Trolls that control the narrative in media and Internet

How to track down robots, bots and "sea lions" that try to neutralise uncomfortable news

from an episode of Solutions's Watch by James Corbett[1]

Let's face it: the "comments" at the end of videos or articles are often dreadful. But who's to say they're even real? And what's the solution to these abominable posts? Not to read the comments, of course. But those who wade into this info war battlespace should at least be aware of the various tactics that trolls*, bots*, spies and "sea lions" are using to derail them from taking meaningful action.

(Picture ma)

Traffic from robots

Comments can be a very rich source of additional information, especially on controversial topics, and this section tends to gain in importance compared to the main content of the publication. However, it is not uncommon to find an abundance of defamatory statements there, such as anti-Semitic, obscene, or offensive language. Although most content creators have become accustomed to not attaching too much importance to them, this can have a serious impact on the sharing of a video or the channel's subscriber count.

The first question is whether the comments in question come from real internet users or are generated by an algorithm. According to an *article by Tech Radar,*[2] which analysed a report on bots, 47% of web traffic – by definition, one would be tempted to say – is attributable to bots, a figure that increases by around 5% each year, while the proportion of traffic attributable to humans decreases every year. And almost 30% of these "bots" are malicious.

Bot traffic is not negative per se, as it is essential for PDAs, search engines and the like, but unfortunately it also contains a multitude of "malicious bots". These will, for example, target websites and mobile applications with web scraping campaigns (extracting information from websites) and data mining and carry out direct attacks on websites or broadcast channels or abuse banking transactions.

Some bots have specific targets and are controlled by intelligence officers appointed to "combat online disinformation".

To prevent bot traffic, many websites use applications that force users to identify themselves as "human" and ask them to perform a small visual or auditory test. However, this is difficult to apply to the comments section or group conversations in chat applications. A way out for content creators who are attacked too often is to publish their content on different platforms, enable the comments section on one, disable it on the other and mention links to alternative publications on all of them.

The technique of trolls

This is not a fantasy: one of the tasks of the *secret services is to control the narrative in the media and social networks,*[3] as controlling public opinion through the manufacture of consent *or censorship*[4] are key elements of any political strategy. The battle between European Commissioner *Thierry Breton* and *X/Twitter* CEO *Elon Musk* to control the *news about the war between Israel and Gaza*[5] is a good illustration of this. So is the *censorship of presidential candidate Robert Kennedy Jr,*[6] the scandal surrounding the "fact checkers" paid for *by the Marianne Fund*[7] or the fact that the *US Supreme Court must rule on the interference of the White House*[8] in the control of social networks.

So, in addition to the "natural" harassment, there are also trolls paid for by the taxpayers. These agents are tasked with controlling the narrative, infiltrating groups, and neutralising overly disruptive information. They operate with multiple identities simultaneously and on different platforms to pollute and disrupt conversations or influence the discussion. An interesting description of some of their practices can be found in a document entitled *"The Gentle Person's Guide to Forum Spies"*[9] on the website *Cryptome.org* (a Wikileaks-affiliated website), which refers to *Cointelpro's* methods.

Cointelpro is apparently a disruptive US intelligence programme that aims to dilute, misappropriate, or take over an internet forum or discussion space, typically a comment section.

Techniques used include, firstly, bombarding an important message with a rapid succession of other messages to move it "down" the list of messages and make it less visible.

Then there is the "weakening of consensus". This is about posting a contrary opinion by starting with a rather weak suggestion without many arguments, but which is gradually reinforced under other usernames so that the reader really gets the impression that a counterargument is gradually being built up that overturns the previously prevailing consensus.

"Watering down" the topic is another technique where readers are constantly led onto side topics, side-tracks, to waste time and keep them in inaction. In the long run, this will cause the productive users to leave the forum, while the others will switch from analysing relevant facts to "chatting" mode.

The "agent" will take the opportunity to gather information in the group by talking about their own interests first. For example, by asking a question like: What system do you use to protect your privacy? Or: Where do you get your resources from? Or even questions that concern the Internet user's private life.

Another recurring tactic is a violent discussion between two identities controlled by the troll agent. If others join in the heated discussion, they are likely to say things that go beyond their intended statements and for which they may later be charged with offences or incitement to hatred and violence.

Smashing the arguments

The most common techniques used to demolish a solid argument are the following: diverting attention from the issue to those who are involved in or exposed to it: Lynching, ridicule, insults, or outrage – usually a whole emotional register is brought up to distract from the actual argument.

Another less easily recognizable method of interrupting a factual discourse is the "sea lion technique". It consists of polite and "naïve" harassment through repeated questions. For example, every assertion is disputed by asking for "proof", which is then repeatedly refuted. These can also be side questions that have to be answered again and again or the constant request to start an unnecessary debate. The aim is to make the user and readers lose patience by causing them to become annoyed or abandon the conversation. As always with trolls, it's best to denounce their actions before you stop replying.

To neutralise this undermining, you first need to be aware that these techniques exist. It is then best to report them in the discussion forum. It is irrelevant whether it is a case of genuine infiltration or spontaneous saboteurs. The most important thing is to show that such interactions are counterproductive and that you should not fall into this trap.

In short, if you pay attention to the course of the conversation, you can focus more based on your own opinion. To what extent and in what way was our attention ultimately drawn to side issues or false conclusions? And how can this affect our actions? Because we must not forget that these techniques are primarily used to disarm arguments and people who could bring about concrete change in social organisation, for example by becoming politically active or appealing to the courts.

And finally, even before suspecting the participants in the dialogue of being vile agents on behalf of the ruling powers, we must also ask ourselves to what extent we ourselves are susceptible to the unconscious use of these less than commendable techniques. Isn't that the attitude of a true gentleman?

Source: Information from CovidHub, https://www.covidhub.ch/guide-gentleman-trolls/, 23 October 2023

(Translation "Swiss Standpoint")

1 *https://www.bitchute.com/video/8dyhRfC5lAWx/*

2 *https://www.techradar.com/news/bots-now-make-up-nearly-half-of-all-internet-traffic-and-thats-very-bad-news-for-our-security*

3 *https://sentadepuydt.substack.com/p/la-cia-et-le-fbi-a-la-tete-de-la*

[4] *https://www.covidhub.ch/incontournables-3-censure/*

[5] *https://www.covidhub.ch/guerre-gaza-europe-controle-info/*

[6] *https://www.covidhub.ch/la-censure-des-geants-dinternet/*

[7] *https://www.francesoir.fr/recherche?search_api_fulltext=fonds%20marianne&page=0*

[8] *https://childrenshealthdefense.org/defender/texas-law-social-media-censorship-supreme-court/*

[9] *https://cryptome.org/2012/07/gent-forum-spies.htm*

*** Glossary**

Trolls

Online jargon, a troll is a "person" who deliberately uses "inflammatory" comments to spark a verbal dispute or intentionally annoy people on the Internet. This is usually done by "posting" inflammatory and digressive, irrelevant, or off-topic messages and posts in an online community. Their communication in these communities is limited to posts aimed at emotionally provoking or unsettling other participants in the conversation.

Bots

The term "bot" is derived from the English word for robot. Like mechanical robots, Internet bots are programmed to fulfil specific, repetitive tasks. To do this, they execute clearly defined commands in the form of algorithms and scripts, which they implement faster than any human being could. Bots are therefore computer programmes that act independently and automatically and are not dependent on the cooperation or monitoring of human beings for their function.

Malware Bots serve various illegal purposes. These include:

- Data and identity theft through scraping, phishing, and keylogging of sensitive information such as passwords, bank details and address data.
- Distributed denial-of-service attacks (DDoS), which can paralyse servers through massive data traffic.
- Use of backdoors in a PC's security system to infect the system.
- Retransmit with spam to redirect data packets.

They include the following types:

- Propaganda or manipulative bots: social bots that simulate user profiles, form digital opinions, and spread political statements, fake news and conspiracy theories or respond to comments and posts using keywords.
- Scam/phishing bots: These bots steal data through pseudo links, fake emails, and fake websites.
- Keylogging bots: Bots that save message traffic or record, save and forward all activity on a PC.
- File-sharing bots: Bots that respond to specific search queries and offer users a link to the desired search term. By clicking on this link, the bot can infect the PC used by that person.
- Spam bots: They send large quantities of spam mails and use address books and contacts of unsuspecting users to specifically expand their spam radius.
- Zombie bots: So-called zombie bots are computers that have been infected with malware by bots or made part of a botnet and provide computing power for large botnet attacks. Compromised PCs are often not easily recognisable as part of a botnet.
- Botnet: Refers to the totality of infected PCs that are joined together to form a network and are used by the users of the malware bots for DDoS attacks.

The five most common large-scale bot attacks are:

- DDoS attacks: deliberately causing server overload.
- Spamming and traffic monitoring: Overloading of mail servers or large-scale data theft.
- Inventory denial attacks: Attacks on online shops to list products as "unavailable".
- Scraping attacks: Data theft and data selling.
- Credential stuffing attacks: fraudulent access to a user account of a Web application following automated connection attempts from a list of access data generally stolen from another web application.