THE REGIONALIST
INSTITUTE FOR REGIONAL SECURITY

COMBATING THE SCOURGE OF RADICALISATION THROUGH TECHNOLOGY

Marissa Price

Key customers: *Australia-New Zealand Counter-Terrorism Committee; Australian Federal Police (Counter-Terrorism Division, National Disruption Group, Diversion Group, Community Liaison Team, Capability Development, Online Operations Team, Terrorism Finance Investigation Unit, Prisons/High Risk Terrorist Offenders)*

Australia must develop ways to combat online radicalisation to avoid depleting its human capital and mitigate risks to internal security. Federal laws preventing born and naturalised Australian citizens who fight in overseas conflicts from returning to the country are a start that we can build on to create a safer Australia. To protect Australians, the Government must recognise that not all citizens and residents who are radicalised travel overseas, and not all support for jihadism and insurgencies is physical.

A huge increase in the availability of smart devices after 2010 has afforded radical recruiters greater access to potential targets across the globe. A particularly vulnerable demographic are Australian children and teenagers, who are increasingly susceptible to the influence of overseas recruiters through their extensive engagement with online media. Utilising a variety of departments, including the defence, innovation and education portfolios, is important in developing a holistic, targeted approach against online recruiters.

CHALLENGES TO THE SECURITY OF ADVANCED NATIONS

Modern technology has brought challenges to Australian security into stark relief. In an interconnected world, extremists are increasingly employing cyber-methods to radicalise individuals in advanced nations. Having radical views is not a new phenomenon but having access to a global platform from which to spread those views is. As a result, private enterprises and public sector agencies have been conducting a great deal of research into information security. Some breaches of security, such as industrial espionage, have been modernised by technology. While these crimes are not new, perpetrators are carrying them out at an increasing volume and speed. Moreover, such cybercrime can be more difficult to detect and trace than its pre-digital antecedents. The Australian Government and interest groups has rightly focussed on the effects of cybercrime on our economy. However, in comparison to the attention on industry security, the investment into research assessing the influence of cybercrime on our communities, including the processes of radicalisation, has not yet been realised. Understanding how and why individuals succumb to radicalisation is important for our political leaders, so that the most effective and responsive policies and legislation can be created.

Radicalisation is a very personal process. The emotional link between the target and the recruiter (or the extremist organisation) is essential to ensure the target's investment in radical activity. Various countries have attempted to profile the characteristics of populations vulnerable to recruiters. But these techniques have been proven to be flawed because understanding the various conditions that can cause an individual to engage in radicalised conduct is difficult and highly variable. There is little to enable an expert to determine a pattern and therefore be able to predict future behaviour.

UNDERSTANDING CHANGES TO RADICALISATION TO INFORM FUTURE IDENTIFICATION AND DE-RADICALISATION POLICY

Prior to the September 11, 2001 terrorist attacks, the general public in developed nations were less accessible to online influencers. News media was available through traditional television and newspaper sources and the 24-hour online news cycle was not yet popular with mass audiences. The reality of jihadist wars did not greatly impact Western civilians, especially in countries such as Australia, which were not situated in conflicted geographical locations. Pre-9/11 radicalisation efforts were constrained to local area recruitment in conflict regions and typically targeted teenagers and young people. Radical

thoughts and activities were passed down through families and acquaintances from one generation to the next.

Developments in digital telecommunications technology across the 2000s significantly increased jihadist's reach in recruiting. An increase in the visibility of violent jihadists altered the way the world viewed their latent power and influence. The 9/11 attacks catapulted terrorism onto the world stage and into the policy considerations of every industrialised nation. Although the main method of communication remained major newspapers and nightly news bulletins until the rise of social media, ordinary citizens could not avoid the implications of 9/11 upon their own lives. Every time they boarded a plane, posted a package or filled out an identity document, the effects of the 9/11 attacks on domestic security policies were on display.

Coinciding with the 9/11 attacks and their psychological aftermath was a significant proliferation of powerful mobile devices. These devices enabled the user to access constant news streams, to see photographs and stories from around the world and to communicate with a range of people in different countries. Research on radicalisation accelerated in 2004 as jihadists linked with Al-Qaeda replied to the 2003 American intervention in Iraq. The 2005 London bombings raised political and popular attention on home-grown terrorism. Radicalised individuals weakened their own countries from within with little or no material support from foreign terrorists.

The two phases to terrorism – first radicalising and then turning to terrorism – are separate from one another and should be treated as such. Not all individuals who express radical thoughts participate in acts of terrorism. And not all people who are terrorists are Muslim. At times, it would appear as though we are looking in the wrong places for the threat that we perceive to be imminent. A shift in paradigm is necessary to remove the misconception that religious faith alone is a pre-determinate factor of radicalisation. By actively trying to limit instances of flawed and inflammatory political rhetoric, our government reduces the risk of its citizens becoming vulnerable to radical recruiters. Ordinary people sympathise with what they see as mistreatment of individuals within their own country, perpetuated by the constant news cycle, articles and opinion pieces that are often driven by their own political agendas. This can be seen in examples such as the "I'll ride with you" social media movement, where everyday Australians pledged to sit with Muslim travellers who feared for their safety on public transport. The

Australian government needs to actively avoid playing into the plans of recruiters by making comments that act to segregate individuals within our multicultural society and influence citizens to act in a prejudiced manner.

The propagandist materials offered by recruiters to potential converts are exaggerated and amplified in a focused attempt to influence the thoughts and feelings of their targets. Generally speaking, this is not enough for radicalisation to occur. In addition, an element of altruism is usually required before an individual will radicalise: the individual must feel that something should be done about an injustice before they are willing to invest in it. Terrorist groups are much like any other group in that a sense of belonging and reciprocity is essential for it to function effectively. As a result, individuals often join terror cells because their friends are already part of one or because they wish to befriend those who are included. Once included into these cells, individuals will obey the commands of senior figures to remain a part of the cohesive unit.

By drawing on elements of psychological practice, we can identify individuals at risk of radicalisation through using a defined list of characteristics drawn from profiling research, and thereby attempt to circumvent these dependent relationships from forming. We can use the knowledge of how individuals are radicalised to dismantle symbiotic relationships that have already formed – essentially 'de-programming' jihadists, especially teenagers. The final trigger for radicalised individuals to act on jihadist intentions is usually not related to the group at all. The trigger can be something as seemingly innocuous as lack of employment, environmental factors, social events, discrimination or a significant loss. Our job is to circumvent that process before the final trigger occurs.

When you consider recent studies on Australian teenagers engaging in radicalisation, a pattern emerges. It does not matter whether the individual was both into the Muslim faith or not: they will participate in radicalisation if they are enticed to do so. Many returnees reported that they felt a great deal of empathy with Muslim minority members who may have experienced discrimination and hardship, usually at the hands of Western governments. Radicalisation is an intensely personal process, and emotions must be triggered within the individual to ensure that they will carry out acts of violence in support of the people they see as their friends and family, who have carefully cultivated the image of government oppression.

When our government uses practices such as racial profiling that supports the illusion of oppression towards a minority group, there is potential for this image to be intensified. For this reason, when Australian security agencies engage in profiling, they should have strict frameworks and accountability mechanisms to ensure that they are not inadvertently creating a rhetoric that marginalises particular groups within our society. The hard-line approaches of identifying and reversing the effects radicalisation should be paired with a softer approach, with the emphasis on the prevention of radicalisation in the first instance.

Using existing frameworks to protect Australian children from online recruiters and influences

Children and teenagers are particularly vulnerable to online recruiters. These groups are cognitively and emotionally immature and vulnerable compared to adults. The rise of online technology makes the vulnerability of these groups alarmingly easy to exploit. Young people searching for their own individuality and identity are vulnerable to the influence – good and bad – of others, including radical groups. The allure of jihadi groups is that they create strong loyalty and solidarity among their members. The uncensored internet can easily expose a vulnerable individual to radicalising propaganda and to others who share these beliefs.

Monitoring and assessing modern technology use by children and adolescents is an important area of focus for Education Departments across Australia, because protecting young people online is greatly challenged by their ability to access anything on the internet. The combination of immaturity, increased access and sustained contact means adolescents absorb information without thinking critically about it, especially teenagers who are experiencing other social, emotional and physical issues. While well-balanced, socially successful adults have the ability to filter information, adolescents do not possess the same skills. The insidious issue of cyber bullying has parallel features and consequences to online radicalisation. Children can access an incessant cycle of information through the use of instant messaging, communication apps and photo sharing. In Australia, students are legally able to leave school at the end of year 10 or the age of 15, whichever occurs earlier. This age is far too young for students to be able to determine how to act appropriately in a world they are yet to understand. Students who leave school early are generally more disposed to vocational outcomes, but they also suffer disproportionately from difficult home circumstances and generally

struggle throughout their schooling lives. When they leave this environment, the supportive structures surrounding the student also disappear and they are then vulnerable to external influences, including radical individuals. As a primary recommendation, students who opt to leave school before the conclusion of Year 12 should be flagged as vulnerable individuals.

It must be noted that it is dangerous to create any public discourse that turns violent extremists into victims, given that they commit acts of terrorism against innocent citizens. However, given the present political and public climate in relation to terrorist activity, achieving such an outcome would be difficult. Initiatives in the US and UK, such as Preventing Violent Extremism and the PREVENT program as a strand of the wider CONTEST strategy, have all drawn criticism from the wider community for the way that they attempt to change the discourse around who and what creates a terrorist. These programs have an intense focus on religion, and at the core they target Muslim populations making their way into the US, Europe and Britain. It is essential for Governments to change the framework for action away from a religious focus. It is interesting for Western Governments to note that the primary British response to unrest and politically motivated violence in Northern Ireland oscillated between criminal deterrence and positive prevention, depending upon the government of the time. Religion was largely downplayed in this extended conflict, because it involved Anglo-Saxon groups of terrorists – not Muslims.

Programs that already exist within Australia can be used by Education Departments as a framework for change in this area. Government initiatives dealing with cyberbullying, such as the e-Safety Commissioner, provide appropriate resources for educational facilities and parents that deal specifically with their role in a young person's life. These resources are all based around the emotional and practical impacts of bullying and cyberbullying, delivered through a series of videos designed to appeal to their target audiences – teens and young adults. These clips are short, emotional and get straight to the point. They encourage students to report instances of abuse and breaches of law. This would be an excellent framework for police services to expand to include online radicalisation processes in an effort to protect the safety of individuals online. In the same way that the e-Safety Commissioner currently aims to make students and families safe from bullying and cyberbullying, the Commissioner could also provide resources and information to protect those same families from recruiting experts. Both of these issues rely on inclusion and emotion. Recruiters are successful when young people are without effective support

networks or when they feel emotionally or physically isolated. The same principles apply in these situations, and the research, Government policy and development put into combating bullying can be used by all identified departments and organisations to combat radicalisation, in the case of young Australians.

Australia must develop ways to neutralise online radicalisation to avoid risks to internal security. By combining a 'hard' strategy of identification and de-radicalisation with a 'soft' strategy of prevention and harm minimisation, Australian policy makers can circumvent the efforts of radical recruiters. Using existing Australian frameworks and legislation, such as the Office of the e-Safety Commissioner, research and program implementation to address radicalisation can be streamlined with work around bullying and cyberbullying to create an effective solution to the effectiveness of online recruiters.