GlobalResearch
Center for Research on Globalization

America's "War On Terror" Morphs into a Diabolical Assault on Civil Rights

DARPA's "Deep Learning"

By Tom Burghardt
Global Research, May 28, 2010
Antifascist Calling... 23 May 2010

Region: USA
Theme: Police State & Civil Rights

As America's War On Terror morphs into an endless assault on civil and human rights, the technophilic fantasies of our masters, and the corporations whom they lovingly serve, even amidst the doom and gloom of capitalism's global economic collapse, have taken extraordinary steps to ensure that the "state of exception" spawned by the 9/11 provocation remains a permanent feature of daily life here in the heimat.

And with moves by Barack Obama's "change" regime to strip Americans of their Miranda rights, "delay" their appearance before a lawful court should they be accused of a national security crime, or even assassinate them if an arm of the secret state fingers them as terrorists (evidence optional), it's a sure bet that as "ideas about security infect virtually all aspects of public policy," as Stephen Graham avers in Cities Under Siege, new silver bullets will be needed to "keep us safe."

Deep Learning: A Nerdy Way to Kill People

Long-time readers of Antifascist Calling are well-aware of the host of bizarre projects hatched in darkness by the Pentagon's geek squad, the Defense Advanced Research Projects Agency (DARPA).

Working on things like Biologically Inspired Platforms and Systems that investigate the natural world, the better to create "significant new defense capabilities," the Defense Sciences Office (DSO) is focused "on understanding, and then emulating, the unique locomotion and chemical, visual, and aural sensing capabilities of animals," in order to hand warfighters neat, new tools to kill people.

Think robo-insects that crawl up walls and fire a bullet into the head of an unsuspecting "terrorist"–or more likely these days, some dissident, journalist or whistleblower–peacefully tucked in for the night.

But biologists and neuroscientists aren't the only ones in on the fun: computer specialists and systems' designers, you too can fight the War On Terror!

One new project, Deep Learning, on tap from the Information Processing Techniques Office (IPTO), proposes to "build a universal machine learning engine that uses a single set of methods in multiple layers (at least three internally) to generate progressively more sophisticated representations of patterns, invariants, and correlations from data inputs."

DARPA avers that "a rapidly increasing volume of intelligence, surveillance, and reconnaissance (ISR) information is available to the Department of Defense (DOD) as a result of the increasing numbers, sophistication, and resolution of ISR resources and capabilities. The amount of video data produced annually by Unmanned Aerial Vehicles (UAVs) alone is in the petabyte range, and growing rapidly."

Therefore, "The goal of the envisioned Deep Learning program is to discover and instantiate in a learning machine (Deep Learning System) a single set of methods that, when applied repeatedly across multiple layers of the machine, yield more useful representations of audio/visual, sensor, and language information, using less labeled data more efficiently than any existing technologies."

Though top-heavy with nerd factor, Katie Drummond at Wiredreports that IPTO is hungering after a system that "can spot activities, like running, jumping or getting out of a car." Ultimately, the "final version will operate unsupervised, by being programmed to hold itself accountable for errors–and then auto-correct them at each algorithmic layer."

DARPA's solicitation envisages Deep Learning as an exemplary means for America's robo-warfighters to autonomously sort out those petabytes of data and then provide CIA and Pentagon drone "pilots" or JSOC kill squads, a more efficient way to snuff out shadowy practitioners of "asymmetric warfare," women, children, the elderly, journalists, etc., you know, the usual suspects.

I can't help but wonder whether its "auto-correcting" algorithms and capacity for holding itself "accountable for errors" means it will deliver itself–or its human masters–to The Hague for the commission of war crimes. A syrupy sweet synth-voice purring "sorry" to splattered human remains of a Hellfire missile strike gone awry just won't cut it in the liability department.

SMITEing America's Enemies

But before one can "kill 'em all, and let God sort them out," bulletproof target sets require corroboration. What better way to name that enemy then by ginning-up yet another sophisticated computer algorithm to delivers the goods!

The indefatigable Lewis Page of Britain's gadfly tech-zine, The Register, reported May 19 that "Pentagon boffins want nothing less than some kind of automated witch-finder technology able to finger 'increasingly sophisticated malicious insider behavior' in the USA."

And why not? After all, the U.S. National Counterintelligence Strategy (NCIS) has proclaimed that "Trusted insiders … are targeting the U.S. information infrastructure for exploitation, disruption, and potential destruction." Or leaking documents that might prove embarrassing to the secret state such as theCollateral Murder video posted in April by Wikileaks.

Accordingly, DARPA is hatching a project, the sinisterly titled Suspected Malicious Insider Threat Elimination, or SMITE, to detect those who might not want us kept safe. DARPAcrats "define [an] insider threat as malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems and sources."

The RFI posted online declares that "Information systems security personnel are drowning in ever expanding oceans of observational data from heterogeneous sources and sensors from

which they must extract indicators of increasingly sophisticated malicious insider behavior."

Heavens! With a new panic on the horizon, call it a much-dreaded ISR and "malicious insider behavior analysis gap," the IPTO gang must surely be working overtime!

Since the "fundamental challenge" (aside from discovering new ways to line the pockets of America's security grifters) "is one of finding a poorly understood, subtle, or hidden signal (indicators of malicious behavior) buried in enormous amounts of noise (observational data of no immediate relevance) under the constraint that the measures of significance are themselves moving targets (based on dynamic context) that must be continually monitored and updated."

Doubtless, there's always a danger some pissed-off contractor at any of the 16 alphabet soup agencies that comprise the U.S. "Intelligence Community," forced to cancel a night on the town with that hot babe over in data mining, just might "go rogue" and become a "malign insider." Fear not, if DARPA has its way (and enough cash can be discretely passed in plain brown envelopes to trusted insiders!) "the challenge" of "detecting deceptive behavior" can be mastered.

Since "deceptive behavior is characteristic of malicious intent which leads to the problem of assigning intent to observed behaviors," better observe and analyze everything!

What better means then, to separate the "insider threat" wheat from the chaff then to "(a) derive information about the relationship between deductions, the likely intent of inferred actions, and suggestions about what evidence might mean and (b) dynamically forecast context-dependent behaviors–both malicious and non-malicious."

Or, as Donald Rumsfeld blithely put it on that halcyon day when the Twin Towers fell: "Need to move swiftly – Near term target needs – go massive – sweep it all up. Things related and not."

And who would blame DARPA for lusting after "on-line and off-line algorithms for feature extraction and detection in enormous graphs (as in billions of nodes) as well as hybrid engines where deduction and feature detection mutually inform one another"?

After all, what with "missed signals" and various failures to "connect the dots" before 9/11 or intelligence "gaps" that drove the Bush administration kicking and screaming into an invasion and occupation of Iraq it didn't want, "security is often difficult because the defenses must be perfect, while the attacker needs to find only one flaw."

Therefore, IPTO's enterprising specialists will place a premium on "forensics" that "could reverse the burden by requiring the attacker and his tools to be perfect, while the defender needs only a few clues to recognize an intrusion is underway."

With such tools in hand perhaps the secret state, laboring like proverbial bees in the geopolitical gardens of the Middle East to efface the looming Iran "threat," will have the means to sequester some potential whistleblower before they'd eventhink about leaking compromising documents that might throw a spanner in the works.

"It will no doubt be a comfort for anyone in a position of trust within the U.S. information infrastructure," Page points out, "to know that mighty military algorithms and hybrid engines will soon sniff your every move so as to forecast any context-dependent malice on

your part–and then in some unspecified way (remember what the E in SMITE stands for) eliminate you as a threat."

And should DARPA's info-warriors fail, there's always a black hood, a silent room and a waterboard to do the trick!

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/