



54006
92000

1005
99
50
{555}

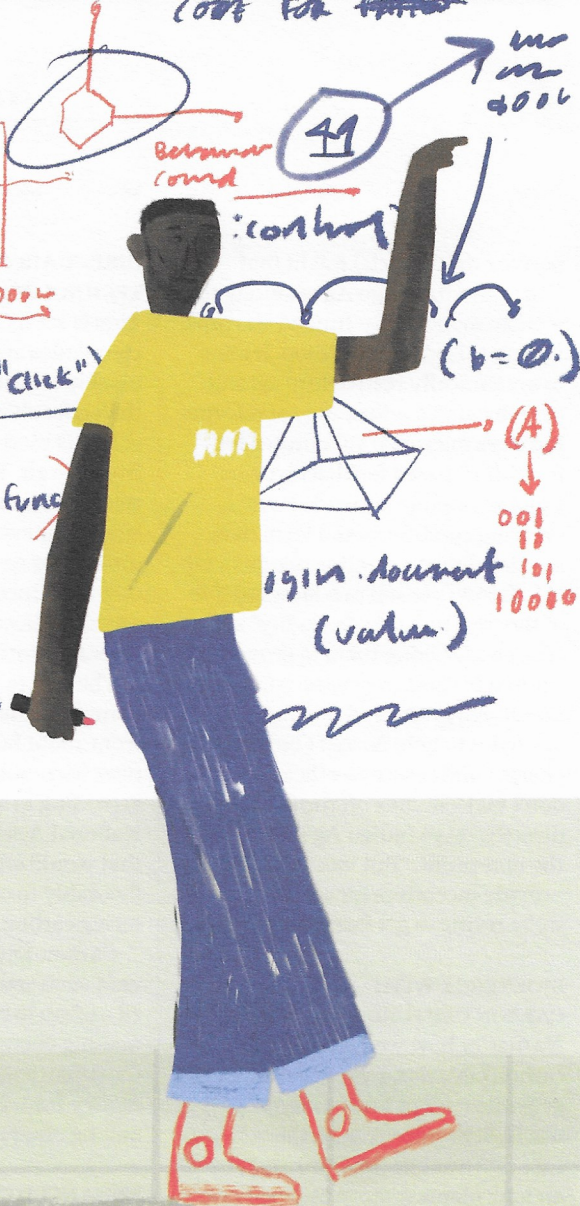
440000

{ -1 ("click")

[balut

STATE = nil

WEAPON



Behavior
cond

:control

RAM

origin document
(value)

(A)

001
10
101
10000

(b=0.)

no
in
4006

41

cost for tattoo



Commercial Talent for Government Weapons: The New Industrial-Military Complex

Technologies for weapons are increasingly coming from business

▼ by Tam Harbert ▼ Illustration by Luke Best

Since the dawn of mankind, whenever people invented something useful, like using a bone for a hammer, it didn't take long before they turned around and hit their neighbor with it. So it should come as no surprise that nations are turning today's technologies into weapons.

And yet, it has, especially for employees at Google, Microsoft, Amazon and other tech companies. In the last two years, many of them have publicly objected to the use of their creations for warfare, domestic surveillance and other applications they consider immoral or unethical.

The resistance comes as the U.S. military tries to woo companies with both a charm offensive and a slate of lucrative contracts, including a gigantic \$10-billion, 10-year Pentagon cloud computing contract called Joint Enterprise Defense Infrastructure. (Microsoft won, beating Amazon.) Silicon Valley culture – rich in innovation and lightning quick to capitalize on it – has led companies to excel in technologies like autonomous driving that are valuable not only in commercial markets – cars and trucks – but also in the military – tanks and drones. Meanwhile, cutting-edge tech development by and for the military has stagnated. The traditional military-industrial complex, in which large prime defense contractors like Raytheon and Lockheed Martin spend years developing a new fighter jet or aircraft carrier, doesn't work well for many emerging technologies.

"The reality is that the expertise and the talent is largely in the commercial world," says Brian Schimpf, co-founder and CEO at Anduril Industries, an AI company that focuses on selling to the military. "Very few folks who are experts in leading technologies are going to the traditional defense companies." We may be heading toward a new "industrial-military complex," in which, for better or worse, business remains decisively ahead of government in creating new sorts of technologies that can also serve as powerful weapons.

That talent and technology gap between commercial and military applications is worrisome, especially when tensions between nations are on the rise, fanned by trade disputes, immigration and cyberattacks. "My concern is not just for the military,

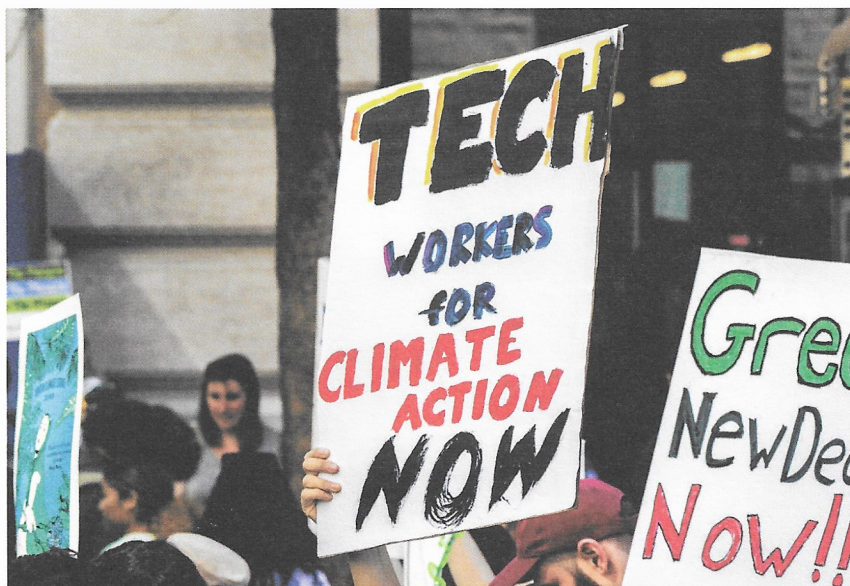
it's also for our national economic competitiveness," says Adam Jay Harrison, an entrepreneur who until recently served as command innovation officer at the U.S. Army Futures Command, an organization the Army created last year to speed new product development and court tech startups. Harrison says it's always been a symbiotic relationship. Many commercial products today use foundational technologies, like GPS and drones, originally developed for the military. Microwave ovens emerged from radar technology developed during World War II. The first one, introduced in 1946 by Raytheon, was named the Radarange.

Amazon CEO Jeff Bezos said last fall.

While Bezos's statement reflects tech industry arrogance, it does go to the heart of the issue. Tech companies and the military need to find better ways to work together, to enable the development of cutting-edge technology that protects the United States without alienating the engineers that invent it. And they delay to our peril. Other countries such as China and Russia are pressing ahead on such technologies with no regard for approval from engineers or citizens.

TECH WORKERS DON'T LIKE THESE "TERMS OF SERVICE"

Part of the problem is that tech-



Tech company workers have been expressing their opinions more loudly.

"If you remove military problems from things that are being actively pursued by civilian innovators, we could miss the things that will drive the next technology revolution," says Harrison. Some prominent tech CEOs agree, but view the problem through the opposite lens. "If big tech companies are going to turn their back on the U.S. Department of Defense, this country is going to be in trouble,"

nology companies and their workers didn't anticipate the allure of military contracts. Now the in-house conscientious objectors complain that nobody ever asked them for permission to use their work this way.

Some companies acquiesce to employee concerns. In summer 2018 Google withdrew from the Defense Department's Project Maven, which uses AI to help target drone strikes, after thousands of employees signed a petition saying the company "should not be in the business of war."

Amazon workers protested the sale of facial recognition software to law enforcement and demanded the company kick Palantir off its AWS cloud service. That highly-funded Silicon Valley startup co-founded by investor Peter Thiel supplies data mining technology for Immigration and Customs Enforcement's deportation and tracking program.

Palantir employees, too, are beginning to protest. According to *The Washington Post*, a group of them petitioned management to give profits from an ICE contract to charity.

ETHICAL LINES ARE BLURRY

Such developments have prompted soul-searching at some tech companies, which are trying to figure out where to draw the line. After Google pulled out of DOD's Project Maven, the company published a set of AI ethics principles, which outlined its views on responsible AI development and specifically said it would not design or deploy AI for weapons. But protests continue. In August 2019, 600 Googlers published a petition asking Google to "publicly commit not to support Customs and Border Protection, Immigration and Customs Enforcement or the Office of Refugee Settlement with any infrastructure, funding, or engineering resources, directly or indirectly, until they stop engaging in human rights abuses."

Some tech employees are quitting. One high-profile case was Meredith Whittaker, a Google program manager who helped organize employee protests. "Making sure AI is just, accountable, and safe, will require serious structural change to how technology is developed and how tech corporations are run," Whittaker wrote in a blog post announcing her resignation in July. "The use of AI for social control and oppression is already emerging, even in the face of developers' best of intentions."

On the other side of the country, Liz O'Sullivan resigned from Clarifai Inc., a New York-based company that

Business is ahead of government in creating new technologies that can serve as weapons.

specializes in AI visual recognition, when its CEO declined to pledge the company would not contribute to lethal autonomous weapons systems. Workers have a right to know what's being done with their innovations, says O'Sullivan, especially when they were originally developed for commercial applications.

Schimpf of Anduril, the defense AI company, agrees. Employees "absolutely have a right to know," he says. "I think it's actually a lack of transparency and a lack of honesty around how these things are being used that's causing the problem." That opaqueness is on both sides, he explains. "On the industry side, [they aren't talking about] military uses of these things, and on the military side, [they are] not being open about how they think about the technology, how its use will be limited, and their rules of engagement."

Maybe. But what happens when a commercial company sees a multi-million-dollar defense opportunity? Does it ask its employees first? "The AI strategy of the military is so essential for weaponized targeting and surveillance that you're seeing even companies with the best intentions getting sucked into it because it's so alluring," says O'Sullivan. "There is an infinite amount of money available to any company willing to push the state of the art forward."

SOFTWARE IS EATING THE MILITARY

When technology is software, it is almost impossible to predict exactly how it could be used. In the old

military-industrial complex, defense contractors built big hardware with a clearly-defined use, like a jet fighter. But the actions of a drone can be changed by tweaking the software, sometimes on the fly.

That's "a fundamental problem for autonomous weapons," writes Paul Scharre in his 2018 book *Army of None*. Scharre is a former U.S. Army Ranger who now works as director of the technology and national security program at the Center for a New American Security. "The essence of autonomy is software, not hardware," he continues, "making transparency very difficult."

AI is even more malleable, says O'Sullivan. "It's not like regular software development where functionality is deterministic and set," making its application clear, O'Sullivan says. With AI, "the very model that helps find people on rooftops for disaster rescue/relief can be the exact same model a general would use for targeting people with the intent to kill."

But O'Sullivan is getting firsthand exposure to the challenges of writing ethical guidelines for AI after co-founding a startup (which recently was still in stealth mode). It's much more complex than she realized, she admits. After all, a strong ethics statement may essentially eliminate certain market opportunities. That's hard enough for a large company, but monumentally hard for a startup hungry for revenue.

Meanwhile, it's not proving to be much easier for the Defense Innovation Board, a DOD advisory body that includes high tech luminaries like former Google CEO Eric Schmidt. The DIB is developing recommendations for DOD AI ethics principles. But at the group's July 2019 meeting, Schmidt noted how rapidly AI is advancing, asking "does a set of principles developed in 2019 apply in 2020?" He also noted the complications of potentially conflicting ethics. While the DIB will recommend ethics for the military, DOD "will rely ▶

on the private sector in many cases for the development of the technology, and...the private sector will be operating under its own set of ethical principles, or lack thereof, as it pursues the deployment of AI.”

THE ANSWERS AREN'T OBVIOUS

In short, there is no clear way forward. Anduril's Schimpf thinks his company's model, a kind of new breed defense contractor that applies Silicon Valley innovation and speed to military problems, is a solution.

But Harrison, who left the Army Futures Command in October 2019, disagrees. “There may be room for one company like an Anduril to unseat one of the big primes, but we're not going to be able to sustain 100 new, venture-backed companies,” he says. Despite lucrative military contracts, the DOD market is not big

enough to support a lot of VC investment, he explains. Instead, he thinks companies can benefit from seed money and early support from DOD: “Leverage the DOD as a starter market and then pivot your business into much larger, more scalable civilian opportunities.”

He acknowledges that that doesn't solve the employee ethics problem, but says the Army Futures Command is trying to build bridges and promote more conversation about such issues. It is in Austin, Texas, partly because the cultural gap between tech and military isn't too wide there, Harrison explains. It is even planning a panel on ethics, technology and warfare for next year's South by Southwest conference. “We are actually trying to take more of a leadership role, to have a conversation with folks that may have some of these alternate

perspectives,” he said just before he left the Army. “Partly, it's because we want to win them over as partners. But the other part is, it's hard to have a democracy when you don't have different parts of your citizenry engaging in meaningful conversations around hard topics.”

Meanwhile, activist and entrepreneur O'Sullivan thinks government regulation and oversight of technology may be the only way employees can be assured their work won't end up in objectionable applications. Like ethics, however, we remain in a gray zone where it's unclear who gets to decide what's objectionable. Virtually all of today's tech is like that prehistoric bone. It can be used to build up or to tear down, to save lives or to destroy them.

TAM HARBERT is a journalist in Washington.

Choosing Water As Part of a Healthy Lifestyle

At Nestlé Waters North America, we believe that choosing water is one of the healthiest choices people can make when deciding what to drink. The shift away from sweetened, caloric drinks to bottled water saved Americans up to 68 trillion calories from 2000 to 2015*. That is why we are proud of the role we play encouraging families and children to choose water – whether it's tap, filtered or bottled – as part of a healthy lifestyle.

But our role doesn't just end there. We are committed to providing these healthy options in a sustainable way – by caring for the water and the land around it, increasing our use of recycled plastic and looking for new packaging solutions.

At Nestlé Waters North America, water is our life's work.

* Beverage Marketing Corporation, 2016



The Healthy Hydration Company™
www.nestle-watersna.com



© 2019 Nestlé Waters North America Inc.