AIR SPACE
ASPC's crowd-sourced blog
https://airpower.airforce.gov.au
Parker, E. (2023) Air/Space 2, bp35020368
Date Published: 6 September 2023

Is the Australian society ready for mass information warfare?

Elliot Parker
Australian Defence Force

Personal data is a significant component in information warfare and Australians must take ownership of their personal data to be resilient against adversarial influence and information operations.

Attacks are increasingly prevalent within the cybersecurity realm, and their impact extend throughout the community (Bonyhady, 2022) – in private and governmental institutions. Australia is still recovering from six major data breaches within a span of five weeks (Thompson, 2022), targeting major Australian companies such as Optus, Woolworths, Telstra, Costa Group, Dialogue, and Medibank, and Latitude. For clients of some of these companies, a significant portion of their sensitive personal information has been released online and sold for profit.

These vulnerabilities are consequences of the internet becoming more prevalent in our everyday lives and an increasingly connected society. We have become reliant on technology as our primary source of information and communication. This reliance can been exploited by state or non-state malicious actors, not only for profit but also to degrade society's ability to collaborate for national defence in times of conflict. Hence, everyone's personal data is a significant component in information warfare. To increase resilience, Australians and the whole society must take ownership of their personal data. Moreover, educating the society on the impact of these vulnerabilities and changes in cultural practices are necessary to increase resilience and minimise the fallout from cyber-attacks.

Personal data refers to any information regarding an individual that can be attributed to them. It may describe their interests, family connections, work, or beliefs/affiliations, amongst other information. Personal data is important to develop an effective information campaign, as it allows for an actor to better understand individuals, their vulnerabilities, and how they can be targeted and exploited.

Information Operations

Information operations involve the collection of physical or digital information about an individual or group as well as the use of such information for dissemination that intend to directly influence views and behaviours. While traditional 'kinetic' warfare similarly intends to influence or coerce, information warfare can be differentiated through operations in the information space (Garman, 2021). For example, 'airdropping' pamphlets out of an aircraft (Central Intelligence Agency, n.d.) to encourage a military to stand down or inserting 'fake news' within social media (Lee, 2020).

Historically, effects based on individualised information and targeting a group were mutually exclusive. Now with the mass amounts of personal data on social media, open-source intelligence (OSINT) can be enhanced to improve an operator's awareness of the targets' information. In addition, vulnerability of personal and private data via cyber-attacks have given malicious actors the ability to enhance their approach and craft more believable information.

Access to personal data allows an information operations actor to understand how to best influence their target, enabling individualised targeting at a mass scale. This access also allows for deeper profiling of individuals to better group and target vulnerable micro-demographics such as oppressed, minority, activist groups, or key high-stake individuals such as defence personnel, community leaders or those working for the government. Attributes such as levels of power or access to sensitive information can be exploited.

Social media already offers an incredible service to advertisers. With the free nature of social media, users are enticed to sign up for connectedness without understanding the true cost of exposing themselves to information operators. Given the amount of information shared, the engagement of different types of media, and their connections, advertising companies can also target micro-demographics to maximise the effectiveness of advertising. Individualised advertising can influence users to feel an artificial need for a product, and use psychology to make them impulsively act on this, rather than stop and think. Cambridge Analytica is an example of this in practice (Lewis & Hilder, 2018).

How will this be used?

Within the context of national defence and whole-of-government picture, information operations transform into information warfare, where adversaries seek to degrade society's ability to collaborate for national defence. Information operations might precede and support a kinetic attack, which can be in a form of an attempt to scatter the population (Jenkins, 2023) and distract key or high-stake individuals mentioned earlier through threats or misinformation (Berthiaume, 2015).

Historically, Operation MINCEMEAT in World War 2 was a plan conceived by the British Intelligence to deceive and confuse Axis forces on the true target for the Allied invasion of Sicily, misleading key decision makers to focus forces away from the real landing point (Imperial War Museum, n.d.). When applied to contemporary settings, personalised data allows for an adversary to target high-stake individuals in national defence and decision making to degrade and overwhelm intelligence and news mediums in order to confuse the narrative and distract from the main effort (Arceneaux & Harman, 2021). Social media alone has proven to be an effective tool to exacerbate the spread of misinformation in conflict zones (Bacio Terracino & Matasick, 2022), which alongside news manipulation can sway the narrative to confuse what is happening in a conflict and why it is even occurring (Wilbur, 2021). When information warfare is in effect, high-stake targets will be pre-occupied and will reduce their ability to make decisions and focus on national defence thereby increasing the vulnerability to allow for physical forces to attack with less resistance.

Either way, it's clear that information warfare will be more prevalent in geo-politics and future conflict, and personal data will continue to leave individuals vulnerable to exploitation and influence.

How can we prepare our society?

Unfortunately, the general response from recent data breaches seems more like annoyance rather than a realisation of the vulnerability of the information space. Whilst responsibility lies on organisations to improve cybersecurity defences and incident response, it is clear that cultural change is required to protect our society against adversarial influence and information operations. This can be achieved through education on cybersecurity awareness (Arceneaux & Harman, 2021), as well as providing resources to help individuals more easily take ownership of the amount of personal information they disclose online.

Services such as news, cloud, and other niche utilities have often been the victim of data breaches through poor security practices or simply their scale of data collected. As a society, we need to be more considerate before sharing information or registering for a service online. If the service is free, we are probably the product and we need to be aware of our 'digital

footprint'. While most legitimate organisations do not collect personal data for unethical gain, their systems are still vulnerable to attackers. Hence, we need to be aware of the amount of data shared, where it's stored, the legitimacy of the site and organisation, and if there are any connections to foreign influence (Baker-White, 2022). We need to always assume that computer systems of organisations are not fool proof. Such system can be compromised, and it is therefore important to educate individuals to take ownership of their personal data. Perhaps a counter-intuitive way to achieve ownership is by anonymising their digital footprint where possible. This could be through a pseudonym or completely anonymous and random email and username. In the event of a data breach, the anonymised information would be harder to attribute than consistent email addresses and usernames across multiple sites and as such less valuable.

Following basic cybersecurity principles will also create a more educated and resilient society. This can be achieved through normalising encryption when communicating with others via end-to-end encryption in mobile phone applications such as *Signal* and *Google's Rich Communication Services* (which also uses the Signal encryption protocol). It is important to note that interacting across the internet has already come a long way with the normalisation of Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption for HyperText Transfer Protocol Secure (HTTPS) web transfers. These make intercepting data as an attacker-in-the-middle much more difficult, through obfuscating the data while in transit to its intended recipients.

The best defence to an information campaign is a society that is educated on how to detect misinformation and influence as well as individuals taking ownership and consideration of what they consume online. The majority of misinformation spread across social media is spread by other individuals (not bots) (Vosoughi, Roy, & Aral, 2018). If individuals are aware that something is trying to influence them, they are able to consciously stop it.

While it is unlikely that a large shift can occur across the broader population's cybersecurity awareness quickly, it's possible to achieve a general awareness of personal data being second nature for those who have an online presence. For this to be possible, there must also be responsibility on organisations and services to uphold their obligations to data security – for example, Telstra's developments in SMS spam/scam filtering (Penn, 2021) as well as more discussion around the issue in media, government, and individuals. For national defence specifically, organisational awareness training and cultural change to expand upon existing physical security practices can effectively develop a better understanding of data security.

Conclusion

Information Operations are becoming more prevalent in society, and modern reliance on the internet poses a threat of misinformation and influence. As such, greater education and awareness of how personal data can be exploited is important to building a more resilient society.

References

Arceneaux, P., & Harman, M. (2021). Social Cybersecurity: A Policy Framework for Addressing Computational Propaganda. *Journal of Information Warfare, Vol. 20, No. 3, Summer 2021*, 22-43.

Bacio Terracino, J., & Matasick, C. (2022, November 3). *Disinformation and Russia's war of aggression against Ukraine*. Retrieved from Organisation for Economic Co-operation and Development: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

Baker-White, E. (2022, October 20). *TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens*. Retrieved from Forbes:

https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=3541390b6c2d

Berthiaume, L. (2015, March 14). *Military intelligence warns of terrorists harassing Canadian Forces personnel, families online*. Retrieved from Ottawa Citizen: https://ottawacitizen.com/news/politics/military-intelligence-warns-of-terrorists-harassing-canadian-forces-personnel-families-online

Bonyhady, N. (2022, October 30). *There's a reason you're hearing about so many hacks*. Retrieved from The Sydney Morning Herald: https://www.smh.com.au/technology/there-s-a-reason-you-re-hearing-about-so-many-hacks-20221027-p5btmi.html

Central Intelligence Agency. (n.d.). *Persian Gulf War Leaflets*. Retrieved from Central Intelligence Agency: https://www.cia.gov/legacy/museum/artifact/persian-gulf-war-leaflets/

Garman, L. (2021, October 06). *Information warfare, an immediate threat*. Retrieved from Defence Connect: https://www.defenceconnect.com.au/key-enablers/8859-information-warfare-an-immediate-threat

Imperial War Museum. (n.d.). *What was Operation Mincemeat?* Retrieved from Imperial War Museum: https://www.iwm.org.uk/history/the-war-on-paper-operation-mincemeat

Jenkins, B. M. (2023, April 17). *Stalled in Ukraine, Kremlin Increasingly Turns to Political Theater*. Retrieved from RAND Corporation: https://www.rand.org/blog/2023/04/stalled-in-ukraine-kremlin-increasingly-turns-to-political.html

Lee, J. M. (2020, October 26). *How Fake News Affects U.S. Elections*. Retrieved from University of Central Florida: https://www.ucf.edu/news/how-fake-news-affects-u-s-elections/

Lewis, P., & Hilder, P. (2018, March 23). *Leaked: Cambridge Analytica's blueprint for Trump victory*. Retrieved from The Guardian: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

Penn, A. (2021, November 29). *We're taking action to block scam SMS messages*. Retrieved from Telstra Exchange: https://exchange.telstra.com.au/were-taking-action-to-block-scam-sms-messages/

Thompson, M. (2022, October 21). *Six major data breaches in five weeks: So why are so many Australian businesses still on the fence about their cyber security?* Retrieved from LinkedIn Pulse: https://www.linkedin.com/pulse/six-major-data-breaches-five-weeks-so-why-many-still-marcus/

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146-1151. doi:10.1126/science.aap9559

Wilbur, D. S. (2021). Propaganda or Not: Examining the Claims of Extensive Russian Information Operations within the United States. *Journal of Information Warfare, Vol. 20, No. 3, Summer 2021*, 146-156.