Active Measures:
The Secret History of Disinformation and Political Warfare

Thomas Rid

London: Profile Books, 2020, 513 pp, £10.99

Colin Challen

The dissemination of disinformation is as old as the hills, and now, thanks to the Internet, its transformation from the analogue age to the digital has given it what Rid explains as a post-modernist persona. Active Measures (AM), that is using disinformation as a political weapon, has evolved into something akin to a quantum uncertainty principle, which makes normal measured evaluations of it impossible. The idea is to make one's target (or victim) question previously trusted authorities, to cease to be sure about anything and to trust no-one who fails that simplest test of agreeing with everything you say. You can only know something is true if you already believe it is true. Evidence can be falsified after all, as in the Trump assessment of the photographic evidence of a presidential inauguration turnout. Or you can say 'there are alternative facts'.

The question I asked myself, reading Rid's book, is whether we have entered a *qualitatively* different world of disinformation, or is it merely that the Internet has aided a *quantitative* explosion of disinformation? It might be a case of both, although Rid's chapters devoted to the Russian (in theory non-governmental) Internet Research Agency (IRA) suggest that efforts by Russians to influence the US elections of 2016 were largely unsuccessful because of a lack of quality, as well as quantity. The young Russians employed on the job had low morale, worked on long, demanding shifts and didn't assess the impact of their work. Impacts can be difficult to measure. Are 'hits', 'likes' and 'shares' real impacts or merely signs of preaching to the converted without changing voting intentions? Rid writes:

> 'On Twitter the IRA's impact practically vanished in the staggering number of election-related tweets. Approximately 1 billion tweets related to the campaigns were posted during the fifteen months leading up to the election. The St Petersburg troll den generated less than 0.05 percent of all election related posts. The IRA, according to the data released by Twitter, boosted candidate Donald

> Trump's retweet count with only 860 direct retweets over the entire campaign.' (p. 407)

Taking the IRA at face value, it is clear it sought to influence the election, but had no reliable means of knowing if it had done so. It's not as if they could do a post-election opinion poll asking people if they were influenced by the Agency's work; by the nature of things the work was concealed. Perhaps new techniques will be developed to track the impact of disinformation on target audiences; but those methods, too, would have to remain invisible and untraceable.

There is certainly a lot more disinformation in cyberspace, and it can be generated from any source: from a teenager in a bedroom to a staffed agency with hundreds (or thousands) of staff. Much of it I would not classify as a product of deliberate AM, unless one extends the definition of AM to all types of disinformation, not just those which are state sponsored. A malicious bad review on Trustpilot may be disinformation but hardly fits the AM definition. Nevertheless, if it helps to eliminate objectivity on the Internet, all such behaviour will provide an accommodating climate for state-led AM. Indeed, state AM actors may tap into general public complaints to hone their message for chosen target groups.

State AM actors will go to extraordinary lengths to conceal themselves as a source. It appears the IRA crowd weren't brilliant at this, and their failure to conceal their electronic trails was a gift to those who sought to exaggerate Russian interference in the 2016 election. However, a more serious case developed from the leaking of US National Security Agency (NSA) hacking tools which fell into the wrong hands – known as the 'Shadow Brokers' – in 2016. US intelligence sources thought there was North Korean as well as Russian involvement with what happened to the leaked tools which, when used by the miscreants, caused global damage estimated in the billions. I won't go into the details here, which read like the plot of a detective story. The important point for me is that leaks happen – even at the NSA – and material can be redeployed against you like so much military hardware. This raises several questions which, so far as I can see, have not been answered. Was it a leak or were the hacking tools stolen? Was there a mole in the NSA? Who was the NSA going to use these hacking tools against? Will the NSA explain what happened (not much chance)? Unfortunately, Rid doesn't really address these questions. Unlike a Sherman tank, cyber weapons can’t easily be pinned down at source.

As the Shadow Brokers case illustrates, AM can cause real harm; and clearly AM now covers a broader territory than simply spreading disinformation to selected human populations or groups. The definition of AM must also include the spread of disinformation between computers, with the intent to sabotage computer programs. Perhaps the most famous example of this activity went by the name of Stuxnet, which was developed by the US and Israel to damage Iran’s nuclear program in 2010. In 2022 we are told that Russia has and continues to wage an AM war on Ukraine. On both sides of the ideological divide, the militarisation of cyberspace is a priority. If only you could get your enemy’s cruise missiles to blow up in their launch tubes! (Somebody’s working on it. . .)

All this is a far cry from the first half of Rid’s book, which looks at AM from the turn of the twentieth century through to the Cold War. This has an almost nostalgic feel to it with, for example, the CIA’s use of balloons to carry bundles of leaflets into East Germany, or the distribution of a jazz magazine in the East with the hope it might help destabilise the Communists’ regimented society. I’m not sure there would be enough jazz buffs in any society to achieve such a thing, but you never know.

Rid has also written a book called *Cyber War Will Not Take Place* (2013). This is a subject which merits much discussion – and a search on the subject on the Internet provides some very interesting results. Whether cyber *war* can take place I think is a purely definitional problem, and it is an area where disinformation – active measures – and destruction could easily merge.

If I have one critical remark to make about Rid’s book it is that he generally writes from a Western perspective. So in the Cold War AM were used to upset totalitarian regimes. In the digital age it’s the nasty Russkies upsetting our harmonious democratic regimes. As the saying goes, there are other products available.

Colin Challen was the MP for Morley and Rothwell from 2001 to 2010. He blogs at <http://www.colinchallen.org>.