Tac Talks

Issue: 03 | 2021

THE WEAPONISED INFORMATION THREAT TO COGNITIVE SECURITY

By LEUT Richard Morris

Introduction

In a friendly port in the not-too-distant future a young frigate sailor scrolls through his smart-phone. He is about to get underway on a patrol in a sensitive and potentially hostile area and wants to hear from home before he loses connectivity for a month. On this occasion, however, instead of seeing updates from his friends back home, the sailor's news feed is bombarded with dramatic images that he can scarcely believe.

An artist's impression of a ballistic missile attack (Source Xinhua)[1]

His homeport has been struck by ballistic missiles, causing catastrophic destruction and loss of life. Amongst the smoking wreckage of the buildings that he once called home, he recognises the dust-caked face of a friend. The image sears in his brain with shattering finality. The enemy has struck first, employing surprise and overwhelming firepower. His little frigate is likely to be next.

Except the attack did not happen. It never happened. The images that the sailor saw were fabricated. The video files were high resolution CGI. The sailor's face he recognised was a 'deep-fake'– a computer generated image indecipherable from real-life video footage. The feed that he viewed was propagated by a horde of artificial-intelligence social media 'bots' unleashed by the adversary then re-tweeted by friendly, reputable sources. It was a 'weaponised information' attack. The enemy initiated it in order to disrupt its target's personnel movements, exploit and observe its communications and test and evaluate its resilience to deception.

In the age of smart-phones and social media, our digital presence is intertwined with our identity. For many, our smart-phones are the tool by which we obtain our news, understand our environment and make the observations which form our reality. This human-machine interface has created a medium, however, which is highly vulnerable to manipulation by powerful state and non-state actors.

Weaponised Information

'Weaponised information', or 'cognitive hacking' is that which is designed to provoke or mislead in insidious or destructive ways.[2] The core principles of the theory, deception, ideological subversion and psychological manipulation, are as old as warfare itself. The digital age however, with its machine-learning and big data exploitation, has supercharged their destructive capabilities.[3] IBM

estimates that 2.5 quintillion bytes of data is created on the internet every day. [4] It is an ever-expanding exploitable database of personal information, social networks and allegiances. It is a big-data set that has historically out-paced the grasps of human capacity to exploit.

Members of No. 462 Squadron partake in Exercise Pink Pill - a Defensive Cyberspace Exercise.

Recent developments in artificial intelligence systems, however, indicate that 'social engineering' is becoming increasingly achievable. The innovation in big-data exploitation is being driven by the free-market internet. Algorithms are already telling us what clothes to buy, what food to eat and what content to watch. Every time we interact with it, we are feeding the 'digital beast' more data. The 'arms race' for the next digital information war is happening right now and we are unconsciously building the arsenal for our future enemies.[5]

'Weaponised information' likely forms one component of a 'three-dimensional' cyber campaign for a potential adversary - physical, informational and cognitive.[6] US Cybersecurity Officials disclosed to the State Intelligence Committee in 2019 that Russian hackers successfully penetrated voter registration databases in multiple US states in 2016 and almost certainly stole valuable voter data.[7] With the physical and informational components successfully exploited, Russian military and civilian propagandists weaponised this data and turned it against the mind of the US voter. More recently, the tools of 'weaponised information' have proliferated to non-state actors. There are reports of 'troll-farms' in the Philippines, where firms offer perception manipulation via social media to anyone who is willing to pay.[8]

A recent research paper from the University of Oxford concluded that 'The manipulation of public opinion over social media platforms has emerged as a critical threat to public life.'[9] The study

detected organised social manipulation campaigns in at least 48 nations. As nation-states have realised the threat of weaponised information, they have sought attack as the best means of defence. The numbers of social media manipulation campaigns increased by 170% in 2017.[10] Already, weaponised information has proved capable of heightening ethnic tensions and intensifying political conflict while simultaneously weakening public trust in the organisations which are considered central to a modern democratic state – a free press, integrity in leadership and fair elections.[11]

If this is what 'weaponised information' can do in a time of relative peace, what could a fully enabled state actor do in a time of armed conflict? The aforementioned example is crude and easily identifiable. It is effective but only for a short-term effect. A blunt instrument, it could in-fact have a detrimental impact for the enemy, by galvanising and alerting the friendly fleet before the real kinetic weapons are sent down-range. A more concerning and effective campaign would be insidious and slow-burn, making detection and interdiction a challenge.

Hypernudging

'Weaponised information' savvy academics call this 'hypernudging', where algorithm driven 'decision guidance' programs alter a victim's behaviour in ways which are dynamic, pervasive but non-detectable.[12] 'Hypernudging' has already been alleged to have contributed to cases of lone-wolf extremism by creating digital 'ecosystems of hate' whereby disenfranchised youth are presented with increasingly hostile imagery by algorithms on streaming websites.[13] Its alleged employment in recent conflicts has coined the term 'hybrid warfare', where an adversary's aggression appears un-attributable, with unrest driven by a vocal but invisible majority.[14] Our digital consumer preferences, one could argue, are already driven by these invisible decision-shaping forces.

The 'weaponised information' threat presents a great challenge to the Australian Defence Force. It falls across multiple pillars and disciplines of Information Warfare (IW) – cyber, information effects, psychological operations, targeting analysis and intelligence. Some analysts believe that the threat justifies a new discipline of IW – cognitive security. As technology develops and the threat materialises, the means of best practice for cognitive security will probably be defined.

In the naval context, however, it is clear that the threat cannot be completely mitigated by simply switching off satellite connectivity or disabling wi-fi. States have tried this, only further inflaming the perceptions to which they were attempting to suppress.[15] Even the smallest idea in an information starved environment can create vicious rumours and discontent. Rumours frequent an operational warship even without deliberate deception.

Thinking Navy

What research that does exist suggests that the best defence is in the mind of the individual.[16] The digital sailor must be equipped with skills in critical analysis and rational thinking, in order to question the objectivity of their daily 'feed'. However, noting 'weaponised information's' potentially insidious and undetectable nature, that measure is only the last-line of defence. Organisations could also conduct intermittent surveys of perceptions in order to gauge subtle shifts which could indicate manipulation. The final strategy is the most dangerous – to disrupt the disruptors, by seeking out and eliminating or discrediting the information source to which the attacks are generated. This 'fight fire with fire' approach, however, potentially threatens the key values of integrity and honesty which are integral to the legitimacy of our profession.

Until a whole of government strategy against 'weaponised information' materialises, operational-level leaders will bear the weight of ensuring that their personnel are aware of the threat of 'weaponised information' and are appropriately prepared and equipped to defend themselves. In the next war of the not-too-distant future, it is likely to be the enemy's first salvo.

LEUT Rich Morris is the Staff Officer – Intelligence (N2) of the Australian Maritime Task Group.

End Notes

[1] 'China Responds with Renewed A2/AD Missile Tests', *Defence Connect,* 15 Jul 2019
[2] Ignatidiu, Sophia, 'The weaponisation of information is mutating at alarming speed,' *The Guardian*, 19 Aug 2019
[3] 'Combating weaponised misinformation: the Future of Risk in the Digital Era', *Deloitte*, 2019
[4] Ignatidiu, Sophia, 'The weaponisation of information is mutating at alarming speed,' *The Guardian*, 19 Aug 2019
[5] 'Armed and Ready: How big data is being "weaponised" against you.' *Wired*, 2018
[6] 'Hackers target third-dimension of cyberspace: users minds', *Live Science*, 31 Jul 19
[7] 'DHS Cybersecurity Chief: Russia "Successfully Penetrated" some state voter rolls', *The Hill,* 02 Jul 17
[8] 'Why crafty internet trolls in the Philippines may be coming to a website near you', *The Washington Post*, 2018
[9] 'Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation,' *Algorithms, Automation and Digital Politics*. 20 Jul 2019 ,
[10] Ibid.
[11] Ibid.
[12] 'Hypernudge': Big Data as a Mode of Regulation by Design', *Information, Communication & Society*, 2016, 1,19
[13] 'How Youtube radicalised Brazil', *The New York* Times, 11 Aug 19,
[14] 'Hybrid warfare: the new conflict between east and west' *BBC news,* 06 Nov 2014
[15] 'India Shut Down Kashmir's Internet Access. Now, "We Cannot Do Anything," *The New York Times*, 14 Aug 19
[16] 'Combating weaponised misinformation: the Future of Risk in the Digital Era', *Deloitte*, 2019