DARPA requests proposals for “Semantic Forensics” system

US Defense Department prepares for mass internet censorship

Kevin Reed
6 September 2019

The US military has issued a call for research proposals from technology partners for the development of an automated system capable of scanning the entire internet and locating and censoring content deemed as “false media assets” and “disinformation.” According to government documents, the requested solution would provide “innovative semantic technologies for analyzing media” that will help “identify, deter, and understand adversary disinformation campaigns.”

On August 23, the Defense Advanced Research Projects Agency (DARPA) issued a solicitation for a so-called Semantic Forensics (SemaFor) program on the federal government business opportunities website. According to the bid specifications, SemaFor “will develop technologies to automatically detect, attribute, and characterize falsified multi-modal media assets (text, audio, image, video) to defend against large-scale, automated disinformation attacks.”

In other words, the US Defense Department is seeking a technology partner that will build a platform to enable the Pentagon to locate any content it identifies as an adversarial “disinformation attack” and shut it down. This technology will cover anything on the internet including web pages, videos, photo and social media platforms.

The documents released as part of the DARPA request say that the technology and software algorithms it is seeking would “constitute advances to the state of the art” that will be top secret and do not include “information that is lawfully publicly available without restrictions.”

These advances would involve moving away from “statistical detection techniques” which are becoming “insufficient for detecting false media assets.” The use of intelligent semantic techniques—the ability for a program to analyze online content within context and determine its meaning and intent—requires the latest developments in artificial intelligence and so-called “neural networks” that have the ability to “learn” and improve performance over time. According to the US Defense Department, semantic analysis will be able to accurately identify inconsistencies within artificially generated content and thereby establish them as “false.”

There are three components to DARPA’s requested solution. The first is to “determine if media is generated or manipulated,” the second is that “attribution algorithms will infer if media originates from a particular organization or individual” and the third is to determine whether the media was “manipulated for malicious purposes.” Although the request makes reference to deterrence, there are no details about how the Pentagon intends to act upon the content it has identified as “false.”

The proposal request also never gets around to specifying who the adversaries are that need to be identified, deterred and understood. However, it is clear that one of the motivations for the initiative is concern about the rise of “deepfake” content. Deepfake videos, for example, involve the use of specialized software to modify video content in ways that completely alter the original image or message and generate a new stream with apparent authenticity.

According to the Dr. Matt Turek, DARPA’s Information Innovation Officer who drafted the Pentagon’s request for proposal, “Mirroring this rise in digital imagery is the associated ability for even relatively unskilled users to manipulate and distort the message of the visual media. While many manipulations are benign, performed for fun or for artistic value, others are for adversarial purposes, such as propaganda or misinformation campaigns.”

The DARPA deadline for proposals is set for November 21, 2019. The agency intends to award the contract to

multiple technology partners across the various disciplines of the project. The solicitation includes details on how the submitting companies will be evaluated and the contracts ultimately awarded.

As several reports have already pointed out, the preposterous idea that artificial intelligence can be deployed to identify content generated by artificial intelligence is the technological equivalent of the proverbial serpent eating its own tail. As pointed out by Gizmodo, “while an automated model sounds nice in theory, in execution, to date, these types of algorithmically generated systems are still flawed and biased, and in more disturbing cases, outright discriminatory. Existing applications do not inspire a lot of faith in a near-future system that would be both effective and just.”

Much of the corporate media coverage about the DARPA bid request has presented the initiative as a legitimate effort to stop online “fake news.” This presentation follows upon the incessant and unproven charges of “Russian interference” in the 2016 elections that were driven by supporters within the US military-intelligence establishment of Hillary Clinton’s candidacy for president.

However, the current effort by the Pentagon to create an automated system for identifying and shutting down so-called “fake news” is part of the ongoing broader effort by the Democrats and Republicans, in cooperation with the intelligence state, to both control social media and online content and use it to monitor the moods, ideas and politics of the public.

Whatever the publicly stated claims of DARPA regarding the desire to stop the use of “false media assets” to target personal attacks, generate “believable” events and propagate ransomware, these tools are undoubtedly part of the imperialist cyberwarfare arsenal currently being developed and deployed by the US military and CIA .