress this point because it has a current relevance to the case of Julian Assange, who you will remember, our Prime Minister Julia Gillard described as someone who had broken the law—acted illegally by publishing the contents of confidential US State Department cables.

"Not only was it perfectly obvious that Mr Assange had broken no Australian law—and despite the strenuous effort of the Americans there is no evidence that he has broken any American ones—but the decision of the High Court in *Spycatcher* makes it quite clear than any action in an Australian court to restrain Mr Assange from publishing the state department cables would have failed. These remarks by the Prime Minister, which were echoed by her Attorney General, are particularly regrettable, not simply because she was so obviously in error from a legal point of view, but whatever one may think of Mr Assange, whatever Julia Gillard may think of Mr Assange, he is after all an Australian citizen."

Facebook—thought-police for the War Party

Special to the AAS

On 31 July the social media company Facebook shut down 32 accounts on its platform, for being "bad actors" engaging in "coordinated inauthentic behaviour". The company's chief cybersecurity officer admitted that "we still don't have firm evidence to say with certainty who's behind this effort", but he dropped a loud hint about Russian election meddling: "Some of the activity is consistent with what we saw from the IRA before and after the 2016 elections." IRA stands for the Internet Research Agency, the alleged "troll factory" in St. Petersburg, Russia, some of whose staff were indicted last February by Russiagate Special Counsel Robert Mueller for interfering in the 2016 US Presidential election though ads and comments from fake internet personas.

Facebook revealed that they were helped to "analyse and identify" the new online activity by the Atlantic Council's Digital Forensic Research Lab (DFRL). The Atlantic Council is a Washington, DC-headquartered think tank that serves as the de facto lobbyist for the North Atlantic Treaty Organisation (NATO). It has been in the forefront of campaigns to provoke conflict with Russia. Its largest contributor is the British government.

Thus Facebook Chairman and CEO Mark Zuckerberg has turned the company he founded while a student at Harvard into a tool of the Anglo-American Party of War. As of contracting a formal partnership last May between Facebook and the Atlantic Council, Zuckerberg and his colleagues have given the highly biased Atlantic Council the power to apply its political judgments and its algorithms, to decide which speech on Facebook comes from "bad actors" and should be silenced.

Facebook had already come under criticism for compiling and commercially sharing personal data on its more than one billion subscribers. In March of this year, the *New York Times* revealed that the British consulting company Cambridge Analytica had accessed personal data on at least 50 million American voters from Facebook; and had provided the data to the Ted Cruz and Donald Trump presidential campaigns.

While the *New York Times* scandal played into allegations of illegal campaign operations by the Trump campaign, more fundamentally it shed light on Facebook's fast and loose handling of its subscribers' personal data. Cambridge Analytica had accessed a total of 87 million Facebook profiles by simply hiring a Cambridge University researcher, Aleksandr Kogan, to claim he was seeking the data for "academic research".

There was no hack, Facebook admitted; rather, Kogan had been given access to the massive database of personal profiles simply on basis of his "academic" request. Facebook officials, including Zuckerberg, chief operating officer Sheryl Sandberg, and the cybersecurity director, Nathaniel Gleicher, acknowledged that they first became aware of the data breach by Cambridge Analytica in 2015, but took no serious action until the *Times* story appeared.

On 10-11 April 2018, Zuckerberg was grilled in US Senate and House of Representatives hearings about both the Cambridge Analytica breach and Facebook's alleged failure to detect Russian election interference in 2016.

Anti-Russia campaign

The allegations of Russian hacking and other interference in the 2016 election have been used by Democrats to

Who is exacerbating divisions among Americans? The Atlantic Council's Digital Forensic Research Lab is encouraging people to help track trolls.
Photo: Screenshot medium.com/dfrlab

claim that Trump "stole" the election from Hillary Clinton. In the version of events peddled by many Clinton supporters, it was "Russian" fake Facebook ads and the "Russian" exposure through WikiLeaks of Clinton's cosiness with Wall Street and various dirty tricks by her campaign (none of this denied by Clinton), that turned voters in key states against the Democratic candidate. Thereby they dodge the reality of popular outrage in those farm and formerly industrial areas against Clinton's aloofness from their economic suffering, and the fact of Clinton's refusal to campaign there.

Cyber forensic experts, including former National Security Agency executive William Binney, have poked holes in the claims that Russian hackers stole emails from the Democratic National Committee (DNC) and gave them to WikiLeaks for online posting. One year ago Binney and other members of Veteran Intelligence Professionals for Sanity (VIPS), an organisation of former US intelligence community officers who have exposed abuses by top intelligence community officials, presented their analysis that the data was likely obtained through a leak, rather than by hacking.

While Obama Administration intelligence officials asserted that there had been Russian hacking, based on an assessment by carefully selected analysts from the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency, the only analysts to have examined the DNC computers directly were from a private firm, CrowdStrike, co-founded by Russian-born Dmitri Alperovitch. In July, Mueller indicted 12 alleged agents of Russian military intelligence for the supposed hack. Russian President Vladimir Putin promptly offered for Mueller to send interrogatories and be present when these men were questioned.

Besides hacking, the "Russian meddling" is alleged to have consisted of buying 3,500 ads on Facebook and other social media, and running Facebook accounts under fake names, for the purpose of inciting various groups in the USA against each other. This activity was attributed to the St. Petersburg "troll farm", the IRA. To the special counsel's shock, their lawyers have appeared in US court to contest the charg-

es. Many questions remain unanswered, regarding when the IRA even existed, who was running it, and for what purpose.

Enter the Atlantic Council

Zuckerberg took a beating during his two days of Congressional hearings in April. Company share prices had collapsed following the *New York Times* revelations. Before Congress, Zuckerberg admitted that Facebook had been cooperating with Mueller's Russiagate probe, but refused to disclose details. It was in the context of the Congressional spotlight, that on 17 May 2018 Facebook announced it was "partnering with the Atlantic Council in another effort to combat election-related propaganda and misinformation from proliferating on its service." Their formalised relationship "would help it better spot disinformation during upcoming world elections", Facebook declared.

Facebook's chief security officer Alex Stamos, according to a Reuters report on his conference call with journalists about the new account closings, explained the Atlantic Council's role: "Companies like ours [Facebook] don't have the necessary information to evaluate the relationship between political motivations that we infer about an adversary and the political goals of a nation-state." Another reason for bringing in the Atlantic Council, Reuters reported, was that "It would also be awkward for Facebook to accuse a government of wrongdoing when the company is trying to enter or expand in a market under the government's control."

Facebook has therefore bankrolled the Atlantic Council through a very large, but undisclosed amount of money, joining the British government as its largest donor.

The Atlantic Council had been in the forefront of anti-Russia propaganda operations surrounding the "Euromaidan coup" which in 2014 overthrew the elected President of Ukraine. It launched its DFRL in 2016 to track alleged Russian operations in eastern Ukraine.

The director of the new lab is Graham Brookie, who served on the National Security Council staff during the second Barack Obama Administration (2013-17). A senior fellow in the Atlantic Council's Cyber Statecraft Initiative is none other than Dmitri Alperovitch of CrowdStrike, authors of the accusations that "Russia" hacked the DNC. Crowdstrike's zeal to blame Russia for cyber-crimes is notorious. In 2017 the company had to retract its claim that the alleged Russian cyber "threat group" it blamed for hacking the DNC, had also hacked and damaged Ukrainian artillery pieces—an accusation the Ukrainian government itself refuted.

As part of the arrangement between Facebook and the Atlantic Council, the DFRL will have unfettered access to the entire Facebook database on its one billion clients worldwide.

Welcome to the new world of public-private Big Brother!

Home Affairs encryption bill: A political tool made in Britain

By Elisa Barwick

Australia's Home Affairs Department, created to streamline coordination of intelligence with the British Secret Service-led Five Eyes spying alliance (USA, UK, Canada, Australian, New Zealand), has produced legislation to allow Australia's intelligence and law enforcement agencies unprecedented access to the private data of citizens.

A draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, first announced in July 2017, was released publicly on 14 August and is open for consultation only until 10 September (assistancebill.consultation@homeaffairs.gov.au). Developed by Home Affairs in conjunction with agencies such as the Australian Security Intelligence Organisation (ASIO), the bill takes aim at the encryption of web transactions and communications, based on the fact that criminal networks also depend upon such protections to transact their business without being caught.

According to the Home Affairs Department, the legislation would force domestic and offshore providers supplying internet-based communications services and devices to assist Australian law enforcement in its pursuits; would create new computer access warrants enabling law enforcement to *covertly* access devices and collect evidence; and would strengthen existing search and seizure warrants for *overt* access to data.

California-based digital civil liberties group, Electronic Frontier Foundation (EFF), says the legislation "unashamedly lifts its terminology and intent from the British law" passed in November 2016, the *Investigatory Powers Act* (IPA, a.k.a. the Snoopers' Charter), sharpening its powers even further. It would allow the government to demand that tech companies re-engineer or substitute apps, services or programs to enable surveillance to be conducted, to hack into computers, or remotely access private data, supposedly to protect national security. Telcos, Internet Service Providers (ISPs), software developers, websites, chat groups, messaging and other apps, email distribution companies, hosting services, etc., would have to comply. The orders and any consequences for consumers would remain secret. The penalty for disclosing information is five years' imprisonment; for not complying with an assistance order, 5-10 years!

Authorities could target individual app or software developers, whether a hobbyist or employee of a multinational company. The wording of the equivalent UK legislation allows authorities to seek out particular employees of a company to conduct a task *without informing his or her employer*. It is even possible to force a coffee shop chain providing free WiFi to deploy malware on its customers, on behalf of the British secret service, according to EFF's Danny O'Brien.

The Australian bill does not allow electronic protections currently afforded to consumers to be weakened, but this and other concessions are "tiny exceptions in a sea of permissions, and easily circumvented", noted EFF. The language is broad enough to allow for far-reaching breaches of privacy, and there is no real oversight other than the Attorney General. For instance, the phrase "any other thing reasonably incidental to any of the above" appears 11 times in the legislation in reference to what specific actions are authorised by various warrants.

A global campaign

In the name of threats to national security from terrorists and hostile foreign states, the UK is working to bring domestic laws around the world into line with the types of illegal spying activities exposed by US National Security Agency (NSA) whistleblower Edward Snowden in 2013.

These claimed threats are a ruse. Terrorism is a very real threat, but it has been actively cultivated by UK and US governments and their proxies to justify regime change against "rogue" states (*Stop MI5/MI6-run Terrorism!*, CEC, June 2017). As for foreign state threats, accusations against Russia and China are often hyped and even baseless, such as when China was falsely accused of hacking Australia's census. And somehow spying on all of us is supposed to allay these threats, despite the fact that experts such as William Binney, a former technical director at the NSA who testified against the IPA in the British Parliament, have demonstrated that mass collection of data swamps the real intelligence capabilities required to stop terrorist threats. ("London/Manchester terrorism report a whitewash", *AAS* 13 Dec. 2017.)

Britain's Home Secretary Sajid Javid pushed the foreign interference barrow at the Five Eyes ministerial meeting on Australia's Gold Coast on 28-29 August, following unproven claims that Russia was behind the March poisoning of Sergei and Yulia Skripal in Salisbury, England. Australia has been a leading nation in the Five Eyes' push for a new standard of state-secrecy to prevent foreign interference—on 28 June the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* was passed, smothering freedom of speech, association and political communication.

The UK's IPA legislation was a precursor to this, introduced by Theresa May in 2015 when she was Home Secretary. When it passed in late 2016, she immediately began talking about the necessity for equivalent powers globally. In early 2016, Britain had already begun negotiating a reciprocal agreement with its US counterparts, whereby the UK could quickly access customer data from US social media or email servers, and vice versa. At the moment this occurs only by formal application to the foreign counterpart's domestic justice system, a very slow process. End-to-end encryption used by many internet services adds to the difficulty, as data is accessible only at its point of origin and final destination, with no access provided to the mediating party.

This is the context for the encryption bill; the same intent was evident in the Official Communiqué of the Five Eyes Ministerial meeting, which had been billed by Australia's Home Affairs Secretary Michael Pezzullo to include "trailblazing" initiatives ("Five Eyes plan global police state", *AAS* 22 Aug.) The spying forum was refocused, the Communiqué said, around collaboration on matters including counter-terrorism, cyber security, foreign interference and border management. The five countries promised they would gang up to deal with any "severe foreign interference incident". On encryption, the statement declared that while "The five countries have no interest or intention to weaken encryption mechanisms", there is an "urgent need for law enforcement to gain targeted access to [encrypted] data".

With a new global economic crisis shaking up the political spectrum, the possibility has never been greater that rebellious voters can force policy changes that will take power away from the City of London and Wall Street Establishment. It is clear that the myriad of new police-state powers are intended to provide the means to suppress democratic revolts that threaten the Establishment.

Don't let the Five Eyes spy on you!

By Elisa Barwick

If the Australian government's latest anti-terror bill passes, sometime in the not-too-distant future you could find yourself unwittingly relaying a trail of personal information and your day-to-day activities to Australia's security agencies. And you would be none the wiser. The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 will allow spy agencies like the Australian Security Intelligence Organisation (ASIO) to hack into your electronic devices, by making app or software providers, chat rooms and the like re-engineer your programs, allowing them to bypass encryption protocols without your knowledge. And that is just one of the new mechanisms these agencies will have to spy on you. (Read more in "Home Affairs encryption bill: A political tool made in Britain", *AAS* 5 Sept.)

Of course we are assured by the government that the new provisions are intended only for "criminal syndicates and terrorists" and that there will be "robust safeguards" in place to prevent their misuse. The rush to pass the bill with as little scrutiny as possible, however, indicates otherwise.

The bill was released to the public on 14 August and tabled 20 September. In a brief consultation period after the draft bill's release, 15,000 submissions were received. Once tabled, the bill was referred to the Parliamentary Joint Committee on Intelligence and Security, but only a three week submission period was scheduled. Why is the government in such a hurry to ram this through?

In his 20 September speech introducing the bill to parliament, Minister for Home Affairs Peter Dutton admitted that "The bill provides law enforcement agencies with additional powers for overt and covert computer access. Computer access involves the use of software to collect information directly from devices", he said. But, he insisted, it is "not a new vehicle to collect personal information".

Dutton claimed the security agencies' lack of access to encrypted communications presents a significant barrier to combating national security threats. The uptake of "encrypted communications platforms by criminal and terrorist groups has been sudden. It represents a seismic shift…." This has interfered with ASIO's ability to spy, he reported.

A Five Eyes play

The legislation did not emerge out of thin air—it is a copy of a UK law passed in November 2016, the *Investigatory Powers Act* (IPA), a.k.a. the "Snoopers' Charter". The Australian bill contains a variation of the UK bill's mechanisms: technical assistance notices which compel service companies to provide assistance, and technical capability notices which require a company to take reasonable steps to develop and maintain a capability to respond to security agency requests.

The UK law allows companies to violate existing laws in order to comply with the notices, and it has been suggested that agencies could compel not only internet service providers, email servers and telcos, but any organisation, from a business to a hospital or political party, to collect information on behalf of the government. The UK Parliament is currently debating another new law, the Counter-Terrorism and Border Security Bill 2017-19, which former MI5 officer Annie Machon has described as a move towards a "techno-Stasi state". Under the legislation, classified information would be shared with the private sector, councils, schools or social workers to enhance spying capabilities. Another provision would allow police to close the entire "Square Mile" City of London banking centre to foot and vehicular traffic in the event of an emergency, terrorist *or economic*. ("'Techno-Stasi' police state laws before UK parliament", *AAS* 27 June.)

Australia has been a leading nation in the Five Eyes' push for a new standard of state-secrecy to prevent so-called foreign interference, with the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* passed on 28 June. Upon its passage, independent federal MP Andrew Wilkie warned that Australia is a "pre-police state"; but the Five Eyes spying alliance, comprising the USA, UK, Canada, Australia and New Zealand, has even bigger plans. As Home Affairs Secretary Michael Pezzullo revealed prior to the Five Country Ministerial meeting held 28-29 August on the Gold Coast, the Five Eyes countries are pushing for a global police-state capability, with a "transnational model of security". ("Five Eyes plan global police state", *AAS* 22 Aug.)

The real agenda is also betrayed by the fact that British authorities have freed 500 terrorists from prison since the 11 September 2001 terrorist attack in the USA; increasing to approximately one per week over the year to March 2018. Despite the relentless wave of new anti-terror laws, the government claims it is powerless to stop these releases. In reality, it is well documented that British security services have maintained a covenant with terrorists, allowing them to operate from the UK. ("Why is British intelligence letting loose convicted terrorists?", *AAS* 19 Sept.)

Terrorism and foreign interference are being used as pretexts to implement police-state controls that will be used to protect establishment interests, as the economy sinks further into crisis and the population revolts against measures such as "bail-in" laws that will seize the savings of ordinary people to prop up the failing financial system.

Opposition to the bill

The proposed Australian powers are broad and will be exercised in secret, so there can be no real oversight outside of the agencies deploying them and the Attorney General's department. The penalty for citizens disclosing information about operations is five years' imprisonment; for not complying with an assistance order, 5-10 years! This is an effective weapon against potential whistleblowers. We already have the example of "Witness K"—the former Australian Secret Intelligence Service officer facing two years in prison for rightly exposing how the Australian government spied on the East Timorese cabinet during negotiations over an oil and gas treaty in 2004.

The brief period of feedback for the draft bill, though not advertised, attracted a great deal of criticism. Of the 15,000 submissions, 14,300 were generated by a Digital Rights Watch campaign, which is indicative of the public dissent. The Australian Human Rights Commission exposed the "breadth of the powers, the ambiguity of certain provisions and the inadequacy of effective safeguards"; Australian Lawyers for Human Rights said the Bill seriously impinges on human rights and "limits the presumption of innocence by allowing covert access to personal communications and criminalising the refusal to share one's passwords".

Human Rights Watch said the Bill would set a dangerous precedent worldwide and that its ambiguities and broad powers could introduce "widespread security vulnerabilities", a concern also raised by the Australian Industry Group, the Communications Alliance and the Digital Industry Group. The Labor Party slammed the "sham" consultation process and the rush to table the bill within ten days of submissions closing.

Submissions to the Parliamentary Joint Committee can be made at www.aph.gov.au/Parliamentary_Business/Committees/OnlineSubmission by noon on 12 October.