The Weaponization of Social Media

by James Corbett
March 2, 2018
Source

http://www.youtube.com/watch?v=0dL8vt1n-f8

Now openly admitted, governments and militaries around the world employ armies of keyboard warriors to spread propaganda and disrupt their online opposition. Their goal? To shape public discourse around global events in a way favourable to their standing military and geopolitical objectives. Their method? The Weaponization of Social Media. This is The Corbett Report.

TRANSCRIPT

It didn't take long from the birth of the world wide web for the public to start using this new medium to transmit, collect and analyze information in ways never before imagined. The first message boards and clunky "web 1.0" websites soon gave way to "the blogosphere." The arrival of social media was the next step in this evolution, allowing for the formation of communities of interest to share information in real time about events happening anywhere on the globe.

But as quickly as communities began to form around these new platforms, governments and militaries were even quicker in recognizing the potential to use this new medium to more effectively spread their own propaganda.

Their goal? To shape public discourse around global events in a way favourable to their standing military and geopolitical objectives.

Their method? The Weaponization of Social Media.

This is The Corbett Report.

Facebook. Twitter. YouTube. Snapchat. Instagram. Reddit. "Social media" as we know it today barely existed fifteen years ago. Although it provides new ways to interact with people and information from all across the planet virtually instantaneously and virtually for free, we are only now beginning to understand the depths of the problems associated with these new platforms. More and more of the original developers of social media sites like facebook and Twitter admit they no longer use social media themselves and actively keep it away from their children, and now they are finally admitting the reason why: social media was designed specifically to take advantage of your psychological weaknesses and keep you addicted to your screen.

> ***SEAN PARKER**: If the thought process that went into building these applications—Facebook being the first of them to really understand it—that thought process was all about "How do we consume as much of your time and conscious attention as possible?" And that means that we need to sort of give you a little dopamine hit every once in a while because someone liked or commented on a photo or a post or whatever, and that's gonna get you to contribute more content and that's gonna get you more likes and comments. So it's a social validation feedback loop. I mean it's exactly the kind of thing that a that a hacker like myself would come up with, because you're exploiting a vulnerability in in human psychology. And I just think that we—the inventors/creators, you know, and it's me, it's Mark, it's Kevin Systrom at Instagram, it's all of these people—understood this consciously and we did it anyway.*

SOURCE: ***[Sean Parker – Facebook Exploits Human Vulnerability]***

It should be no surprise, then, that in this world of social media addicts and smartphone zombies, the 24/7 newsfeed is taking up a greater and greater share of people's lives. Our thoughts, our opinions, our knowledge of the world, even our mood are increasingly being influenced or even determined by what we see being posted, tweeted or vlogged. And the process by which these media shape our opinions is being carefully monitored and analyzed, not by the social media companies themselves, but by the US military.

> ***MARINA PORTNAYA:*** *When the world's largest social media platform betrays its users, there's going to be outrage.*
>
> ***ABC HOST:*** *The study to see whether Facebook could influence the emotional state of its users on that news feed.*
>
> ***CNN ANCHOR:*** *It allowed researchers to manipulate almost 700 thousand users news feeds. Some saw more positive news about their friends, others saw more negative.*
>
> ***CNN GUEST:*** *Well I'm not surprised. I mean we're all kind of lab rat than the big Facebook experiment.*
>
> ***PORTNAYA:*** *But it wasn't only Facebook's experiment. IT turns out the psychological study was connected to the US government's research on social unrest.*
>
> ***MORNING JOE GUEST:*** *This is really kind of creepy.*
>
> ***PORTNAYA:*** *And it gets worse. What you may not know is that the US Department of Defense has reportedly spent roughly $20 million conducting studies aimed at learning how to manipulate online behavior in order to influence opinion. The initiative was launched in 2011 by the Pentagon's Defense Advanced Research Projects Agency, otherwise known as DARPA. The program is best described as the US media's effort to become better at detecting and conducting propaganda*

> *campaigns via social media. Translation: When anti-government messages gain ground virally, Washington wants to find a way to spread counter opinion.*
>
> ***SOURCE: US military harnesses social media to manipulate online behaviour***

The DARPA document that details the Pentagon's plans for influencing opinions in the social media space is called "Social Media in Strategic Communication." DARPA's goal, according to their own website is "to develop tools to help identify misinformation or deception campaigns and counter them with truthful information."

Exactly what tools were developed for this purpose and how they are currently being deployed is unclear, but Rand Walzman, the program's creator, admitted last year that the project lasted four years, cost $50 million and led to the publication of over 200 papers. The papers, including "Incorporating Human Cognitive Biases in a Probabilistic Model of Retweeting," "Structural Properties of Ego Networks," and "Sentiment Prediction using Collaborative Filtering" make the thrust of the program perfectly clear. Social media users are lab rats being carefully scrutinized by government-supported researchers, their tweets and facebook posts and instagram pictures being analyzed to determine how information spreads online, and, by implication, how the government and the military can use these social media networks to make their own propaganda "go viral."

As worrying as this research is, it pales in comparison to the knowledge that governments, militaries and political lobby groups are already employing squadrons of foot soldiers to wage information warfare in the social media battlespace.

> ***AL-JAZEERA ANCHOR:*** *The Pentagon's got a new plan to counter anti-american messages in cyberspace. It involves buying software that will enable the American military to create and*

control fake online personas—fake people, essentially—who will appear to have originated from all over the world. The plan is being undertaken by CENTCOM (US Central Command), and the objective of the online persona management service is to combat enemy propaganda by influencing foreign social media websites. CENTCOM has hired a software development company called "Ntrepid," and, according to the contract, the California-based company will initially provide 50 user licenses, each of which would be capable of controlling up to 10 fake personas. US law forbids the use of this type of technology, called "sockpuppets," against Americans, so all the personas will reportedly be communicating in languages like Arabic Persian and Urdu.

SOURCE:* *Persona Online Management, Fake Online Personas, Sock Puppets, Astroturfing Bots, Shills

***CTV ANCHOR**: So is it okay to have the government monitor social media conversations and then to wade in and correct some of those conversations? With more on this, let's go to technology expert Carmi Levy. He's on the line from Montreal. Carmi, do you think the government's monitoring what you and I are saying right now? Is this whole thing getting out of line, or what?*

[…]

CARMI LEVY: It opens up a bit of a question. I'd like to call it a Pandora's box about, you know, what exactly is the government's aim here, and what do they hope to accomplish with what they find out? And as they accumulate this information online—this data on us—where does that data go? And so I think as much applaud the government for getting into this area, the optics of it are potentially very big brother-ish. And the government really does need to be a little bit more concrete on what its intentions are and how it intends to achieve them.

SOURCE: ***[CTV Confirms Government(s) employing Internet Trolls, Shills & PR Agents to 'correct misinformation']***

4WWL REPORTER: *New evidence that government owned computers at the Army Corps of Engineers office here in New Orleans are being used to verbally attack critics of the Corps comes in an affidavit from the former editor-in-chief of nola.com. Jon Donley, who was laid off this past February, tells us via satellite from Texas in late 2006 he started noticing people presenting themselves as ordinary citizens defending the Corps very energetically.*

JON DONLEY: *What stuck out, though, was the wording of the comments was in many ways mirroring news releases from the Corps of Engineers.*

[…]

4WWL REPORTER: *These commenters tried to discredit these people and when Rosenthal investigated, she discovered the comments were coming from users at the internet provider address of the Army Corps of Engineers offices here in New Orleans. She blamed the Corps for a strategy of going after critics.*

SANDY ROSENTHAL: *In the process of trying to obscure the facts of the New Orleans floodings, one of their tactics was just verbal abuse.*

SOURCE: ***[Government Sock Puppets]***

NAFTALI BENNETT: *Mo'etzet Yesha in conjunction with My Israel has arranged an instruction day for wiki editors. The goal of the day is to teach people how to edit in Wikipedia, which is the number one source of information today in the world. As a way of example, if someone searches the Gaza flotilla, we want to be there. We want to be the guys who influence what is written there, how it's written, and to ensure that it's*

balanced and Zionist in the nature.

SOURCE: Course: Zionist Editing on Wikipedia

These operations are only the visible and publicly-admitted front of a vast array of military and intelligence programs that are attempting to influence online behaviour, spread government propaganda, and disrupt online communities that arise in opposition to their agenda.

That such programs exist is not a matter of conjecture; it is mundane, established, documented fact.

In 2014, an internal document was leaked from GCHQ, the British equivalent of the NSA. The document, never intended for public release, was entitled "The Art of Deception: Training for a New Generation of Online Covert Operations" and bluntly stated that "We want to build Cyber *Magicians*." It then goes on to outline the magic "techniques" that must be employed in influence and information operations online, including deception and manipulation techniques like "anchoring," "priming" and branding propaganda narratives. After presenting a map of social networking technologies that are targeted by these operations, the document then instructs the magicians how to deceive the public through "attention management" and behavioural manipulation.

That governments would turn to these strategies is hardly a shocking development. In fact, the use of government shills to propagate government talking points and disrupt online dissent has been openly advocated on the record by high-ranking government officials for the past decade.

In 2008, Cass Sunstein, a law professor who would go on to become Obama's Information "Czar," co-authored a paper entitled "Conspiracy Theories" in which he wrote that the "best response" to online "conspiracy theories" is what he calls "cognitive infiltration" of groups spreading these

ideas.

> *"Government agents (and their allies) might enter chat rooms, online social networks, or even real-space groups and attempt to undermine percolating conspiracy theories by raising doubts about their factual premises, causal logic or implications for political action. In one variant, government agents would openly proclaim, or at least make no effort to conceal, their institutional affiliations. […] In another variant, government officials would participate anonymously or even with false identities."*

It is perhaps particularly ironic that the idea that government agents are actually and admittedly spreading propaganda online under false identities is, to the less-informed members of the population, itself a "conspiracy theory" rather than an established conspiracy fact.

Unsurprisingly, when confronted about his proposal, Sunstein pretended to not remember having written it and then pointedly refused to answer any questions about it.

> ***LUKE RUDKOWSKI**: My name is Bill de Burgh from Brooklyn College, and I know you've written many articles. But I think the most telling one about you is the 2008 one called "Conspiracy Theories," where you openly advocated government agents infiltrate activist groups of 9/11 Truth and also stifle dissent online. I was wondering why do you think it's the government's job, or why do you think the government should go after family members who have questions and 9/11 responders who are lied to about the air, survivors whose testimony conflicts, and also government whistleblowers that were gagged because they released information that contradicts the official story.*
>
> ***CASS SUNSTEIN**: I think it was Ricky who said I'd written hundreds of articles and I remember some and not others. That one I don't remember very well. I hope I didn't say that. But*

> *whatever was said in that article, my role in government is to oversee federal rule making in a way that is wholly disconnected from the vast majority of my academic writing, including that.*
>
> *[…]*
>
> ***RUDKOWSKI**: I just want to know is it safe to say that you retract saying that conspiracy theories should be banned or taxed for having an opinion online. Is it safe to say that?*
>
> ***SUNSTEIN**: I don't remember the article very well. So I hope I didn't say either those things.*
>
> ***RUDKOWSKI**: But you did and it's written. Do you retract them?*
>
> ***SUNSTEIN**: I'm focused on my job.*
>
> ***SOURCE:** **Obama Information Czar Cass Sunstein Confronted on Cognitive Infiltration of Conspiracy Groups***

Now, a decade on from Sunstein's proposal, we know that military psyops agents, political lobbyists, corporate shills and government propagandists are spending vast sums of money and employing entire armies of keyboard warriors, leaving comments and shaping conversations to change the public's opinions, influence their behaviour, and even alter their mood. And they are helped along in this quest by the very same technology that allows the public to connect on a scale never before possible.

Technology is always a double-edged sword, and sometimes it can be dangerous to wield that sword at all. There are ways to identify and neutralize the threat of online trolls and shills, but the phenomenon is not likely to go away any time soon.

Each of us must find our own answer to the question of how best to incorporate these technologies into our life, but the

next time you find yourself caught up in an argument with an online persona that may or may not be a genuine human being, it might be better to ask yourself if your efforts are better spent engaging in the argument or just turning off the computer.