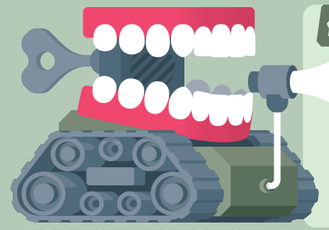
BOT ARMIES IN PUBLIC CONSULTATIONS

BY PETER STOYKO

Automated software applications ("bots") have been weaponized to unduly sway public opinion and online government consultations. A good defence starts with knowing the mischief each type of bot can get up to.

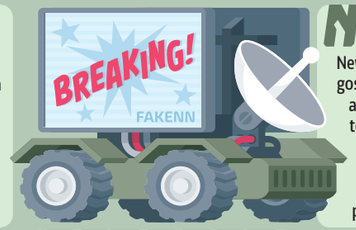
Not all bots are bad. Many Internet-enabled services rely on them. Some bots can fight the good fight by improving political transparency. Knowing your bot allies is the second element of an effective defence.

CHATBOT



While impersonating citizens on social media and comment threads, these conversationalists flood the zone with advocacy, polarize debate, sow confusion, mock opponents, and otherwise discourage good-faith dialogue.

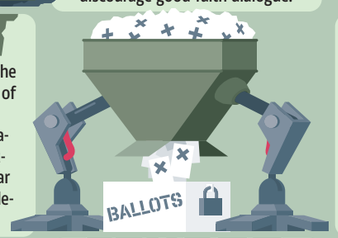
NEWSBOT



Newsbots spread propaganda and gossip. Real news that fits their agenda is amplified by reposting to social media sites. Sensational stories distract the public and muddy the facts. Misinformation is spread to manipulate political participation.

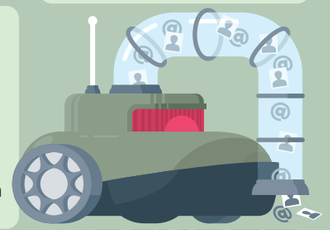
VOTEBOT

These are the ballot stuffers of the bot world who inflate the tallies of online polls and petitions. They can also highjack public consultations by flooding them with written submissions to give particular policy stances the veneer of widespread public support.

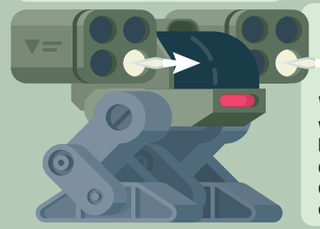


SCRAPER

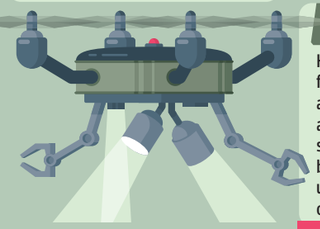
Scraperbots pull personal information from Web pages and online public records. The data is used by other bots to impersonate real people in official submissions. Without follow-up checks, most identity-theft victims will not learn of advocacy made in their name.



CENSOR



Denial-of-service attacks are attempts to shut down Web sites by bombarding them with bot traffic launched from hijacked computers and connected devices. These attacks can shut down consultations or censor Web content.

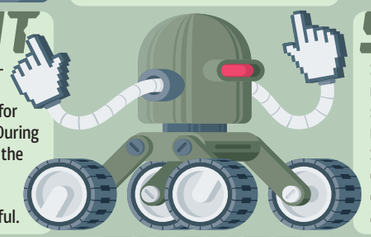


HACKBOT

Hackbots roam the Web looking for vulnerabilities to exploit. Once a weakness is discovered, the bot alerts hackers and infects the system with nefarious code. Data breeches and corruptions can undermine confidence in a voting or consultation process.

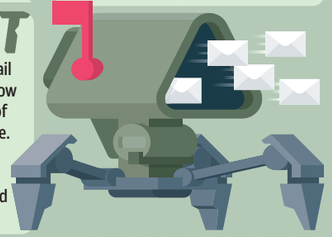
CLICKBOT

Clickbots trigger online advertisements. Originally, these bots defrauded those paying for ads on a pay-per-click basis. During consultations, clickbots drain the ad budgets of opponents or solicitation campaigns while making the ads seem successful.

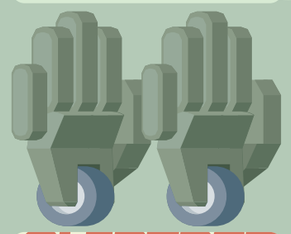


SPAMBOT

Spambots spew unsolicited e-mail messages at targets. Even with low success rates, the large volume of messages ensures some influence. Spam bombardments hinder consultations by drowning out other voices. Embedded links and attachments can infect systems.

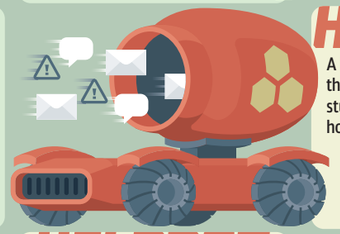


PUSHER



"Pushing hands" are not bots but are low-wage workers doing the same work as political bots, often aided by automation tools. They are mobilized through piece-rate crowd-sourcing platforms (e.g. Amazon's Mechanical Turk) or clandestine networks.

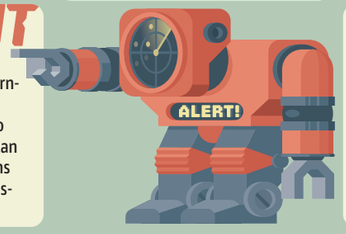
HONEYBOT



A honey*pot* is a software enclave that attracts computer viruses to study them up close. Similarly, a honey*bot* acts as a decoy for other bots to record messages and tactics. Findings are publicized, sent to authorities, and used to devise counter-measures.

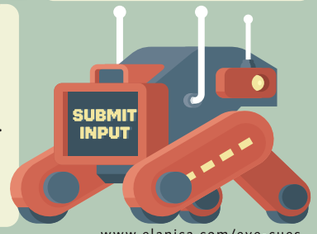
ALERTBOT

Alertbots monitor the activity of politicians, activists, or government processes and publicize activity that would normally go unnoticed. That transparency can raise awareness of consultations (or lack thereof) and the submissions of various players.



HELPBOT

Helpbots were originally designed to fight parket tickets, file tax returns, or otherwise overcome convoluted bureaucratic processes. Machine learning discovers tactics most likely to result in successful submissions, which can help those without technical expertise.

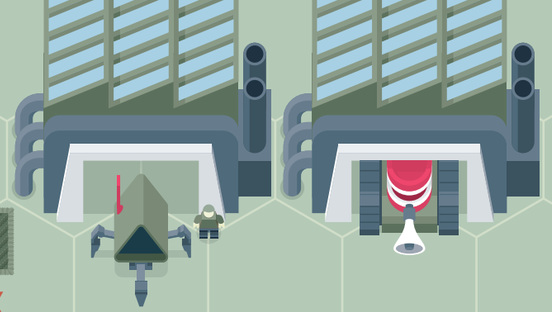


www.elanica.com/eye-cues

cues by elanica™

THE BATTLEFIELD

LINES OF DEFENCE



1 CIVIC CULTURE

Promotion of civic literacy, healthy information diets, and critical self-defence makes the public resilient.

BUILDING

Software for making bots is becoming mainstream and easier to use. Bots may become a common way to interact with technology.

SOCKPUPPETING

Bots can manipulate participation by playing both sides of a debate.

2 DATA PRIVACY

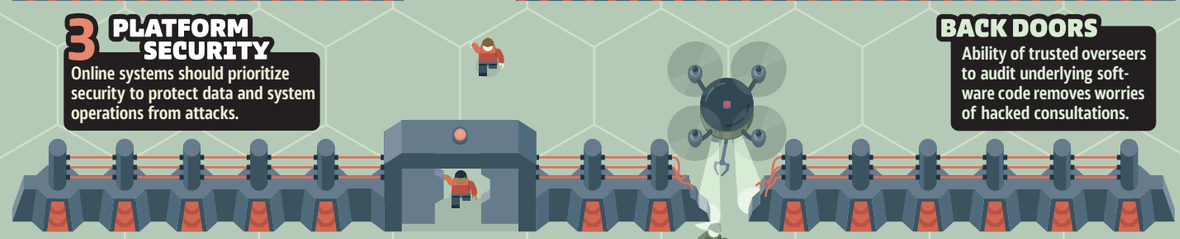
General Data Privacy Regulation is the bulwark against highjacked identity and manipulation.

TARGETING

Scraped data is often used to develop voter profiles to tailor online ads and propagandized news.

3 PLATFORM SECURITY

Online systems should prioritize security to protect data and system operations from attacks.



BACK DOORS

Ability of trusted overseers to audit underlying software code removes worries of hacked consultations.

4 IDENTITY MANAGEMENT

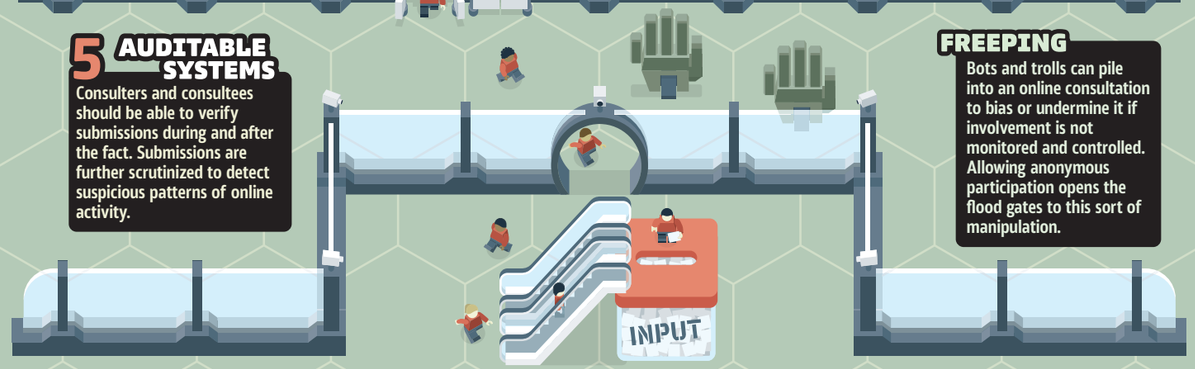
Eligibility to offer input or vote is authenticated without adding onerous barriers.

IDENTITY THEFT

Real identities are often used to gain entrance into consultation processes.

5 AUDITABLE SYSTEMS

Consulters and consultees should be able to verify submissions during and after the fact. Submissions are further scrutinized to detect suspicious patterns of online activity.



FREEPING

Bots and trolls can pile into an online consultation to bias or undermine it if involvement is not monitored and controlled. Allowing anonymous participation opens the flood gates to this sort of manipulation.