FROM THE ADOLESCENT BEDROOM TO THE CHIEFS OF STAFF: FAKE NEWS AND FUTURE WARFARE

Dr. Carl Miller
Research Director, Centre for the Analysis of Social Media, Demos

Strange beginnings

In 2003 a teenager called Chris Poole started an anonymous image board site named after a Japanese trend called 4chan. It was a remote, largely anonymous pocket of the Internet, and on it new feelings of identity and collectivity began to set its inhabitants apart from the mainstream. It grew quickly and soon millions of posts were flowing through the site, all of them impenetrable to anyone not steeped in the thickly woven layers of lore, slang, inter-board trolling, in-jokes and running feuds that each of the different boards on 4chan quickly developed.

This might be a strange place to start the story of Fake News, but it was on 4chan where the reality of Fake News today really started. For Fake News is not just people sharing incorrect things. It's the intentional creation and amplification of information with a grounding in human behaviour and psychology to change peoples' attitudes and beliefs. And it was 4chan who accidentally stumbled on it.

4chan saw companies, corporates, and 'normies' joining 'their' space in greater and greater numbers. They thought their internet was being invaded, and decided to launch a counter-invasion.

They began working out how to cause information to spread, how to grab attention, how to use the internet to influence the wider offline world. 4chan's boards began to fill with discussions of social engineering, psychological manipulation, and ideational diffusion, much of it taken from mainstream academic literature. They worked together, tested things, and began to find ways to use the internet to change what people saw and thought. They called it attention hacking, and used it for another invasion: using images of cats.

Attention hacking: proto-Fake News offensives

Part of 4chan's campaign of attention hacking was to use the internet to break into the mainstream media. They used an auto-voting programme that spread on 4chan to manipulate TIME magazine's online public poll to find the world's 100 most influential people. Chris Poole came first. They built fake social media accounts — 'sockpuppets' — to make certain hashtags trend and appear more popular than they were. They created fake websites that looked like the real thing, and manipulated search engine rankings to knock corporate websites off the front pages with their own jokes and forgeries.

Then there were the 'actions' where 4chan would swarm a target. In 2006, 4chan began a series of organised raids on the online game Habbo Hotel. Acting on rumours that moderators there were banning avatars based on their skin colour, they arrived en masse, blocking entrances and causing servers to crash. 4chan celebrated each victory with an endless deluge of shareable images ("memes") of cats.

4chan succeeded in what they set out to do. It wasn't really about cats; all of this was really about seizing and using attention and influence. Forgeries, spoofs, gaming, swarm-actions, manipulating search engines and memes were all part of a new body of techniques and skills that were forming. It was about finding ways of using the internet to become more influential, to change in controllable ways what people saw and even what they thought.

Cont...

The military get interested: UK, Russia, US

Others quickly began to copy and develop the techniques that 4chan pioneered. Political communications consultants brought attention hacking into political campaigns. Viral advertising agencies opened, and the murkier, more illicit side of online advertising sold search engine manipulation software to build bots and spam services.

Militaries can never stay out of questions of influence and they, like 4chan and advertisers before them, re-defined their professional art to put information at its heart. In 2014, a memo was sent across the British military entitled Warfare in the Information Age:

"The common theme" the memo states, "is that information-centric capability employed in information-centric operations can ameliorate many of the shortcomings of a reducing number of platforms and people." A new doctrine was developed, called Integrated Action. "Part of the whole purpose of Integrated Action is to change attitudes and behaviour in our favour".

In December 2014, the Security Council of the Russian Federation also published a new military doctrine. "The characteristic features and specifics of current military conflicts are…military force, information, political and economic measures" they concluded.

Or take AJP 3.10, NATO's Allied Joint Doctrine for Information Operations from November 2009. "The ever-increasing use of technologies such as the internet have resulted in a world where information plays an increasingly important role" it states. The doctrine explains that information operations should be used to target an enemy's 'will':

"For example, by questioning the legitimacy of leadership and cause, information activities may undermine their moral power base, separating leadership from supporters, political, military and public, thus weakening their desire to continue and affecting their actions."

State security and information warfare

Fake News is many things, of course, but as military after military redefined warfare, it became part of a concerted, systematic exploitation of the internet by militaries and state security bureaucracies around the world, facing outwards at foreign publics, and also at domestic populations.

- China employs two million people to write 448 million social media posts to 'distract the public, change the subject'.
- In Saudi Arabia, researchers have revealed thousands of 'fake' Twitter accounts generating hundreds to thousands of tweets per hour of "anti-Shia and anti-Iranian propaganda".
- In Mexico, an estimated 75,000 automated accounts are known locally as Peñabots, flood hashtags associated with corruption or political scandal.
- In the Philippines, salaried social media commentators mount a "fanatic defense of Duterte" and manipulate online polls.
- In Turkey, 6,000 'white trolls' have allegedly been enlisted to manipulate discussions, drive particular agendas, and counter government opponents on social media.

Freedom House assessed 65 countries for online 'manipulation tactics'. They found that 30 had evidence of paid pro-Government commentators, 20 showed evidence of political bots, 16 had seen deliberately misleading news pumped out during elections, and in 10 countries social media had been 'hijacked', forcibly taken over to spread information against the owners' wishes.

Your opinion is a military target

The concept of what a conflict or a military operation really is has widened: transferring outside the kinetic arena and into the battlefield of ideas, information, beliefs and opinions. Compared to a tank, or a missile, Fake News is trivially cheap and technically straightforward to do.

It is a new form of warfare that is not described in international law, and not bounded by international norms. It is also a form of control that inherently benefits authoritarian States more than liberal, democratic or rights-respecting ones.

An assault is being made on your beliefs. Your opinions are objectives, your news diet a strategic target. This is the reality of Fake News; a weapon in a new kind of warfare, redefined for the information age.