BRIEFING NOTES

#BN-35-Emerging technology and military application-Feb2021

NATIONAL DEFENCE AND THE INFODEMIC

Author: Dave McMahon
Clairvoyance Cyber Corp
www.clairvoyance.network
info@clairvoyance.network
819.664.2708

CONTEXT

In January 2021, Twitter and Facebook permanently suspended U.S. President Donald Trump's account for incitement of violence, fuelled by mis-information, conspiracies and toxic narratives. Twitter also banned Trump's former national security adviser Michael Flynn and attorney Sidney Powell as part of a purge of QAnon accounts. Google blocked the Parler social networking app for inciting ongoing violence in the U.S.

As social media platforms have begun to moderate agents of conspiracy and misinformation. Yet these positive actions "have simply moved them to 'alt-tech' platforms like [Gab, Telegram and 8kun], where there's no moderation and less critical analysis." - Wired

Alt-media acts as a resonance chamber for conspiracy believers, reinforcing toxic narratives without healthy scepticism or rational discourse.

Jigsaw, a division of Google focused on countering digital extremism, cyberattacks and misinformation, says that "online conspiracy theories are surprisingly convincing – and present significant danger to the real world."

Meanwhile, regulation and moderation of social media will likely generate considerable policy debate in the next year.

But how did we get here?

BELIEFS

The Internet is fertile ground for many strange beliefs.

75% of Americans believe in the paranormal
70% think there is a government cover-up of UFOs
57% think psychics are legitimate
45% imagine ghosts
26% follow Astrology and
2% are convinced that the Earth is flat or it is possible to get stuck in a mirror
but only 30% think the theory of evolution is true, or that the universe is 13.7 Billion years old.

Thereofre, it should not be surprising that dangerous conspiracies beliefs are propagated in cyberspace and gaining ground.

QAnon is a disproven and discredited far-right conspiracy theory alleging that a cabal of Satan-worshipping pedophiles is running a global child sex-trafficking ring and plotting against the US president Donald Trump.

Other conspiracies include ones that assert that governments and industry are run by the deep state a fifth column the Illuminati or lizard people.

Many of the same followers believe that Moon landing was faked, Vaccines cause autism, Alien abductions happen frequently, Bigfoot and Elvis sightings, secret government weather control, or radio towers can read your mind or alter your mood. More contemporary conspiracies claim that 5G causes COVID19 or cancer, and 9/11 was a government operation. Russia has been implicated in creating propagating, amplifying many of these conspiracies in an effort to disrupt and erode trust in democracy.

Global Research is an example of a Canadian conspiracy site with 275,000 followers that has been marked as a Kremlin proxy for dis-information.

HISTORY

The difference between conspiracy narratives and disinformation is agency. Conspiracy beliefs assign a casual agent to explain an event or effect, independent of the facts or scientific explanation. Misinformation is just wrong. Sometimes the bigger the lie, the better it sells.

Psychological Operations (PSYOPS), Cyber Psychological Operations (CYOPS), propaganda, influence operations, information warfare, electronic deception and mis-information are nothing new.

Deception operations have been practiced in warfare and statecraft for thousands of years. Even electronic deception and influence activities are generations old. The Interdepartmental committee on Information Warfare in 1994, looked deeply at semantic warfare and information peacekeeping, designed solutions waiting for the problem to arrive in cyberspace.

The messages and methods are the same, only the medium has evolved. But, unlike conventional methods of subterfuge, and influence, cyber delivery systems allow for amplification using artificial intelligence and semantic botnets) and more convincing counterfeits (deep fakes). The Internet permits anyone to self-publish nonsense or through pseudoscience sites in a compelling format.

Consider that every wetware attack, propagation of toxic meme or harmful narrative is delivered through an electronic network. Alternatively, most hacking is facilitated by social engineering.

CHALLENGE

The greatest challenge of our lifetime will be the war on truth. We had forecasted these decades ago. Concluding that using the cyber to attack truth systems and trust, is far easier than understanding the technology itself. Hence, the quick adoption by extremist groups, and technologically-disadvantaged states.

The speed and scale of delivery of toxic messages and contagion, mean that we need to address foreign propagated nonsense before it can generate an organic following domestically.

We need to counter mis-information and conspiracy with reason, scientific method, healthy skepticism, critical analysis, trust, and truth.

In this matter, it is imperative that we move to define and preserve of universal values and norms.

It will also be necessary to enforce normative values and counter mis-information through technical means, legal recourse and persistent engagement in the cognitive domain.

MINISTRY OF TRUTH

Large telecoms carriers and service providers have been reticent to police Internet content. Child safety protocols have been put in place, but they rely on independent 3rd parties to determine what to filter. Validating the truthfulness of posts or toxicity of messages is a delicate affair and not without moral hazard. Folks have the right to believe all sorts of silly things, unless it harms others in a tangible way.

Industry is the owner-operators of cyber space, the custodians of data and in a position to enforce the rules. Furthermore, online platforms will be compelled to establish acceptable use policies, curate the validity and acceptability of information content and enforce rules and norms in cyberspace for users and governments alike.

The telecommunications and cyber defence industry will need to capitalize on the tradecraft of advertising and entertainment industry, to counter influence, interference and alt-truths.

Counter-radicalization programs have already successfully identified the most effective messages of threat actors, then move to counter bad actors by dismantling their networks and substituting a positive narrative.

We ought not mimic Russia and China in their method of propagating fractured narratives, conspiracies, and a fire hose of falsehoods. Canada must take moral high ground in this fight. Countering with misinformation and propaganda typically backfires.

We need to:

- Teach populations to think critically and rationally;
- Establish authoritative sources; stand-up independent third parties to curate information and fact check;
- Apply reputational rating scores in the same way that we do for spam;
- Institute careful thought-out government regulation; and
- Seek civil and criminal prosecution of those who deliberately starting or spreading misinformation on important issues, like health and safety.