MIT Technology Review

The war and peace issue

Vol 122 No. 6 | Nov/Dec 2019 | $9.99 USD $10.99 CAD

The everything ~~store~~ war

Why Amazon is poised to become America's newest defense giant

Pioneering penis transplants for wounded veterans

p. 70

The fatal flaw that could make AI weapons useless

p. 44

Why high-tech war is immoral, by the author of *Jarhead*

p. 20

12
0 74808 01308 1

This issue asks: Can technology be a force for good even in something as evil as war?

Yes, says one school of thought. Today's weapons may be more lethal than ever, but it's thanks partly to their lethality and accuracy that advanced nations no longer send young men to kill each other by the tens of thousands.

Moreover, technology may be able to help predict emerging conflicts (as Tate Ryan-Mosley explains on page 12), and help repair the damage after those that do take place. Finally, of course, countless civilian technologies began life as military projects.

Today, for example, researchers are developing brain-computer interfaces that tomorrow's troops might use to control weapons with their minds. But the prototypes of those interfaces are allowing paralyzed people to regain the use of their limbs, as Paul Tullis reports (page 36). Similarly, Andrew Zaleski's inside account of the extraordinary surgical effort behind one of the world's first penis transplants (page 70) shows how medical advances for war veterans are likely to end up helping many civilians.

However, those same advances could have happened if some of the vast spending on military hardware (which Konstantin Kakaes lays out on page 34) went into peacetime research. And the costs of high-tech weaponry aren't only financial.

The proof of that is in Afghanistan, which this year surpassed Vietnam as America's longest-running war. While Vietnam threw the US into generational turmoil, Afghanistan is almost absent from the national debate. That's thanks in part to the drones that allow most American troops to stay at home.

Yet the drones' supposedly scalpel-like precision is a myth, Ali M. Latifi reports from Afghanistan (page 56): civilian casualties keep mounting, only sporadically monitored and investigated by either the US or the Afghan government. And in a powerful essay (page 20), Anthony Swofford, who served as a Marine in the Gulf War and wrote the memoir *Jarhead*, argues that advanced weapons like drones create a "moral distance" from the killing, and thus enable more of it.

Blind reliance on technology can go awry in other ways. The deep-learning algorithms that power a growing array of smart weapons contain basic flaws that could be exploited to turn them against their owners, writes Will Knight (page 44). Activists have used digital tools to document the Syrian regime's war crimes in unprecedented detail, reports Eric Reidy (page 64), yet it continues to commit them with impunity. Janine di Giovanni interviews a US paratrooper turned professor (page 30) and Britain's former top soldier (page 60) on the failures of international diplomacy and military strategy that technology can't fix. And Obi Anyadike reports from Nigeria on how techniques for "deradicalizing" violent extremists do little good when the social conditions that radicalized them remain unchanged (page 16).

IAN ALLEN

Gideon Lichfield is editor in chief of MIT Technology Review.

In our cover story on page 24, Sharon Weinberger shows how Amazon is cementing its influence in Washington by providing digital infrastructure for US intelligence and law enforcement, and aims to do the same for the Pentagon. Joan Donovan (page 48) explains how memes have gone from silly jokes to serious geopolitical weapons. Haley Cohen Gilliland looks at why dogs still make better bomb-sniffers than any electronic gizmo (page 40), and Patrick Howell O'Neill canvasses national security experts on how the US might respond to a real cyberwar (page 52).

Finally, a piece of short fiction by Jasper Jeffers, a serving US Army colonel, imagines a new breed of technologically augmented super-soldiers. Once again, the lesson is clear: when human judgment fails, no amount of technology can make war more successful, or more moral.

1

Strategy

2

Battlefield

3

Aftermath

Cover illustration by Tim O'Brien

Customer service and subscription inquiries

National
800-877-5230

International
903-636-1115

E-mail
customer_service@
mittechnologyreview.info

Web
www.technologyreview.com/
customerservice

MIT Records (alums only)
617-253-8270

Reprints
techreview@wrightsmedia.com
877-652-5295

Licensing and permissions
licensing@technologyreview.com

MIT Technology Review

One Main Street
13th Floor
Cambridge, MA 02142
617-475-8000

The mission of MIT Technology Review is to make technology a greater force for good by bringing about better-informed, more conscious technology decisions through authoritative, influential, and trustworthy journalism.

Technology Review, Inc., is an independent nonprofit 501(c)(3) corporation wholly owned by MIT; the views expressed in our publications and at our events are not always shared by the Institute.


DC
PWR
SLEEP

ZUMA PRESS

Strategy

1

IDs of march: US troops have made the capture of biometric data—including retina scans and fingerprints—part of their arsenal in countries like Afghanistan. So-called "identity dominance" is used to track insurgents, guard against infiltration, and control population movements.

Photograph by Louie Palu

Bringing order to chaos

Predicting conflict could save lives. Are we finally getting better at it? By Tate Ryan-Mosley

People have been trying to predict conflict for hundreds, if not thousands, of years. But it's hard, largely because scientists can't agree on its nature or how it arises. The critical factor could be something as apparently innocuous as a booming population or a bad year for crops. Other times a spark ignites a powder keg, as with the assassination of Archduke Franz Ferdinand of Austria in the run-up to World War I.

Political scientists and mathematicians have come up with a slew of different methods for forecasting the next outbreak of violence—but no single model properly captures how conflict behaves. A study published in 2011 by the Peace Research Institute Oslo used a single model to run global conflict forecasts from 2010 to 2050. It estimated a less than .05% chance of violence in Syria. Humanitarian organizations, which could have been better prepared had the predictions been more accurate, were caught flat-footed by the outbreak of Syria's civil war in March 2011. It has since displaced some 13 million people.

Bundling individual models to maximize their strengths and weed out weakness has resulted in big improvements (see "Inside a conflict model"). The first public ensemble model, the Early Warning Project, launched in 2013 to forecast new instances of mass killing (see "Where mass violence may strike next"). Run by researchers at the US Holocaust Museum and Dartmouth College, it claims 80% accuracy in its predictions.

Improvements in data gathering, translation, and machine learning have further advanced the field. A newer model called ViEWS, built by researchers at Uppsala University, provides a huge boost in granularity. Focusing on conflict in Africa, it offers monthly predictive readouts on multiple regions within a given state. Its threshold for violence is a single death (see "Ethiopia's ethnic violence").

Some researchers say there are private—and in some cases, classified—predictive models that are likely far better than anything public. Worries that making predictions public could undermine diplomacy or change the outcome of world events are not unfounded. But that is precisely the point. Public models are good enough to help direct aid to where it is needed and alert those most vulnerable to seek safety. Properly used, they could change things for the better, and save lives in the process.

Inside a conflict model

How an event turns into a model input

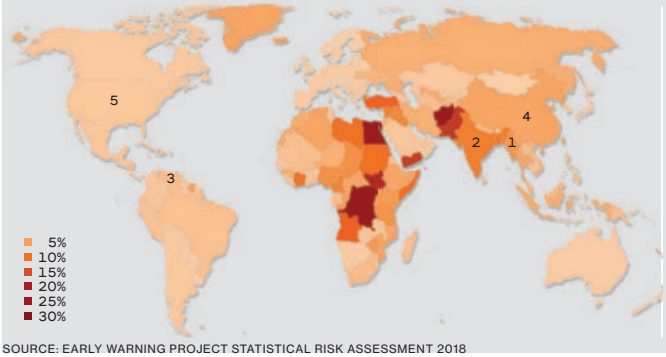
A death or protest occurs.

News agencies, NGOs, and others write about the event.

Monitoring systems scour the reports in search of keywords like "death," "protest," "uprising," or "massacre."

Relevant incidents are examined by human researchers, who code them according to the actors involved, the time and place, and an estimate of the data's precision.

- Distance to neighboring country
- Travel time to nearest city
- Distance to nearest petroleum resource
- Proportion of agricultural area
- Proportion of barren area
- Population size
- Recent deaths
- Recent protest
- Democracy
- Time since independence
- Proportion of population "excluded"
- Growth in GDP per capita



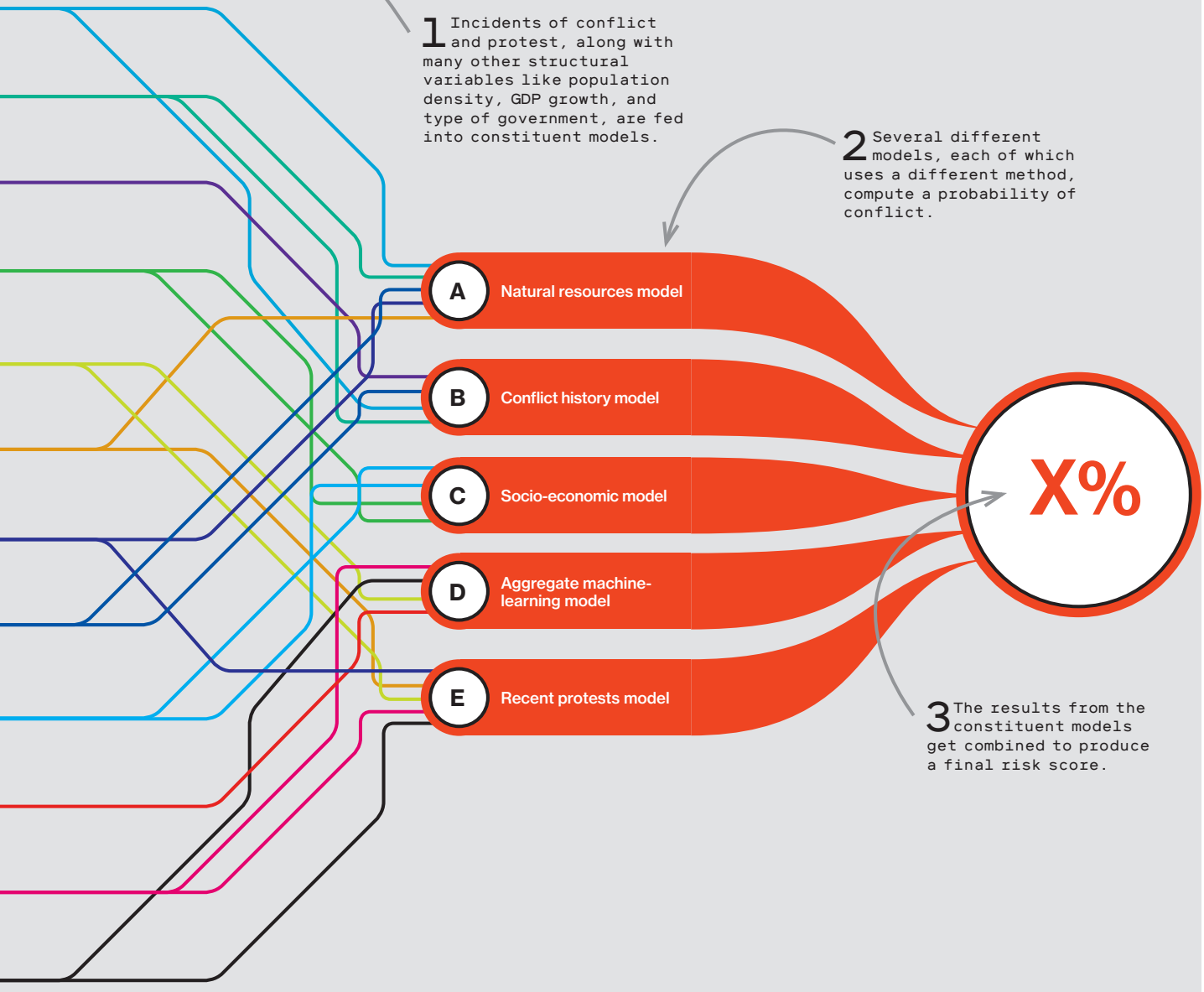
SOURCE: EARLY WARNING PROJECT STATISTICAL RISK ASSESSMENT 2018

Where mass violence may strike next

In the world of conflict prediction, there is a truism: the best predictor of violence is a history of violence. One illustration is the Early Warning Project's 2019 predictions for the sites of new mass killings, defined as the death of over 1,000 civilians in a year due to the deliberate action of armed groups (2020 figures weren't available at press time): the Democratic Republic of Congo, Afghanistan, India, and Myanmar rank among the 30 highest-risk countries.

The global rankings also highlight some of the model's shortcomings. Venezuela ranks low, despite a widely held belief that extrajudicial killings by security forces have been rife. So does the US, despite a rising threat of white supremacist gun violence.

The path from on-the-ground event to prediction requires complex analytical machinery, as this idealized conflict ensemble model shows.



1. Myanmar

Risk: 5.4% | Rank: 22

Myanmar's history of violence, its restrictions on movement, and its population size all contribute to a high risk of new mass killings. Its Rohingya Muslim minority is an ongoing target.

2. India

Risk: 7.8% | Rank: 14

In February 2019, a suicide bomber from Pakistan blew up Indian paramilitary trucks. Since then, new instances of violence have kept springing up, centered on the disputed region of Kashmir.

3. Venezuela

Risk: 1.5% | Rank: 55

A United Nations report in July 2019 suggested that the government had carried out more than 9,000 extrajudicial killings in the previous 18 months. The model didn't code them as systematic political killings, resulting in a lower risk rating.

4. China

Risk: 4% | Rank: 30

China's population size, limited freedom, and history of mass violence contribute to its risk of new mass killings. Tensions seem to be rising, as protests in Hong Kong have drawn accusations of police brutality.

5. United States

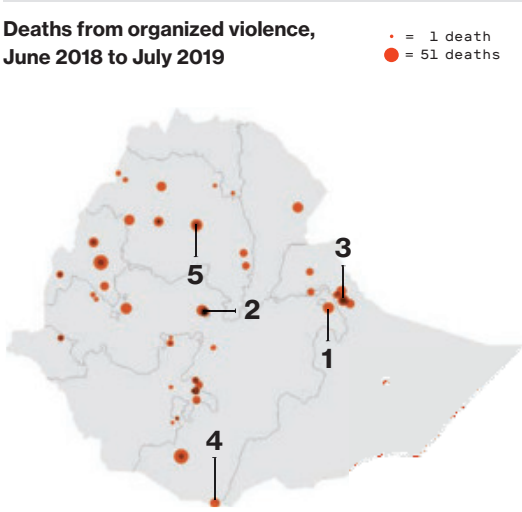
Risk: 0.8% | Rank: 80

In September, the US Department of Homeland Security recognized white supremacist terror as a national security threat. Several mass shootings targeting minority groups indicate a trend that the model doesn't capture.

Case study

Ethiopia's ethnic violence

Deaths from organized violence, June 2018 to July 2019



In April 2018, Abiy Ahmed was sworn in as prime minister of Ethiopia, promising to end years of ethnic unrest and antigovernment protests. Much of the international community thought Ahmed, who is of mixed Oromo and Amhara ethnicity, might usher in an era of unity and reform. But by December, ethnic violence had forced almost 3 million people from their homes.

Throughout the violence, which is still ongoing, Uppsala University's ViEWS model has been making predictions on what will happen in Ethiopia.

The results show how far the field of conflict prediction has come: ViEWS can forecast three different types of conflict risk—state-based, one-sided, and non-state—in a geographical grid with cells just 55 kilometers on a side and take into account even a single death attributable to organized violence. That kind of resolution, impossible just a few years ago, promises to make predictions far more useful to the United Nations and humanitarian organizations that are trying to help turn the tide back toward peace.

To better illustrate how this works, we've identified five key moments between June 2018 and July 2019 when conflict in Ethiopia escalated. We then compared them with ViEWS's output to see whether the violence was properly predicted ahead of time and how, when the model missed its guess, events changed its ensuing predictions.

BEFORE EVENT — **AFTER EVENT**

Probability of conflict July 2018: **17%** — **August 2018** — Probability of conflict October 2018: **17%**

Location 1 on map

The Ethiopian government moved to abolish the Liyu police force in the state of Somali—home to a large population of ethnic Somalis—and tried to oust its president. This set off a series of violent clashes.

The model had identified this particular region as having a very high risk of conflict—a 1 in 6 chance. That proved right.

August 2018: **1%** — **September 2018** — November 2018: **22%**

Location 2

Soldiers from the Oromo ethnic group, which make up a third of Ethiopia's population, returned to Addis Ababa after a conflict in Eritrea. Sectarian tensions boiled over, killing 35 people—most from other minority groups.

The model did not do well at predicting this. The capital, Addis Ababa, is generally at a lower risk of conflict thanks to relatively good infrastructure, policing, and economic growth.

October 2018: **1%** — **November 2018** — January 2019: **9%**

Location 3

Prime Minister Ahmed carried out a series of ethnically charged arrests across the country. Violence erupted between Oromo and Somali ethnic groups, resulting in 22 deaths in the eastern village of Tuli Guled.

The arrests were distributed across the country, and the country-level prediction for violence shot up to 67%. The model didn't precisely predict where the violence would occur, which accounts for the low score in this region.

November 2018: **7%** — **December 2018** — February 2019: **10%**

Location 4

A wave of violence hit restive Moyale in December after regional governments handed over security to the federal government. The violence culminated in a shooting inside a local hotel that claimed at least a dozen lives..

Refugees often flee from Ethiopia to Kenya through Moyale, and the Oromo and Somali ethnic groups have a history of clashing here. ViEWS correctly labeled the area as having a relatively high risk.

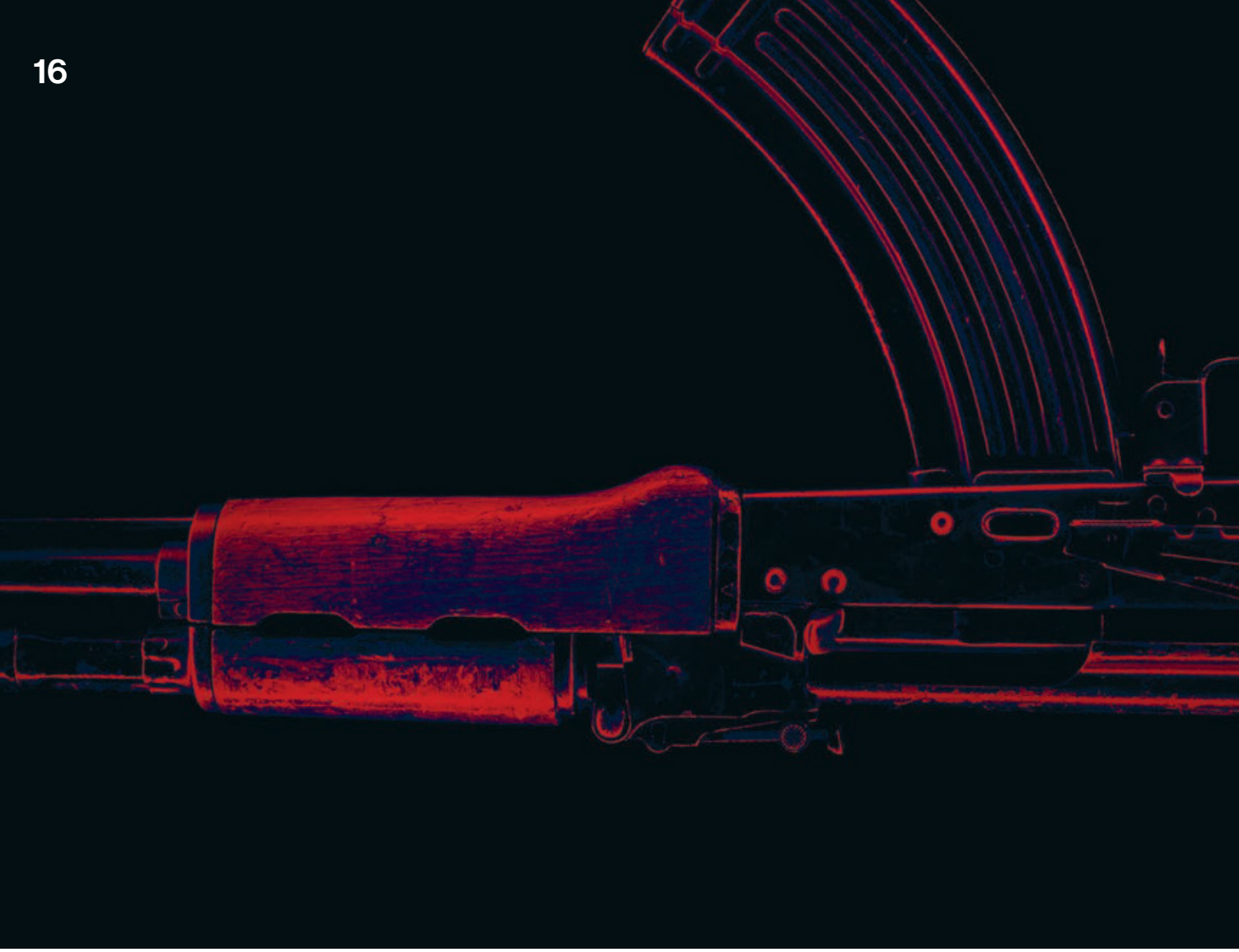
May 2019: **1%** — **June 2019** — August 2019: **14%**

Location 5

After an attempted coup against the Amhara state government by military leaders, the federal government ordered a five-day internet blackout. Police arrested over 250 people suspected of conspiracy in the coup, many belonging to the Amhara ethno-nationalist group.

Coups are, by their nature, hard to predict. The model did not foresee this one, but the probability of conflict rose dramatically after the coup.

SOURCE: VIOLENCE EARLY WARNING SYSTEM, UCDP GED; UPPSALA UNIVERSITY



Radical transformation

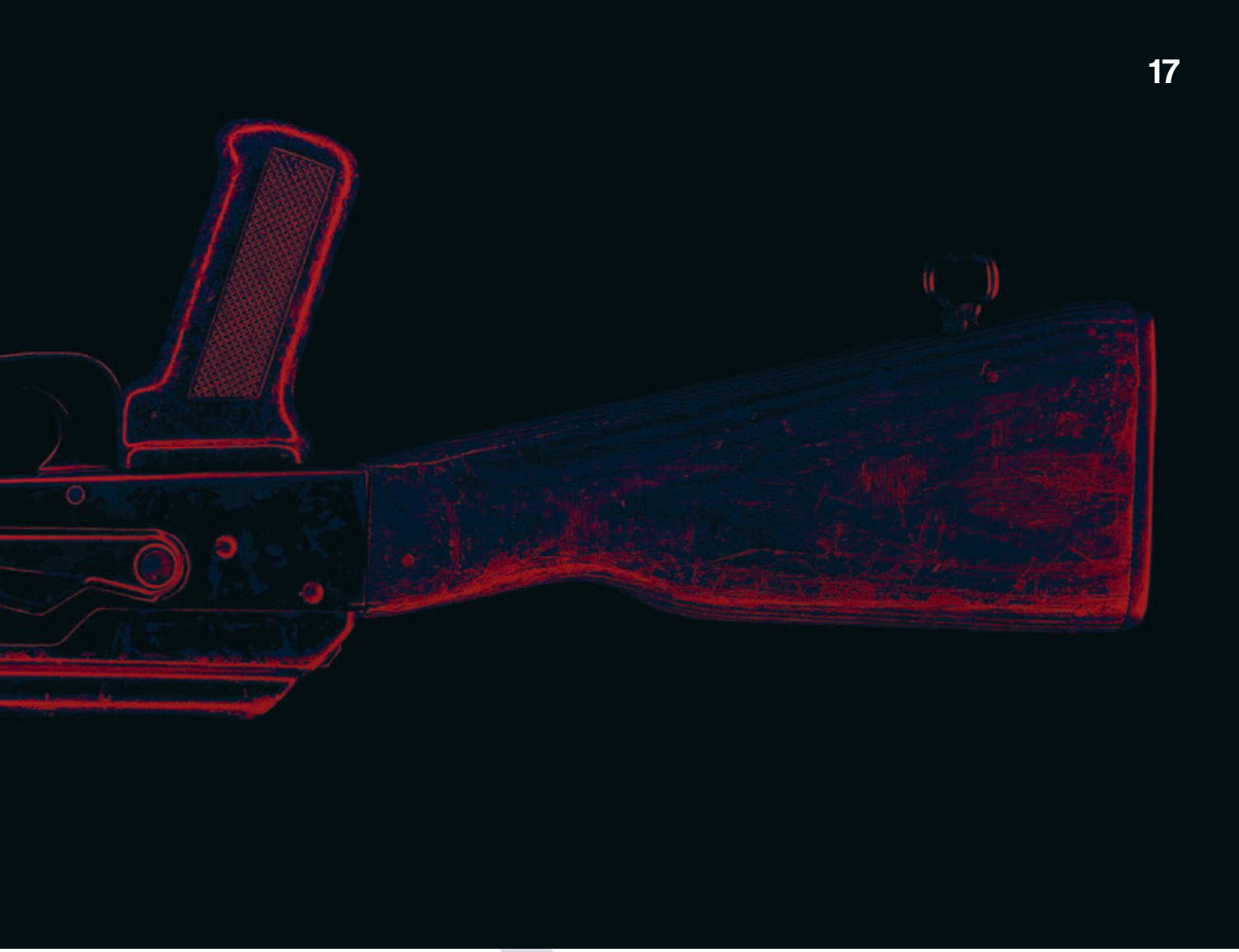
AFTER YEARS OF EFFORT TO PREVENT AND REVERSE RADICALIZATION, THE JURY'S STILL OUT ON WHETHER IT WORKS. BY OBI ANYADIKE

Malam Aminu is a slight, bespectacled man with a neat goatee and a disconcerting droopy eyelid that by turns makes him look sinister and then not quite all there.

When I first met him, in 2015, he was an inmate in Nigeria's Kuje Prison, and one of the most senior members of Boko Haram being held in custody. He was also one of 41 subjects in a new experiment being conducted by the government.

Faced with a difficult war against insurgents in the remote northeast, Nigeria had decided on a new strategy to tackle extremism: a mixture of amnesty, demobilization, and reprogramming to whittle away jihadist recruits. The idea was to undermine Boko Haram through bloodless attrition, not just by slugging it out on the battlefield.

The program was designed and run by Fatima Akilu, a soft-spoken psychologist who had trained in the UK and the US. She drew on prison-based schemes under way in Saudi Arabia, Singapore, and Australia, adapting them to Nigeria. The new approach involved changes across a range of policy areas: shifting the school curriculum to promote "critical thinking," overhauling a sclerotic justice system, tinkering with the health services so that psycho-social care could be expanded.



WIKIMEDIA COMMONS

"The solutions are as complex as the reasons for radicalism," Akilu told me.

The most visible part of her strategy, though, was in Kuje. Directed at prisoners who were convicted or suspected terrorists, it aimed at more than just getting detainees to renounce violence. Its goal was thorough deradicalization: totally expunging extremist beliefs, values, and behavior.

This represented an immense cultural shift for Nigeria. Its jails are notorious for their neglect and abuse of inmates, but in Kuje's "de-rad" wing—built with funds given to Nigeria by the European Union—the focus was different. The idea was to build a human connection between the alleged extremists—known as "clients" rather than inmates—and the wardens, who were retrained and renamed the "treatment team." Their job was to assess the needs of the militants under their care, and to identify the most effective ways to deprogram them.

When I first met Aminu, he was dressed in a crisp white dashiki and seated in an air-conditioned classroom in a new wing segregated from the rest of the overcrowded and unsanitary jail. Here on the de-rad side, clients were treated differently. They could wear their own clothes and had access to a new mosque, a sports area, and properly equipped vocational training programs. Not surprisingly, they were roundly hated by the hundreds of long-suffering regular inmates.

"We try as much as possible to help them," says Wahaab Akorede, the manager of the Kuje program. "We tell them we are not police or security—we're doctors. That's why it's called treatment."

Protect and prevent

Over the past 20 years, as detentions of terrorists have mounted around the world, a dizzying range of de-rad programs like the one in Kuje have sprung up in almost every major country. Authorities in Nigeria and elsewhere worried they were simply creating a revolving door if they released terrorists back into the community once their sentences had been served. Yet indefinite detentions, such those at Guantánamo Bay, weren't a popular or legal way to deal with the problem either. So began the explosion of post-crime deradicalization schemes.

Prison-based initiatives vary, from monitored informal chats with a local imam (a technique favored in Victoria, Australia) to structured models like that run by the government in Saudi Arabia. The Saudi approach includes a prison-based counseling phase,

rehabilitation therapy, and then post-release "aftercare"—all touted as something of a gold standard.

Riyadh claims recidivism is extremely low, but independent researchers are skeptical of the official numbers: there have been at least 11 high-profile cases of participants who have returned to terrorism. Saudi methods have also been questioned. For a start, participants are usually low-level supporters of dangerous organizations rather than hard-core militants. The program is also focused on preventing domestic terror attacks. It may therefore turn a blind eye to the export of jihad abroad, which means deradicalization "is not truthfully being achieved," wrote Tom Pettinger, a researcher at the University of Warwick, in a 2017 paper.

Other models, many of them in Europe, seek to prevent people from becoming radicalized in the first place. Britain's Prevent program, for example, seeks both to educate communities on the risks of radicalization and to stage interventions. Public workers in schools, universities, and local councils are required to report on anyone who shows radical tendencies, a system that the government says has diverted more than 1,200 people from extremism.

Increasingly, though, prevention efforts have focused on the internet. The web is seen as a dangerous shortcut to radicalization, providing "a cheap and effective way to communicate, bond, and network with like-minded movement members," says Daniel Koehler, founding director of the German Institute on Radicalization and De-Radicalization Studies.

Looking at former right-wing German extremists, Koehler found that the perceived anonymity of the internet encouraged people to take more extreme positions. Being part of a radical echo chamber online "creates a kind of ticking time bomb: a rapidly decreasing amount of alternatives and options in combination with an increasing amount of ideological calls for action," he says.

The argument is that the speed and saturation of online communication can easily accelerate radicalization. Stuck inside an information bubble, impressionable people are exposed to more and more extreme viewpoints until—finally—their activities shift to the next, horrifying level.

Twitter, Facebook, and YouTube have been visible parts of this machine, driven in large part by ISIS, which has placed great value in its social-media operations. At the height of the "caliphate" in 2014, it had teams devoted to creating and uploading ISIS-branded propaganda from Afghanistan to West Africa in a round-the-clock news cycle. In 2014, there were estimated to be between 46,000 and 90,000 active ISIS support accounts worldwide, both official and unofficial, in a variety of languages.

Most attempts to stamp out radicalism online have focused on shutting down the accounts of those who preach violence: Twitter claimed to have suspended more than 1.8 million accounts from 2015 to 2018. This has been effective when done rapidly and consistently. The ISIS presence on Twitter has diminished in quantity and visibility.

But taking down social-media accounts goes only so far, and there are many platforms for extremists to inhabit. Twitter is merely "one node in a wider jihadist online ecology," pointed out a study last year by British and Irish researchers on platforms' takedowns of terrorist material. Pro-ISIS users also favor services like Google Drive, Sendvid, and especially Telegram, where group "owners" have much greater control over membership and access.

Online obsession

Attempts to control or ban extremists online are repressive rather than preventative, but critics also say they end up displaying the biases of platform owners and the media rather than focusing on where the greatest threat is. ISIS has received disproportionate attention compared with other jihadist groups, for example. And only recently, in the wake of atrocities

GETTY

like the Christchurch mosque shootings in New Zealand, has the far right attracted attention, despite years of increasing white supremacist activity online.

There's also been a lot of attention and funding for fighting online activity compared with other avenues for radicalization. One reason is the "relative ease of creating and quantifying social media datasets compared to other forms of field work," wrote J.M. Berger, an author and analyst on extremism, in a paper last summer. Yet there are still no established causal links between online extremism and offline violence. A Unesco report in 2017 concluded that "social media constitutes a facilitating environment rather than a driving force for violent radicalization or the actual commission of violence." And a review of 227 convicted UK terrorists concluded that the vast majority of online extremists don't become terrorists. However, those who commit terrorist acts "regularly engage in activities in both [online and offline] domains," noted Elizabeth Pearson of Kings College, London, in a 2017 paper.

Finally, of course, there's little consensus on where to draw the line between extremism and what's merely offensive to some people or threatening to a certain group in power. That makes it easy for governments to suppress political speech in the name of clamping down on extremism—it's how China justifies the detention of more than one million Muslim Uighurs, for example.

Learning from the past

Whether they focus on technology or ideology, many de-rad and disruption programs have encountered trouble in the long term. Nigeria's fell out of favor when the government changed; it is now under the control of the military, with a far less strategic role.

In France, one early project was shut down amid protests from locals, and two other proposals have similarly struggled. Last year Prime Minister Édouard Philippe announced a fresh attempt at de-rad but admitted that the technocratic approach had been optimistic. "No one has a magic formula for deradicalization, like you might de-install dangerous software," he said.

This has led some governments to lean on older, more trusted tactics. Radio and TV programming are long-established ways of encouraging behavioral change. From Bosnia to Mali, research-driven storylines have been shown to slowly alter the values and behaviors of the audience. In northeast Nigeria, Radio Dandal Kura ("meeting place") broadcasts phone-ins, education programs, and peace messages across the region. It has been successful, not least at getting under the skin of Boko Haram: the movement's leader, Abubakar Shekau, released a video threatening its female presenters and calling them "prostitutes."

"No one has a magic formula for deradicalization, like you might de-install dangerous software."

The last time I saw Malam Aminu was in 2018. He was living quietly in a village in central Nigeria, having been released from Kuje—along with 14 other former jihadists—not long after we first met.

In the old days, he said, he believed that "if you were ready to use violence, you could achieve your aims." He wasn't radicalized by the internet, but by experience and outrage. He'd once been a senior commander in Boko Haram and a member of its *shura*, or consultative council. Now, though, he'd learned tolerance and knew how to listen to others' points of view. Much of this he attributed to Akilu, the psychologist at Kuje. He also said the imams on the treatment team eventually got him to reconsider his views.

But he remained firm in his core beliefs. The poverty of northern Nigeria and the indifference of the wealthy had stirred him to action, he explained, and he still thought the solution was strict *sharia*, Islamic law. What he disagreed with was Boko Haram's extreme violence. He had fallen out with Shekau, questioning his religious knowledge, strategy, and tactics.

But living outside the prison again, he felt abandoned by the Nigerian government. Akilu had privately paid for him to go back to school, but there had been no reintegration package from the government, not even a parole officer to report to. One day he was in jail; the next he had to fend for himself.

Six of the men who were freed from Kuje with him were "his boys," and he stayed in touch. Three have since rejoined Boko Haram. He said it wasn't necessarily ideological: one of them—a man I'd been introduced to in Kuje as "the Commander"—had been rejected by his family and was sleeping on the streets. His former comrades found him and persuaded him to rejoin.

Aminu said he would not return to violence. But his beliefs would still be considered radical by most. "It's only because I've repented," he told me. "[It's] the reason why I don't backslide."

I couldn't help wondering whether it wasn't in fact Boko Haram that had left him.

Obi Anyadike is a journalist and researcher based in Kenya, and editor at large for The New Humanitarian.

WHY CLEAN WAR IS BAD WAR

By sanitizing warfare, technology eliminates accountability for how, when, and why we fight, argues the author of *Jarhead*.

Shortly after I turned 18, the United States Marine Corps trained me to live, think, and operate as one of the most lethal humans walking the earth. They transformed me from a typical suburban American kid into their ideal fighting machine through a perfected, scientific regimen of psychological rewiring, physiological restructuring, and moral recoding. After 10 months in the grunt lab, I was assigned to an infantry battalion. I operated with a new kinesiology of the body and soul that had not only prepared me for war but created a thirst for any brand of conflict. I had an understanding of what perfection on the battlefield would look, sound, and taste like. I had become a Battle Bot.

My lethality increased with each personnel addition: from me, the rifleman, to the four-man fire team, the squad, the platoon, the company, the battalion. Each time, add new men, add new hunger, more firepower, more expertise, more technology with which to lay waste to the enemy. As the fighting organism grows in size, so does the inability to pause mission and consider whether the killing is just or moral: the killing *just is*.

By **Anthony Swofford**

Swofford, circa January 1991, at 1st Marine Division headquarters in Saudi Arabia.


R

Every generation of American warfighters is handed excellent new gadgets with which to wage war. And who doesn't love a new toy? Their creators become fabulously rich developing, training the military on, and helping deploy the newest technology. The tech often acquires catchy nomenclature and is extremely effective at killing large numbers of people: think of the MOAB, Mother of all Bombs. Fat Man. Hellfire. Sidewinder.

During Operation Desert Shield, the Barrett .50 caliber semi-automatic sniper rifle arrived in the Saudi Arabian desert where I and my battalion and tens of thousands of other American forces waited for war with Iraq. At the time the military possessed only a few dozen of the weapons, and my sniper team partner and I were two of a select group trained to deploy the Barrett in combat for the first time.

A celebratory, even giddy atmosphere took over the remote desert range that had been purpose-built for us and this new weapon. Division-level officers came out to watch us train. We were served three hot meals a day. At night we burned massive bonfires and discussed our imminent march to war.

My partner, Johnny, was a sergeant, a division-level, school-trained sniper, and—truthfully—a better shot than I was. With the Barrett we both hit iron targets out at 1,600 to 1,800 yards. The shooting was easy. The shooting was fun. We had been gifted this weapon that extended our dark arts by nearly a thousand yards. The Geneva Convention banned us from using a .50 caliber weapon on a human target, so the official reason the weapons had been released to us was to stop enemy vehicles. But we all knew the best way to stop a vehicle is to kill the driver. The technology told us so. And we listened to the technology.

Had I been given the chance, I would have used the Barrett on a human target. Specifically, on his head. At night, sleeping under our Humvee, I dreamed of observing an Iraqi convoy through my scope. Johnny and me in a sniper hide a thousand yards away. Johnny my spotter, me on the Barrett. I fire and put a round into the head of the driver of the first truck and then methodically kill more men from this God-like distance with this menacing new rifle. The Barrett's technological enhancement of my sniping skills made me more lethal, and more morally compromised, if only in theory and in dream.

Many now profess that the young Marine or soldier with a rifle is obsolete. The greatest weapons race of all is among academic scientists trying to win DARPA funding for new warfighting technology they insist will require scant human interface with the killing act, thus relieving the combatant of the moral quandary and wounds of war. Private-sector startups sell a myth of smart war through AI, or robotic soldiers. In labs where the newest and cleanest ways to kill are being invented, the conversation is not about the morality of going to war, but rather the technology of winning. But when you rely on a myth of technology and distance killing to build a rationale for easy war, your country will lose its soul.

"The enemy meets us where we are weak," an Air Force pilot friend told me once. In Vietnam, America's advanced bombers were ambushed by North Vietnam's lower-quality aircraft, Russian-built MiGs. We should not have lost as many aircraft and pilots as we did.

In Afghanistan, over 18 years of war, we have learned that the Taliban, al Qaeda, and ISIS do not regularly present en masse on the battlefield. The most technologically advanced military in the history of the world cannot claim victory against an enemy that chiefly employs small arms and shoulder-launched grenades and missiles and basic guerrilla tactics. They are nearly impossible to pinpoint, despite our billions of dollars of surveillance satellites and drones. Mostly we find the bad guys with a little bit of luck or a cash payment to a village elder. Paper technology.

Sophisticated weapons systems have one drawback: the enemy must expose himself within the effective killing range in order for the weapon to work as intended. The smart combatant, of course, rarely exposes himself. So when we do home in on enemy fighters, we use a $30 million aircraft to drop a JDAM (joint direct attack munition) and kill a dozen guys living in tents on the side of a mountain. What has that $30 million technological advantage bought us? The highly (and expensively) trained aviator piloting a beautifully complex flying and killing machine just extinguished some men living under canvas and sticks, men with a few thousand rounds of small arms ammo at their disposal. The pilot will return to his expensive air base or carrier. He will have a hot shower, eat hot chow, Skype his wife and children, maybe play some Xbox, and hit the gym

"We allow technology to increase moral distance; thus, technology increases the killing."

Swofford's platoon, around April 1991, somewhere in the Saudi Arabian desert. The author is front row, third from left. His sniper team partner, Sergeant John (Johnny) Krotzer, is second from left.

COURTESY PHOTOS

before he hits the rack. He will not, nor will he be asked to, concern himself with the men he killed a few hours ago. And in a draw or valley a few klicks away from where the pilot's munitions impacted, there is another group of men living under extremely basic circumstances, eating boiled rice and maybe a little roasted meat. They will ambush an American convoy or attack a government-friendly village in the morning. Native grit debases our technologically superior forces and materiel. Native grit wins a war.

Imagine if 9/11 had included a ground invasion by a technologically superior enemy. Imagine if they still occupied your city: you and your children would have fought a battle today, with bricks, rifles, and roadside bombs. The attacks on 9/11 activated an American impulse that had been dormant for decades: the will to defend home territory. But since World War II that will, whether real or manufactured by political and journalistic spin, has not translated to a military victory on foreign soil.

The reality is that it's difficult to locate the morality of and passion for defending an American military outpost built overseas out of Hesco barriers and Geocells. The enemy will hit us where we are weak, and we are weak inside a military compound infiltrated by a single Taliban fighter wearing an Afghan army uniform. His father or brother died on that mountain the other day, or a year ago, or 15 years ago. Inside the base wire we think we are strong and safe, but actually we are weak because we lack a moral necessity for being there. The Taliban fighter fires an AK-47 with a 30-round magazine and kills a few unarmed Americans—a soldier, a CIA operative, a military contractor—plus a friendly Afghan soldier.

We are incapable of stopping this attack because it was not hatched in a university weapons lab funded by DARPA; it was born on the side of a mountain or in a village 100 or more years ago. The impulse for the retaliatory strike is in the young man's DNA and in the dirt and rain and crops of his home place. Lethal soldiers with lethal weapons have trampled his country and kin for decades—centuries, even. We will never out-tech the deepest passion to persevere and claim victory and sovereignty over one's own land for one's own people.

At the street level, war is a people business. And people are complex. They are also fragile. Their bodies break, crumble, split open, and cease operating with surprising ease when met with the awesome newest war technology. The reality of a war-dead civilian or combatant is not changed by how advanced the tool was that delivered the fatal assault to the body.

The lust for new defense technology is an insidious attempt to distance ourselves and our leaders from the moral considerations and societal costs of waging war. It's not so much about the newest tools—swarm drones, exoskeletons, self-guided sniper projectiles. It is that this reliance on technological cool, the assumption that it lessens or alters the lethality of war, allows zero accountability for how, when, and why we fight.

This is not an anti-intellectual or anti-technology argument. I am not a grunt who thinks wars can only be won with boots on the ground. However, all wars must eventually be won with boots on the ground. The problem is not the technology, but the equivocation that high-tech military armament invariably invites. If fighting war is like swiping your smartphone for an order of groceries or posting a meme to Instagram, how bad can it really be? And if a politician is seduced by the lies and supposed ease of technological warfare and leads us into a mistaken conflict, is it really his or her fault? Didn't we all think it would be a breeze?

The moral distance a society creates from the killing done in its name will increase the killing done in its name. We allow technology to increase moral distance; thus, technology increases the killing. More civilians than combatants die in modern warfare, so technology increases worldwide civilian murder at the hands of armies large and small.

The person with the least amount of distance from the killing—typically an infantryman or special operator—is the most morally stressed and compromised individual in the war's chain of command. When close-quarters combatants understand that the killing they have practiced is not backed by a solid moral framework, they question every decision taken on the battlefield. But they also question the meaning of the fight. They count their dead friends on one or even two hands. They count the men they have killed on one or two hands, or by the dozen. The moral math will not compute.

The photos and videos of war on our television screens, on our computers, on our smartphones, tell us nothing about the moral computations of the warfighter. The warfighter understands that when a friend is killed on patrol, that is just part of the package. Another part of the package is going back out on another patrol tomorrow. But as you live and operate for longer in a hostile environment, your hatred of the enemy increases and your trust in leadership decreases. You create a moral wound against yourself.

War was supposed to be easy or fast, because of smart bombs and the latest bit of warfighting technology. But this means nothing when years later you only see dead men, women, and children when you try to sleep.

When we believe the lie that war can be totally wired and digitized, that it can be a Wi-Fi effort waged from unmanned or barely manned fighting apparatus, or that an exoskeleton will help an infantryman fight longer, better, faster, and keep him safe, no one will be held responsible for saying yes to war. The lie that technology will save friendly, civilian, and even enemy lives serves only the politicians and corporate chieftains who profit from war. The lie that technology can prevent war, or even create compassionate combat, is a perverse and profane abuse of scientific thinking.

Anthony Swofford is the author of the memoirs Jarhead and Hotels, Hospitals, and Jails and the novel Exit A.


amazon

THE EVERYTHING ~~STORE~~ WAR

BY SHARON WEINBERGER

AMAZON HAS SPENT A DECADE GETTING READY TO BECOME ONE OF THE WORLD'S BIGGEST NATIONAL SECURITY CONTRACTORS. HERE'S HOW IT HAPPENED—AND WHY.

ILLUSTRATIONS BY PABLO DELCAN

In July, when President Donald Trump was in the Oval Office with the Dutch prime minister, he took a few moments to answer questions from reporters. His comments, in typical fashion, covered disparate subjects—from job creation to the "squad" of congresswomen he attacks regularly to sanctions against Turkey. Then a reporter asked him about an obscure Pentagon contract called JEDI, and whether he planned to intervene in it.

"Which one is that?" Trump asked. "The Amazon?"

The reporter was referring to a lucrative and soon-to-be-awarded contract to provide cloud computing services to the Department of Defense. It is worth as much as $10 billion, and Amazon has long been considered the front-runner. But the deal was under intense scrutiny from rivals who said the bid process was biased toward the e-commerce giant.

"It's a very big contract," said Trump. "One of the biggest ever given having to do with the cloud and having to do with a lot of other things. And we're getting tremendous, really, complaints from other companies, and from great companies. Some of the greatest companies in the world are complaining about it."

Microsoft, Oracle, and IBM, he continued, were all bristling.

"So we're going to take a look at it. We'll take a very strong look at it."

Shortly afterwards, the Pentagon put out an announcement: the contract was on hold until the bid process had been through a thorough review.

Many saw it as yet another jab by Trump at his nemesis Jeff Bezos, the CEO of Amazon and owner of the Washington Post. Since arriving in the White House, Trump has regularly lashed out at Bezos over Twitter—blaming him for negative press coverage, criticizing Amazon's tax affairs, and even griping about the company's impact on the US Postal Service.

After all, until just a few months ago most Americans had never heard of JEDI, much less cared about it. Compared with efforts to build large fighter aircraft or hypersonic missiles—the kinds of headline military projects we're used to hearing about—the Joint Enterprise Defense Infrastructure program seemed downright boring. Its most exciting provisions include off-site data centers, IT systems, and web-based applications.

Perhaps it's equally mundane that Amazon would be in the running for such a contract. It is, after all, the world's leading provider of cloud computing; its Amazon Web Services (AWS) division generated more than $25 billion in revenue in 2018.

But Trump's diatribe wasn't just about a contract war between a handful of technology companies. It was a spotlight on the changing nature of Amazon and its role in national security and politics. The company has spent the past decade carefully working its way toward the heart of Washington, and today—not content with being the world's biggest online retailer—it is on the brink of becoming one of America's largest defense contractors.

> "What if we were to take advantage of all these incredible solutions that have been developed and driven by people who have nothing to do with the federal government?"

RETURN OF THE JEDI

The Sheraton Hotel in Pentagon City, a neighborhood adjacent to the Department of Defense, feels a world away from the ethos of Silicon Valley and its fast-moving startup culture. In March 2018, the 1,000-seat ballroom of the 1970s-era brutalist hotel was packed with vendors interested in bidding on JEDI. As the attendees sat in tired King Louis–style ballroom chairs, a parade of uniformed Pentagon officials talked about procurement strategy.

For the Beltway's usual bidders, this was a familiar sight—until Chris Lynch took the stage. Lynch, described by one defense publication as the "Pentagon's original hoodie-wearing digital guru," was sporting red-framed sunglasses pushed up above his forehead and a Star Wars T-shirt emblazoned with "Cloud City."

He had arrived at the Pentagon three years earlier to freshen the moribund military bureaucracy. A serial entrepreneur who worked in engineering and marketing in Seattle, he quickly earned the enmity of federal contractors who were suspicious of what the Pentagon planned to do. Some took his casual dress as a deliberate sneer at the buttoned-up Beltway community.

"There's a place for that and it's not in the Pentagon," says John Weiler, the executive director of the IT Acquisition Advisory Council, an industry association whose members include companies hoping to bid on JEDI. "I'm sorry, wearing a hoodie and all that stupid stuff? [He's] wearing a uniform to kind of pronounce that he's a geek, but really, he's not."

Even those who weren't offended thought Lynch made it clear where his preferences lay—and it wasn't with traditional federal contractors.

"What if we were to take advantage of all these incredible solutions that have been developed and driven by people who have nothing to do with the federal government?" he asked during his speech to the packed ballroom. "What if we were to unlock those capabilities to do the mission of national defense? What if we were to take advantage of the long-tail marketplaces that have developed in the commercial cloud industries? That's what JEDI is."

The Pentagon had certainly decided to make some unconventional moves with this contract. It was all going to a single contractor, on an accelerated schedule that would see the contract awarded within months. Many in the audience inferred that the deal was hardwired for Amazon.

Weiler says the contract has "big flaws" and that the Pentagon's approach will end up losing potential cost efficiencies. Instead

of having multiple companies competing to keep costs down, there will only be a single cloud from a single provider.

That one-size-fits-all approach hasn't worked for the CIA—which announced plans to bring in multiple providers earlier this year—and it won't work for the Department of Defense, he says. And he says the deal means all existing apps will be required to migrate to the cloud, whether that's appropriate or not. "Some things don't belong there," he says. "Some things weren't designed to take advantage of it."

In August 2018, Oracle filed a protest with the Government Accountability Office arguing that the contract was "designed around a particular cloud service." (IBM followed suit shortly afterwards.) The same month, the publication Defense One revealed that RosettiStarr, a Washington investigative firm, had been shopping a dossier to reporters alleging an effort by Sally Donnelly, a top Pentagon official and former outside consultant to Amazon, to favor the e-commerce company. RosettiStarr has refused to identify the client who paid for its work.

The drama continued. In December 2018, Oracle, which didn't make the cut for the final stage of bidding, filed new documents alleging a conflict of interest. Deap Ubhi, who worked with Lynch in the Pentagon's Defense Digital Services office, had been negotiating employment with Amazon while involved with JEDI, Oracle claimed.

Questions were also raised about a 2017 visit to the West Coast by James Mattis, then the secretary of defense, which included a visit to Silicon Valley and a drop-in at Amazon's headquarters in Seattle. On his way there, Mattis declared himself a "big admirer of what they do out there," and he was later photographed walking side by side with Bezos.

(Mattis's admiration for innovation wasn't always matched by his discernment; until 2017, he served on the board of Theranos, the blood diagnostics firm that was exposed as a fraud.)

Amazon and the Pentagon have denied claims of improper behavior, and in July they received the backing of a federal judge, who ruled that the company had not unduly influenced the contract. That, however, was before President Trump stepped in.

"From day one, we've competed for JEDI on the breadth and depth of our services and their corresponding security and operational performance," an AWS spokesperson told MIT Technology Review.

Whatever the outcome of the JEDI review, it's clear that the Pentagon's dependence on Silicon Valley is growing.

One reason may have to do with the priorities of the Department of Defense itself. Once, it led the way in computer science—many of the technologies that made cloud computing possible, including the internet itself, originated from military-sponsored research. Today, however, the money big tech firms bring to information technology dwarfs what the Pentagon spends on computing research. The Defense Advanced Research Projects Agency (DARPA), which funded the creation of the Arpanet (the precursor to the internet) starting in the 1960s, is still involved in computer science, but when it comes to cloud computing, it is not building its own version.

Jonathan Smith, a DARPA program manager, says the agency's cloud work

today is focused on developing secure, open-source prototypes that could be adopted by anyone, whether in government, academia, or commercial companies, like Amazon.

"I mean, pragmatically, when you look at technology, I think in days gone by the DOD was like Godzilla," he said. "But now we're just a big mean machine."

A FORCE AWAKENS

All this is a rapid turnaround from a little more than a decade ago, when Amazon successfully fought a government subpoena for customer records relating to some 24,000 books as part of a fraud case. "Well-founded or not, rumors of an Orwellian federal criminal investigation into the reading habits of Amazon's customers could frighten countless potential customers into canceling planned online book purchases," the judge wrote in the 2007 ruling in favor of Amazon. Those familiar with the corporate culture at the time say it was generally antagonistic toward working with the government. Unlike Larry Ellison, who has openly bragged about the CIA being the launch customer for Oracle, Bezos was part of a second wave of tech moguls who were wary of ties to the feds.

Yet the company was already making its first forays into the cloud computing services that would eventually make it an obvious government partner. In 2003 two employees, Benjamin Black and Chris Pinkham, wrote a paper describing a standardized virtual server system to provide computing power, data storage, and infrastructure on demand. If Amazon found this system useful, they suggested, so would other businesses. One day soon, those who didn't want to operate their own servers wouldn't have to: they could just rent them.

The duo presented the idea to Bezos, who told them to run with it. Launched publicly in March 2006, well before rival services like Microsoft Azure and Google Cloud, AWS now dominates the market. Cloud services provided Amazon with 13% of its overall business in 2018, and a disproportionate share of its profit. AWS boasts millions of customers, including Netflix, Airbnb, and GE.

Providing infrastructure to other companies opened the door to serving government agencies. In 2013 AWS scored a surprise victory to become the CIA's cloud computing supplier. The deal, worth $600 million, made Amazon a major national security contractor overnight.

Since then, things have accelerated. Amazon has been investing heavily in new data centers in Northern Virginia, and in February 2019, after a heavily publicized contest, the company announced it had selected Crystal City, Virginia—a suburb of Washington, DC, less than a mile from the Pentagon—as the site for its second headquarters. (New York was also chosen as a joint winner, but Amazon subsequently dropped its plans following public opposition to the tax breaks the city had given the company.)

All of this has happened without much friction, whereas other technology giants have had bumpy relationships with the national security apparatus. In 2015 Apple publicly defied the FBI when it was asked to break into a phone owned by one of the perpetrators of a mass shooting in San Bernardino, California (the FBI withdrew its request after paying hackers almost $1 million to gain access). And Google pulled out of the bidding for JEDI last year after an employee revolt over its work on a Pentagon artificial-intelligence contract, Project Maven.

Amazon has not seen the same kind of staff backlash—perhaps because it is notorious for a hardball approach to labor negotiations. And even when its workers did get restless, it wasn't because of Amazon's CIA or Pentagon links, but because it sold web services to Palantir, the data analytics company that works with Immigration and Customs Enforcement. Amazon employees wrote an open letter to Bezos protesting

"immoral U.S. policy," but it has had little, if any, effect.

And it would be a surprise if it did. It's hard to imagine that after more than five years of providing the computer backbone for the CIA as it conducts drone strikes around the world, Amazon would suddenly balk at working on immigration enforcement.

EMPIRE STRIKES BACK

So why has Amazon moved into national security? Many think it comes down to cold hard cash. Stephen E. Arnold, a specialist in intelligence and law enforcement software, has used a series of online videos to trace the evolution of Amazon from 2007, when it had "effectively zero" presence in government IT, to today, when it appears set to dominate. "Amazon wants to neutralize and then displace the traditional Department of Defense vendors and become the 21st-century IBM for the US government," he says.

Trey Hodgkins agrees. "The winner of [the JEDI] contract is going to control a substantial portion of the clouds across the federal government," says Hodgkins, until recently a senior vice president at the Information Technology Alliance for Public Sector, an association of IT contractors. The alliance disbanded in 2018 after it raised concerns about JEDI, after which Amazon, one of its members, left and formed its own association. Civilian agencies, he says, look to the Pentagon and say, "You know what? If it's good enough and substantial enough for them—scalable—then it's probably going to be okay for us."

But Arnold believes Amazon is making a wider move into the global business of law enforcement and security. The company's cloud-based facial-recognition software, Rekognition, which can detect age, gender, and certain emotions as well as identifying faces, is already being used by some police departments, and in 2018 Amazon bought Ring, which makes smart doorbells that capture video.

Ring might seem like a good consumer investment, but the company, Arnold believes, is creating technology that can mine its treasure trove of consumer, financial, and law enforcement data. "Amazon wants to become the preferred vendor for federal, state, county, and local government when police and intelligence solutions are required," he says. This summer, Vice News revealed that Ring was helping provide video to local police departments.

But that's only the start. Arnold predicts Amazon will move beyond the US law enforcement and intelligence markets and look globally. That, he predicts, is worth tens of billions of dollars.

The bottom line isn't the only concern, however: there's also influence. One former intelligence official I spoke with says the government contracts and the Washington Post purchase aren't two distinct moves for Bezos, but part of a broader push into the capital. Far from a conspiracy, he says, it's what captains of industry have always done. "There's nothing crooked in it," the former official said. "Bezos is just defending his interests."

The company's cloud-based facial-recognition software, which can detect age, gender, and certain emotions as well as identifying faces, is already being used by some police departments, and in 2018 Amazon bought Ring, which makes smart doorbells that capture video.

And perhaps the ultimate goal is not just more government contracts, but influence over regulations that could affect Amazon. Today, some of its biggest threats aren't competitors, but lawmakers and politicians arguing for antitrust moves against tech giants. (Or, perhaps, a president arguing it should pay more taxes.) And Bezos clearly understands that operating in Washington requires access to, and influence on, whoever is in the White House; in 2015 he hired Obama's former press secretary, Jay Carney, as a senior executive, and earlier this year AWS enlisted Jeff Miller, a Trump fund-raiser, to lobby on its behalf.

Amazon told MIT Technology Review that the national security focus is part of a larger move into the public sector.

"We feel strongly that the defense, intelligence, and national security communities deserve access to the best technology in the world," said a spokesperson. "And we are committed to supporting their critical missions of protecting our citizens and defending our country."

Not everyone agrees. Steve Aftergood, who runs the Project on Government Secrecy at the Federation of American Scientists, has tracked intelligence spending and privacy issues for decades. I asked him if he has any concerns about Amazon's rapid expansion into national security. "We seem to be racing toward a new configuration of government and industry without having fully thought through all of the implications. And some of those implications may not be entirely foreseeable," he wrote in an email. "But any time you establish a new concentration of power and influence, you also need to create some countervailing structure that will have the authority and the ability to perform effective oversight. Up to now, that oversight structure doesn't seem to [be] getting the attention it deserves."

If observers and critics are right, the Pentagon JEDI contract is just a stepping-stone for Amazon to eventually take over the entire government cloud, serving as the data storage hub for everything from criminal records to tax audits. If that concerns some of those on the outside looking in, it's business as usual for those inside the Beltway, where the government has always been the biggest, and most lucrative, customer.

"Bezos is smart for getting in early," says the former intelligence official. "He saw, 'There's gold in them thar hills.'"

Sharon Weinberger is the Washington bureau chief for Yahoo News and the author of The Imagineers of War: The Untold Story of DARPA, the Pentagon Agency That Changed the World.

“We’ve forgotten what an existential threat is.”

T R : Q + A

Misunderstanding tomorrow’s dangers means we’re fighting yesterday’s wars, argues one paratrooper turned academic.

By **Janine di Giovanni** / Photograph by **Stephen Voss**

Sean McFate is a former paratrooper in the US Army’s 82nd Airborne Division; he’s also worked as a private military contractor in West Africa. Today he’s a professor at the National Defense University and Georgetown’s School of Foreign Service.

His book *The New Rules of War*, published earlier this year, dissects the ways warfare must change in order for America to succeed. War reporter Janine di Giovanni sat down to ask him about his vision for the future of conflict.

Q: What are you calling for? What’s your manifesto?

A: I wrote this book because I was angry. I’ve lost good friends in Iraq and Afghanistan. As a taxpayer, we’ve flushed six trillion dollars down the toilet. And as a vet, it hurts me to see our national image tarnished. Yet we have the best military in the world—even our adversaries know that. So what’s the problem?

It’s not the military—we have a great military. The problem is that our strategic IQ is low. War is won and lost at the strategic level—not the tactical level, not the operational level. So where do you send people to train to think strategically to win? We have a dearth of that. We get lucky, not smart.

Q: What do you mean?

A: Why are we doing things like buying more Ford-class aircraft carriers, or F35s? That stuff should be slashed. I would cut away the expensive conventional weapons, and beef up the things that are very effective in modern war: political warfare, strategic influence, lawfare, economic might, and deception. Want to blunt Russian encroachment in the Baltics? Forget shows of force—military deterrence is obsolete. Instead, start a “color revolution” on their border. Moscow is paranoid and would shift resources to squashing it. Want China out of the South China Sea? Stop throwing carrier groups into the region. Instead, covertly support the Uighur insurgency. Internal regime security will steal Beijing’s attention away.

Militaries can no longer kill their way out of problems in a global information age, and this is driving war into the shadows. Today, plausible deniability is more potent than firepower: winners and losers are no longer decided on the battlefield, but by those who can discern truth from lies. The best weapons today don’t fire bullets.

Q: So let’s say you were appointed national security advisor tomorrow. What would be different?

A: The first thing is I would push to slash the Department of Defense budget in half. And then I would pump up things like the State Department, which has been left to die on the vine. But the State Department needs a cultural revolution of its own.

Then: Why is Iran a national security threat? We think of it as existential—and it is if you’re like Israel or Saudi Arabia, but not if you’re the United States. We’ve forgotten what an existential threat is.

I would implement strategies across the globe that utilize and harness the new rules of war for us. They're all doing it: Russia, China, Iran … They're all fighting these things called shadow wars, and they're very effective.

Q: What is a shadow war? How would you describe it?

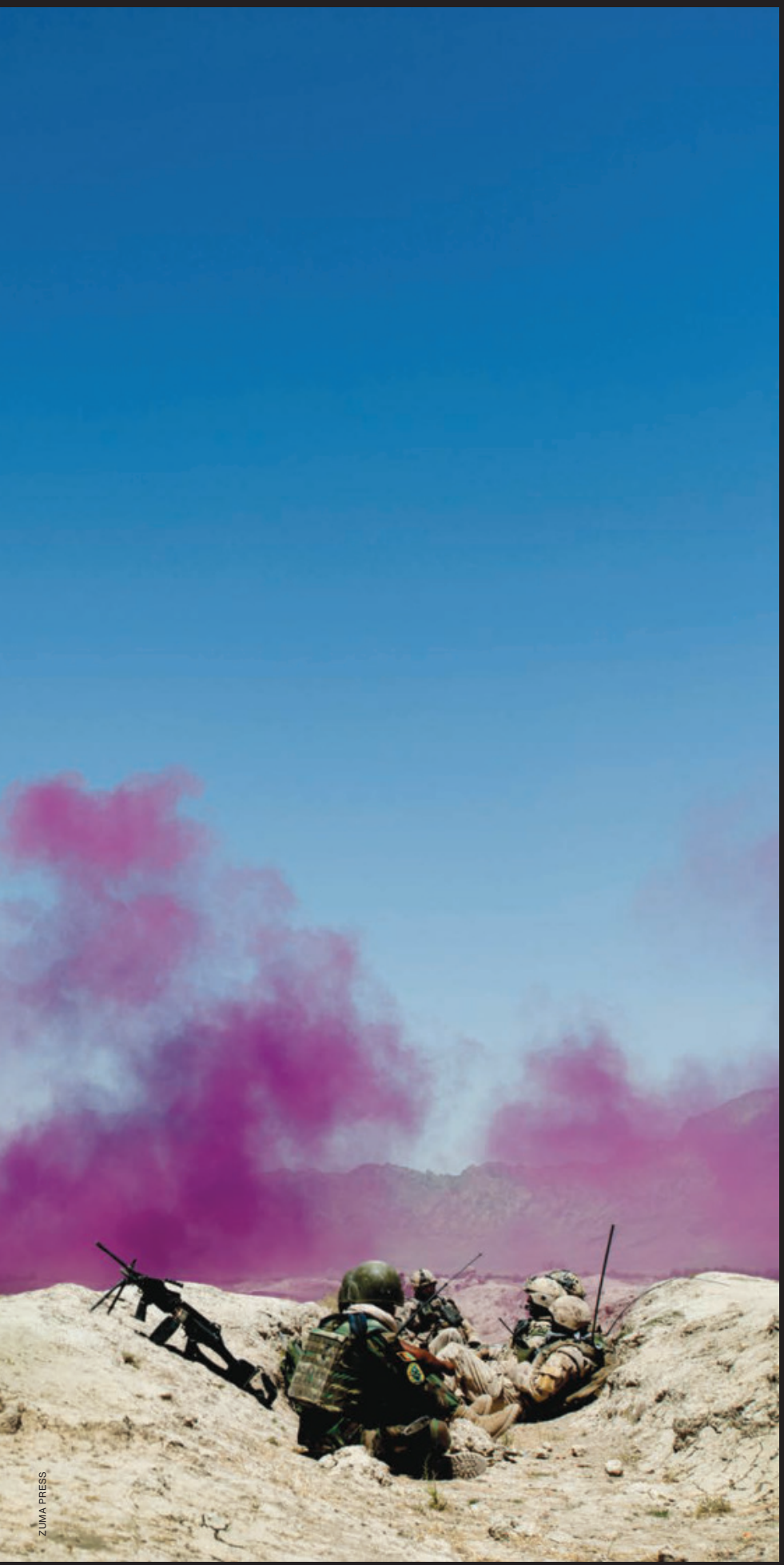
A: Shadow wars are a certain type of war where plausible deniability eclipses firepower in terms of effectiveness. Think about how Russia was in Crimea. In older war tactics, when they would put their heel on another state, they'd send in the tanks. Now, in 2019, that's not how they do it. They have military backup, but they use covert and clandestine means. They use special forces, they use mercenaries, they use proxies, they use propaganda—things that give them plausible deniability. They manufacture the fog of war and then exploit it for victory.

Q: So we should go back, in a way, to the tactics of the Cold War?

A: I don't want to go down the trap of a new Cold War … but we have done these things in the past. There is no missile that will fix the political circumstances of Syria or Taiwan. But that's how we think. That's why we struggle.

Additional research by Misia Lerska.

Battlefield



ZUMA PRESS

2

Signs of life: Even the most advanced militaries sometimes rely on old-fashioned techniques to get the job done. This purple smoke let off by Afghan and Canadian soldiers tells US drones flying overhead not to mistakenly attack them instead of their intended target.

Photograph by Louie Palu

Amount the US government paid Lockheed Martin (the largest US defense contractor) in 2018

$40.5 billion

SOURCE: GENERAL SERVICES ADMINISTRATION

$30.7 billion

Total military budget of Brazil

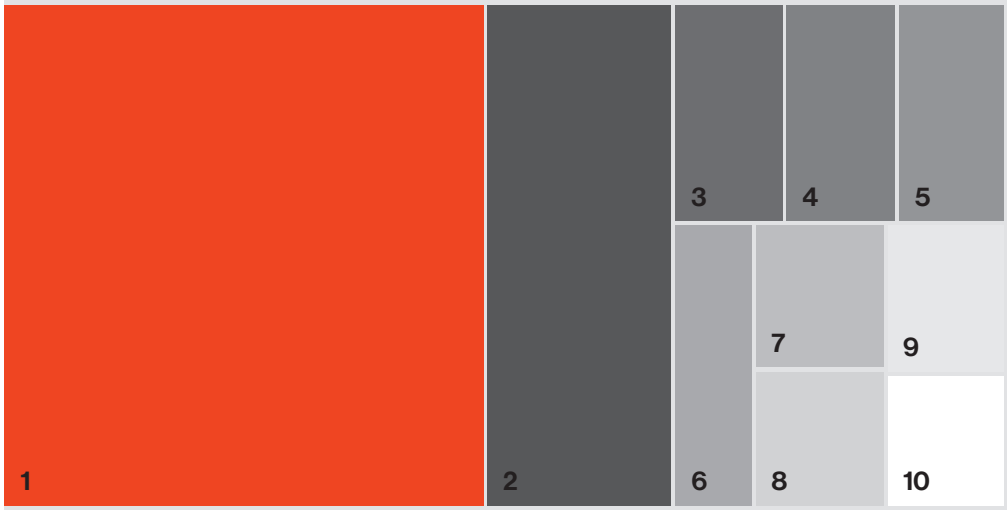
Minimum size of classified US defense and intelligence budget

$81 billion

Empire, state-building

The United States spends more money on the military than any other nation on Earth—far more. This enormous budget pays for the only global fighting force in the history of the world. But in the last 30 years, China has gone from spending about $20 billion each year on its military to spending about $250 billion each year. Does this mean that the era of American military dominance dating to the collapse of the Soviet Union is now drawing to a close? Or is American hegemony—whether for good or for ill—a reality that will persist in coming decades? It is, of course, impossible to predict the future, but examining the current state of key technologies that underpin America's ability to globally project power shows just how large its lead is.

—Konstantin Kakaes



SOURCE: SIPRI MILITARY EXPENDITURE DATABASE; *ESTIMATES

The price of power

The size of America's lead in annual military spending only hints at the vast difference that has accumulated over the decades.

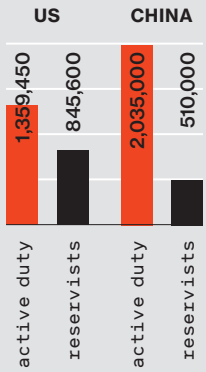
Billions of dollars, 2018:

1. US	$649	6. Russia	$61
2. China	$250*	7. UK	$50
3. Saudi Arabia	$68*	8. Germany	$49
4. India	$67	9. Japan	$47
5. France	$64	10. South Korea	$43

Comparing the US and China

If one counts the number of people in it, China's military is slightly larger than America's.

Years of enormous military budgets have bought the US the ability to surveil the globe and project power. As its long, inconclusive engagement in Afghanistan proves, this doesn't necessarily mean America will always prevail. But it has a unique expeditionary ability. Refueling aircraft and amphibious assault ships might not sound like the bleeding technological edge, but they are of crucial military importance.



SOURCE: INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. *THE MILITARY BALANCE 2019*

$61 billion — *Total military budget of Russia*

Annual amount of "bureaucratic waste" in DOD spending, according to a Pentagon audit performed by McKinsey — **$25 billion**

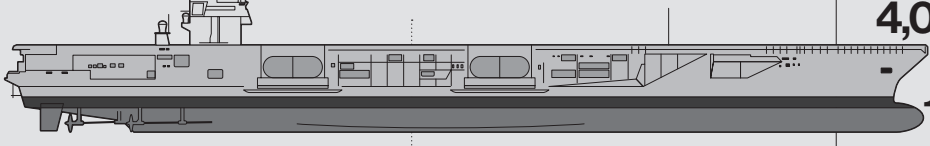
$26 billion — *Total defense budget of Italy*

Aircraft carriers and major amphibious assault ships

More than any other single technology, aircraft carriers enable the American military to project force almost anywhere in the world. Some experts worry that they are vulnerable to attack by China. But as Loren Thompson of the Lexington Institute has pointed out, aircraft carriers are hard to find and tough to sink. As Thompson writes, "The bottom line is that China is nowhere near overcoming the hurdles required for successful attacks against US aircraft carriers."

Giant supercarriers

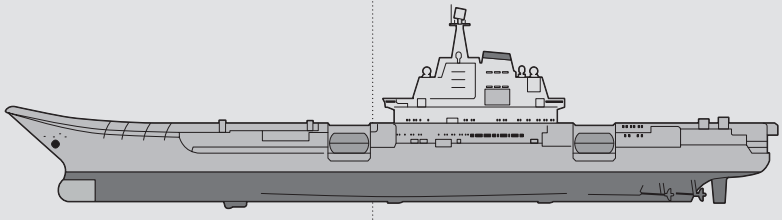
US | CHINA



11 Each can carry about 90 airplanes. The newest of these cost about $13 billion to build (and are behind schedule and over budget).

0 According to a May 2019 Pentagon report, China will bring a third, larger carrier into service in 2022. It is unclear if this carrier will be comparable in size and capability to an American supercarrier.

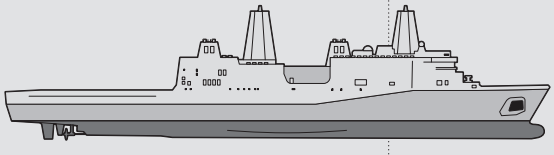
Amphibious assault ships



9 Similar to small aircraft carriers, each can carry 20 to 30 airplanes and helicopters as well as a landing force of over 1,500 Marines.

2 China operates one small aircraft carrier, which it bought from Russia. A domestically made clone is undergoing sea trials.

Amphibious transport docks



23 Each can carry a landing force of 500 to 700 troops and several large, speedy hovercraft, on which they can deploy onto 80% of the world's coastline.

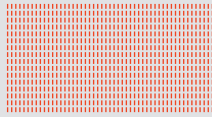
5 In contrast to the older US fleet, the first "Yuzhao" class ship was commissioned in 2007. They can each carry 600 to 800 troops, much like their American counterparts.

Satellites and select aircraft

US		CHINA
530+	In-flight refueling aircraft	18
274	Heavy transport aircraft	27
4,030	Transport & multi-role helicopters	842
177	Military & dual-purpose satellites	99

SOURCE: THE UNION OF CONCERNED SCIENTISTS, INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

Overseas bases



800+ (US)

3 (CHINA)

Depending on how one counts – many smaller American bases are secret – the US has a military presence in between 50 and 80 countries around the world, dispersed among hundreds of bases.

By contrast, China has three foreign bases, in Djibouti, Tajikistan, and Cambodia. It also has substantial numbers of troops deployed as part of UN peacekeeping missions.

SOURCE: PRESS REPORTS

Nuclear-powered submarines

US		CHINA
14	Ballistic missile	4
53	Attack/ cruise missile	6

SOURCE: INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

ILLUSTRATIONS BY JOHN MACNEILL; SOURCE: INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, *THE MILITARY BALANCE 2019*

The US military is trying to develop a brain-computer interface you could wear like a helmet. What if it succeeds?

By PAUL TULLIS Illustration by Enrico Nagel

In August, three graduate students at Carnegie Mellon University were crammed together in a small, windowless basement lab, using a jury-rigged 3D printer frame to zap a slice of mouse brain with electricity.

The brain fragment, cut from the hippocampus, looked like a piece of thinly sliced garlic. It rested on a platform near the center of the contraption. A narrow tube bathed the slice in a solution of salt, glucose, and amino acids. This kept it alive, after a fashion: neurons in the slice continued to fire, allowing the experimenters to gather data. An array of electrodes beneath the slice delivered the electric zaps, while a syringe-like metal probe measured how the neurons reacted. Bright LED lamps illuminated the dish. The setup, to use the lab members' lingo, was kind of hacky.

A monitor beside the rig displayed stimulus and response: jolts of electricity from the electrodes were followed, milliseconds later, by neurons firing. Later, the researchers would place a material with the same electrical and optical properties as a human skull between the slice and the electrodes, to see if they could stimulate the mouse hippocampus through the simulated skull as well.

They were doing this because they want to be able to detect and manipulate signals in human brains without having to cut through the skull and touch delicate brain tissue. Their goal is to eventually develop accurate and sensitive brain-computer interfaces that can be put on and taken off like a helmet or headband—no surgery required.

Human skulls are less than a centimeter thick: the exact thickness varies from person to person and place to place. They act as a blurring filter that diffuses waveforms, be they electrical currents, light, or sound. Neurons in the brain can be as small as a few thousandths of a millimeter in diameter and generate electrical impulses as weak as a twentieth of a volt.

The students' experiment was intended to collect a baseline of data with which they could compare results from a new technique that Pulkit Grover, the team's principal investigator, hopes to develop.

"Nothing like this is [now] possible, and it's really hard to do," Grover says. He co-leads one of six teams taking part in the Next-generation Nonsurgical Neurotechnology Program, or N^3, a $104 million effort launched this year by the Defense Advanced Research Projects Agency, or DARPA. While Grover's team is manipulating electrical and ultrasound signals, other teams use optical or magnetic techniques. If any of these approaches succeed, the results will be transformative.

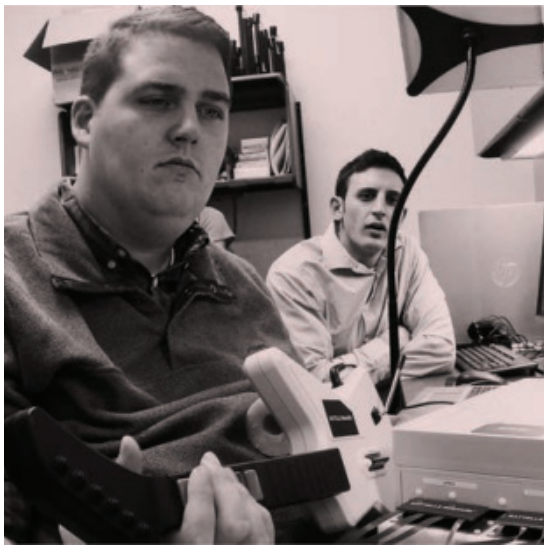
Surgery is expensive, and surgery to create a new kind of super-warrior is ethically complicated. A mind-reading device that requires no surgery would open up a world of possibilities. Brain-computer interfaces, or BCIs, have been used to help people with quadriplegia regain limited control over their bodies, and to enable veterans who lost limbs in Iraq and Afghanistan to control artificial ones. N^3 is the US military's first serious attempt to develop BCIs with a more belligerent purpose. "Working with drones and swarms of drones, operating at the speed of thought rather than through mechanical devices—those types of things are what these devices are really for," says Al Emondi, the director of N^3.

UCLA computer scientist Jacques J. Vidal first used the term "brain-computer interface" in the early 1970s; it's one of those phrases, like "artificial intelligence," whose definition evolves as the capabilities it describes develop. Electroencephalography (EEG), which records electrical activity in the brain using electrodes placed on the skull, might be regarded as the first interface between brains and computers. By the late 1990s, researchers at Case Western Reserve University had used EEG to interpret a quadriplegic person's brain waves, enabling him to move a computer cursor by way of a wire extending from the electrodes on his scalp.

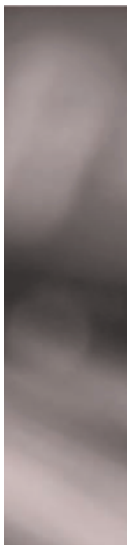
Both invasive and noninvasive techniques for reading from the brain have advanced since then. So too have devices that stimulate the brain with electrical signals to treat conditions such as epilepsy. Arguably the most powerful mechanism developed to date is called a Utah array. It looks like a little bed of spikes, about half

the size of a pinkie nail in total, that can penetrate a given part of the brain.

One day in 2010, while on vacation in North Carolina's Outer Banks, Ian Burkhart dived into the ocean and banged his head on a sandbar. He crushed his spinal cord and lost function from the sixth cervical nerve on down.



"I'm super motivated for it—more than anyone else in the room."



He could still move his arms at the shoulder and elbow, but not his hands or legs. Physical therapy didn't help much. He asked his doctors at Ohio State University's Wexner Medical Center if there was anything more they could do. It turned out that Wexner was hoping to conduct a study together with Battelle, a nonprofit research company, to see if they could use a Utah array to reanimate the limbs of a paralyzed person.

Where EEG shows the aggregate activity of countless neurons, Utah arrays can record the impulses from a small number of them, or even from a single one. In 2014, doctors implanted a Utah array in Burkhart's head. The array measured the electric field at 96 places inside his motor cortex, 30,000 times per second. Burkhart came into the lab several times a week for over a year, and Battelle researchers trained their signal processing algorithms to capture his intentions as he thought, arduously and systematically, about how he would move his hand if he could.

A thick cable, connected to a pedestal coming out of Burkhart's skull, sent the impulses measured by the Utah array to a computer. The computer decoded them and then transmitted signals to a sleeve of electrodes that nearly covered his right forearm. The sleeve activated his muscles to perform the motions he intended, such as grasping, lifting, and emptying a bottle, or removing a credit card from his wallet.

That made Burkhart one of the first people to regain control of his own muscles through such a "neural bypass." Battelle—another of the teams in the N^3 program—is now working with him to see if they can achieve the same results without a skull implant.

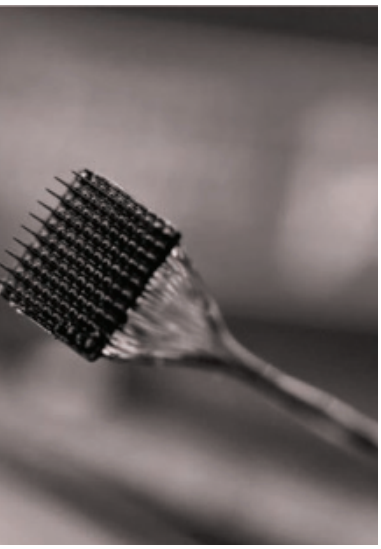
That means coming up not just with new devices, but with better signal processing techniques to make sense of the weaker, muddled signals that can be picked up from outside the skull. That's why the Carnegie Mellon N^3 team is headed by Grover—an electrical engineer by training, not a neuroscientist.

Soon after Grover arrived at Carnegie Mellon, a friend at the University of Pittsburgh Medical School invited him to sit in on clinical meetings for epilepsy patients. He began to suspect that a lot more information about the brain could be inferred from EEG than anyone was giving it credit for—and, conversely, that clever manipulation of external signals could have effects deep within the brain. A few years later, a team led by Edward Boyden at MIT's Center for Neurobiological Engineering published a remarkable paper that went far beyond Grover's general intuition.

Boyden's group had applied two electrical signals, of high but slightly different frequencies, to the outside of the skull. These didn't affect neurons close to the surface of the brain but those deeper inside it. In a phenomenon known as constructive interference, they combined to produce a lower-frequency signal that stimulated the neurons to fire.

COURTESY OF BATTELLE

Grover and his group are now working to extend Boyden's results with hundreds of electrodes placed on the surface of the skull, both to precisely target small regions in the interior of the brain and to "steer" the signal so that it can switch from one brain region to another while the electrodes stay in place. It's an idea, Grover says, that neuroscientists would be unlikely to have had.



Meanwhile, at the Johns Hopkins University Applied Physics Laboratory (APL), another N^3 team is using a completely different approach: near-infrared light.

Current understanding is that neural tissue swells and contracts when neurons fire electrical signals. Those signals are what scientists record with EEG, a Utah array, or other techniques. APL's Dave Blodgett argues that the swelling and contraction of the tissue is as good a signal of neural activity, and he wants to build an optical system that can measure those changes.

The techniques of the past couldn't capture such tiny physical movements. But Blodgett and his team have already shown that they can see the neural activity of a mouse when it flicks a whisker. Ten milliseconds after a whisker flicks, Blodgett records the corresponding neurons firing using his optical measurement technique. (There are 1,000 milliseconds in a second, and 1,000 microseconds in a millisecond.) In exposed neural tissue, his team has recorded neural activity within 10 microseconds—just as quickly as a Utah array or other electrical methods.

The next challenge is to do all that through the skull. This might sound impossible: after all, skulls are not transparent to visible light. But near-infrared light can travel through bone. Blodgett's team fires low-powered infrared lasers through the skull and then measures how the light from those lasers is scattered. He hopes this will let them infer what neural activity is taking place. The approach is less well proven than using electrical signals, but these are exactly the types of risks that DARPA programs are designed to take.

Back at Battelle, Gaurav Sharma is developing a new type of nanoparticle that can cross the blood-brain barrier. It's what DARPA calls a minimally invasive technique. The nanoparticle has a magnetically sensitive core inside a shell made of a material that generates electricity when pressure is applied. If these nanoparticles are subjected to a magnetic field, the inner core puts stress on the shell, which then generates a small current. A magnetic field is much better than light for "seeing" through the skull, Sharma says. Different magnetic coils allow the scientists to target specific parts of the brain, and the process can be reversed—electric currents can be converted to magnetic fields so the signals can be read.

It remains to be seen which, if any, of these approaches will succeed. Other N^3 teams are using various combinations of light, electric, magnetic, and ultrasound waves to get signals in and out of the brain. The science is undoubtedly exciting. But that excitement can obscure how ill-equipped the Pentagon and corporations like Facebook, which are also developing BCIs, are to address the host of ethical, legal, and social questions a noninvasive BCI gives rise to. How might swarms of drones controlled directly by a human brain change the nature of warfare? Emondi, the head of N^3, says that neural interfaces will be used however they are needed. But military necessity is a malleable criterion.

In August, I visited a lab at Battelle where Burkhart had spent the previous several hours thinking into a new sleeve, outfitted with 150 electrodes that stimulate his arm muscles. He and researchers hoped they could get the sleeve to work without having to rely on the Utah array to pick up brain signals.

If your spinal cord has been broken, thinking about moving your arm is hard work. Burkhart was tired. "There's a graded performance: how hard am I thinking about something translates into how much movement," he told me. "Whereas before [the accident] you don't think, 'Open your hand'"—the rest of us just pick up the bottle. "But I'm super motivated for it—more than anyone else in the room," he said. Burkhart made it easy to see the technology's potential.

He told me that since he started working with the Utah array, he's become stronger and more dexterous even when he isn't using it—so much so that he now lives on his own, requiring assistance only a few hours a day. "I talk more with my hands. I can hold onto my phone," he says. "If it gets worked out to something that I can use every day, I'd wear it as long as I can."

Ian Burkhart, at far left, was paralyzed by an accident and is working with researchers at Battelle to develop better brain-computer interfaces.

Burkhart had a Utah array, shown at right, implanted in his motor cortex in 2014. The Battelle group is now trying to develop a way to read his brain signals without a surgical implant.

DAMIAN GORCZAN

Paul Tullis is a writer living in Amsterdam.

Uncommon scents

DEPLOYING ANIMALS IN WAR SOUNDS LIKE A RELIC OF THE PAST. BUT EVEN THE WORLD'S MOST TECHNOLOGICALLY ADVANCED MILITARIES CONTINUE TO RELY ON THEIR KEEN SENSES—AND MACHINERY LOOKS UNLIKELY TO CATCH UP ANYTIME SOON.

BY HALEY COHEN GILLILAND
–
PHOTOGRAPH BY BOB O'CONNOR

For nearly as long as armies have fought one another, they have enlisted animals to help. Horses, especially, were decisive for millennia. As historian Morris Rossabi has written of the Mongol conquest of Asia, "Mobility and surprise characterized the military expeditions led by Genghis Khan and his commanders, and the horse was crucial for such tactics and strategy. Horses could, without exaggeration, be referred to as the intercontinental ballistic missiles of the thirteenth century." Historian David Edgerton notes that as late as the First World War, "Britain's ability to exploit world horse markets was crucial to its military power."

Horses are still of occasional importance, as in the American invasion of Afghanistan in 2001, when Special Forces troops on horseback called in bomb strikes via satellite radios, using laser designators and GPS reference points to guide the bombs. But horses are only very rarely the tool that separates defeat from victory: in all but the most exceptional circumstances, they have been replaced by tanks, trucks, satellites, and airplanes.

Researchers at the National Institute of Standards and Technology adapted a bomb detector with a design inspired by a Labrador.

Yet while horses are largely gone from modern armies, dogs are not. As of 2016, the US military counted over 1,740 military working dogs among its ranks. At Lackland Air Force Base in San Antonio, the military breeds its own sleek puppies—mainly German shepherds and Belgian Malinois—who are groomed for military service from their first whimper. Some will wash out; others will go on to four to seven months of basic obedience instruction before receiving more specialized training in how to guard bases, ambush enemy combatants, and sniff out explosive devices. From there the field narrows further. The US Army estimates that to produce 100 war-ready dogs, it must train 200.

Before entering buildings in Afghanistan, Thomas, a US army paratrooper who asked to be identified by a pseudonym, would often send his platoon's Belgian Malinois in first to ensure that no enemy soldiers or other surprises waited inside. During one day of particularly fierce fighting, Thomas was in a building, looking for somewhere to treat a wounded soldier, when he heard a noise from an adjacent room. As he rounded the corner to investigate, he remembers seeing "a shadow and a flash of light." It was a Taliban-hired Chechen fighter with an AK assault rifle aimed directly at his face.

Just as the fighter squeezed the trigger of his weapon, the platoon's dog came blazing into the room from the hallway and latched onto his neck, jerking him backwards. His shot was diverted, sparing Thomas's life.

After that, Thomas brought the dog on every mission he could. "Sometimes people would say to me—'Oh, you don't need a dog for that,'" he says. "And I'd say, 'Yeah, I need a dog. Are you on the ground? You're not on the ground. I'm bringing the dog.'"

The military also relies heavily on dogs to sniff out explosives. Dogs' sense of smell is estimated to be 10,000 to 100,000 times stronger than the average human's. Billions of dollars' worth of research on artificial detectors have yet to produce anything better. Unlike metal detectors, which are also used to locate roadside bombs and landmines, canines can be trained to pick up on non-metallic explosive devices concocted from fertilizer and other household items. This talent has proved particularly useful in Afghanistan, where many buried explosives are improvised from common chemicals packed into plastic jugs.

Scientists have long tried—and failed—to create devices capable of outperforming a dog's snout. Starting in 1997, DARPA dedicated $25 million to an initiative called "Dog's Nose," which distributed grants to scientists to develop landmine detectors. At that point, an estimated 100 million mines were buried in approximately 60 countries. But according to the DARPA program's director, Regina Dugan, the technology to find them had not advanced much since the Second World War. "The only landmine detection equipment issued to US soldiers in the field were the metal detector and a sharp, pointy stick," she wrote in 2000. (The stick was to prod the ground for anomalies.)

The resulting machines, most of which featured polymer-coated tubes that reacted when exposed to explosives, seemed promising when used in sterile laboratories. But in more realistic environments things got messier. When one of the machines was pitted against landmine-detecting dogs at Auburn University in Alabama in 2001, the highest-performing canines were approximately 10 times more sensitive. In a 22-acre grassy facility in Missouri where DARPA invited participants to test their devices, some were too responsive, reacting to plants and soil in addition to explosives.

A decade later, in 2010, the commander of the Joint Improvised Explosive Device Defeat Organization (JIEDDO) admitted that despite a whopping $19 billion of government investment in spy drones, radio jammers, and aircraft-mounted sensors meant to combat improvised explosive devices (IEDs), dogs remained unparalleled as detectors of the dangerous devices. While sensors typically found half of the IEDs before they exploded, dog teams located 80% of them.

The newest artificial detectors can detect smaller traces of chemicals than a dog can. But those detectors are big, explains Matthew Staymates, a mechanical engineer and fluid dynamicist at the National Institute of Standards and Technology (NIST): "It's got to plug into a wall, you need an enormous amount of infrastructure, gases, and vacuum pumps—and you have to bring the sample to your machine."

Nonetheless, artificial detectors have a role to play in places like airports, where all passengers must pass through security checkpoints, and dogs have provided inspiration for improving them. Staymates used a 3D printer to replicate the nose of a female Labrador retriever named Bubbles. The result is a snout-shaped extension that goes on the front of commercially available explosives detectors. It sniffs air like a dog, inhaling and exhaling several times a second instead of continuously sucking air in as such machines normally do.

"You want to be able to sample the environment in a smart way, and dogs have given us a lot of insight into what that looks like."

Dolphins can distinguish between air gun pellets and corn kernels from 50 feet.

PICTURES OF SUCCESS: Dolphins still beat sonar

A smattering of blocky white buildings perch at the cut where San Diego Bay meets the Pacific Ocean: Naval Base Point Loma. The complex houses not only hulking warships but also dozens of dolphins, sea lions, and other sea creatures.

The animals are part of the US Navy Marine Mammal Program, which was established in 1959, after scientists found that dolphins were adept at delivering messages and identifying threats underwater. During the Vietnam War, Navy dolphins named Garth, John, Slan, Tinker, and Toad were stationed in Cam Ranh Bay, a deep-water bay in the country's southeast, to discourage enemy swimmers from attacking a key ammunition pier there.

To avoid predators and locate food, dolphins have evolved extraordinary echolocation abilities. While assessing their underwater environments, they make loud broad-spectrum burst pulses that sound, to humans, like clicks. By listening to the echoes of those clicks, dolphins can detect a three-inch (eight-centimeter) ball from 584 feet—roughly speaking, that's a tennis ball two football fields away—and distinguish between air gun pellets and corn kernels from 50 feet. They can discern such fine differences even in cacophonous harbors, where man-made sonar has trouble distinguishing between returning echoes and the ambient sounds of boats, waves lapping the shore, and other noises.

These talents, which scientists struggle to fully comprehend, have helped the Navy in more recent wars, too. In 2003, the Navy flew nine of its dolphins to identify mines in Umm Qasr, an Iraqi port on the Persian Gulf—making them the first marine animals to clear mines in a war zone.

Before the dolphins entered the murky waters, the Navy dispatched unmanned sonar drones to map the seafloor. The 80-pound (36-kilogram) machines identified 200 aberrations, according to a 2003 article in Smithsonian magazine, but could not distinguish between threatening objects and innocuous organic ones.

To determine which of the 200 items were cause for concern, the Navy relied on the dolphins of Special Clearance Team One. While their handlers floated nearby in black rubber boats, the dolphins zipped through the water hunting for mines planted by Saddam Hussein's forces. When they found one, they would alert their handlers by zooming back to the boat and touching a rubber disk with their noses. Then the dolphins would return to the suspected mine and mark it with a tether or acoustic transponder for a diver to disarm later. In a week, the dolphins helped the Navy identify and disable more than 100 anti-ship mines.

Sixteen years on—to the chagrin of some animal-rights groups like PETA, which argue that dolphins do not understand the danger associated with their military work—the creatures look unlikely to be replaced by machines anytime soon.

Even when an undersea mine isn't obstructed by mud, explains Mark Xitco, the director of the Naval Marine Mammal Program, a sonar system must send out many hundreds of pings, which must then be analyzed to create an accurate picture of the object. A dolphin does the same task in a fraction of a second with a few dozen echolocation clicks. When mines have been buried, the Navy doesn't even bother with robots; only dolphins are up for the challenge. To Xitco, this is not entirely surprising. "Technology improves every year. We're making amazing strides," he reflects. "But dolphins have millions of years of evolution as a head start."

—Haley Cohen Gilliland

COURTESY PHOTO

The researchers found that this method, counterintuitively, pulls in samples of air from farther away, drawing in more of the chemicals floating around. "Nine times out of 10, you don't know where the bad guy with a pipe bomb in his backpack is," Staymates explains. "So you want to be able to sample the environment in a smart way, and dogs have given us a lot of insight into what that looks like."

Despite this progress, a dog is still much more effective than an electronic bomb-sniffer—not least because an animal, like a human but unlike a machine, can react to unpredictable situations. So some scientists have focused their efforts not on replacing working animals, but on improving their performance.

In 2017, a team at MIT's Lincoln Laboratory developed a new mass spectrometer, about the size of a large dresser, that could identify trace amounts of chemicals on a par with canine performance. Not only was it impressively sensitive, but it was fast, completing its assessments in about one second. The researchers were excited about the device's potential not to substitute for bomb-sniffing dogs, but rather to help train them.

The team had dogs locate explosives previously hidden in canisters, which were also analyzed with the spectrometer. The machine discovered that some of the perceived errors the dogs made—identifying explosives in supposedly empty vessels—weren't errors at all; the containers had been cross-contaminated. That allowed the trainers to better regulate when to praise and reward their canine students, reinforcing their detection abilities.

Though some labs wanted to adapt the machine to replace dogs, the MIT team disagreed. In a news release at the time, Roderick Kunz, who led the research, said: "Our feeling is that such a tool is better directed at improving the already best detectors in the world—canines."

Haley Cohen Gilliland is a writer in Los Angeles.

CAN YOU TELL THE DIFFERENCE BETWEEN A TURTLE AND A GUN?

The fog of

Last March, Chinese researchers announced an ingenious and potentially devastating attack against one of America's most prized technological assets—a Tesla electric car.

The team, from the security lab of the Chinese tech giant Tencent, demonstrated several ways to fool the AI algorithms on Tesla's car. By subtly altering the data fed to the car's sensors, the researchers were able to bamboozle and bewilder the artificial intelligence that runs the vehicle.

In one case, a TV screen contained a hidden pattern that tricked the windshield wipers into activating. In another, lane markings on the road were ever-so-slightly modified to confuse the autonomous driving system so that it drove over them and into the lane for oncoming traffic.

Tesla's algorithms are normally brilliant at spotting drops of rain on a windshield or following the lines on the road, but they

GETTY IMAGES

A DRONE EQUIPPED WITH AI COMPUTER VISION CAN BE FOOLED.

AI war

MILITARIES ARE DESPERATE TO MAKE USE OF AI-BASED WEAPONS AND TOOLS, BUT THESE ARE VULNERABLE TO A VERY DIFFERENT KIND OF ATTACK.
BY WILL KNIGHT

work in a way that's fundamentally different from human perception. That makes such "deep learning" algorithms, which are rapidly sweeping through different industries for applications such as facial recognition and cancer diagnosis, surprisingly easy to fool if you find their weak points.

Leading a Tesla astray might not seem like a strategic threat to the United States. But what if similar techniques were used to fool attack drones, or software that analyzes satellite images, into seeing things that aren't there—or not seeing things that are?

Artificial intelligence-gathering

Around the world, AI is already seen as the next big military advantage.

Early this year, the US announced a grand strategy for harnessing artificial intelligence in many areas of the military, including intelligence analysis, decision-making, vehicle autonomy, logistics, and weaponry. The Department of Defense's proposed $718 billion budget for 2020 allocates $927 million for AI and

GETTY IMAGES

machine learning. Existing projects include the rather mundane (testing whether AI can predict when tanks and trucks need maintenance) as well as things on the leading edge of weapons technology (swarms of drones).

The Pentagon's AI push is partly driven by fear of the way rivals might use the technology. Last year Jim Mattis, then the secretary of defense, sent a memo to President Donald Trump warning that the US is already falling behind when it comes to AI. His worry is understandable.

In July 2017, China articulated its AI strategy, declaring that "the world's major developed countries are taking the development of AI as a major strategy to enhance national competitiveness and protect national security." And a few months later, Vladimir Putin of Russia ominously declared: "Whoever becomes the leader in [the AI] sphere will become the ruler of the world."

The ambition to build the smartest, and deadliest, weapons is understandable, but as the Tesla hack shows, an enemy that knows how an AI algorithm works could render it useless or even turn it against its owners. The secret to winning the AI wars might rest not in making the most impressive weapons but in mastering the disquieting treachery of the software.

Five algorithms work together to outwit five humans in the battlefield-based video game Dota 2.

Battle bots

On a bright and sunny day last summer in Washington, DC, Michael Kanaan was sitting in the Pentagon's cafeteria, eating a sandwich and marveling over a powerful new set of machine-learning algorithms.

A few weeks earlier, Kanaan had watched a video game in which five AI algorithms worked together to very nearly outmaneuver, outgun, and outwit five humans in a contest that involved controlling forces, encampments, and resources across a complex, sprawling battlefield. The brow beneath Kanaan's cropped blond hair was furrowed as he described the action, though. It was one of the most impressive demonstrations of AI strategy he'd ever seen, an unexpected development akin to AI advances in chess, Atari, and other games.

The war game had taken place within Dota 2, a popular sci-fi video game that is incredibly challenging for computers. Teams must defend their territory while attacking their opponents' encampments in an environment that is more complex and deceptive than any board game. Players can see only a small part of the whole picture, and it can take about half an hour to determine if a strategy is a winning one.

The AI combatants were developed not by the military but by OpenAI, a company created by Silicon Valley bigwigs including Elon Musk and Sam Altman to do fundamental AI research. The company's algorithmic warriors, known as the OpenAI Five, worked out their own winning strategies through relentless practice, and by responding with moves that proved most advantageous.

It is exactly the type of software that intrigues Kanaan, one of the people tasked with using artificial intelligence to modernize the US military. To him, it shows what the military stands to gain by enlisting the help of the world's best AI researchers. But whether they are willing is increasingly in question.

Kanaan was the Air Force lead on Project Maven, a military initiative aimed at using AI to automate the identification of objects in aerial imagery. Google was a contractor on Maven, and when other Google employees found that out, in 2018, the company decided to abandon the project. It subsequently devised an AI code of conduct saying Google would not use its AI to develop "weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people."

Workers at some other big tech companies followed by demanding that their employers eschew military contracts. Many prominent AI researchers have backed an effort to initiate a global ban on developing fully autonomous weapons.

To Kanaan, however, it would be a big problem if the military couldn't work with researchers like those who developed the OpenAI Five. Even more disturbing is the prospect of an adversary gaining access to such cutting-edge technology. "The code is just out there for anyone to use," he said. He added: "war is far more complex than some video game."

The AI surge

Kanaan is generally very bullish about AI, partly because he knows firsthand how useful it stands to be for troops. Six years ago, as an Air Force intelligence officer in Afghanistan, he was responsible for deploying a new kind of intelligence-gathering tool: a hyperspectral imager. The instrument can spot objects that are normally hidden from view, like tanks draped in camouflage or emissions from an improvised bomb-making factory. Kanaan says the system helped US troops remove many thousands of pounds of explosives from the battlefield. Even so, it was often impractical for analysts to process the vast amounts of data collected by the imager. "We spent too much time looking at the data and not enough time making decisions," he says. "Sometimes it took so long that you wondered if you could've saved more lives."

COURTESY IMAGE

A solution could lie in a breakthrough in computer vision by a team led by Geoffrey Hinton at the University of Toronto. It showed that an algorithm inspired by a many-layered neural network could recognize objects in images with unprecedented skill when given enough data and computer power.

Training a neural network involves feeding in data, like the pixels in an image, and continuously altering the connections in the network, using mathematical techniques, so that the output gets closer to a particular outcome, like identifying the object in the image. Over time, these deep-learning networks learn to recognize the patterns of pixels that make up houses or people. Advances in deep learning have sparked the current AI boom; the technology underpins Tesla's autonomous systems and OpenAI's algorithms.

Kanaan immediately recognized the potential of deep learning for processing the various types of images and sensor data that are essential to military operations. He and others in the Air Force soon began lobbying their superiors to invest in the technology. Their efforts have contributed to the Pentagon's big AI push. But shortly after deep learning burst onto the scene, researchers found that the very properties that make it so powerful are also an Achilles' heel.

AI-guided missiles could be blinded by adversarial data, and perhaps even steered back toward friendly targets.

Just as it's possible to calculate how to tweak a network's parameters so that it classifies an object correctly, it is possible to calculate how minimal changes to the input image can cause the network to misclassify it. In such "adversarial examples," just a few pixels in the image are altered, leaving it looking just the same to a person but very different to an AI algorithm. The problem can arise anywhere deep learning might be used—for example, in guiding autonomous vehicles, planning missions, or detecting network intrusions.

Amid the buildup in military uses of AI, these mysterious vulnerabilities in the software have been getting far less attention.

Moving targets

One remarkable object serves to illustrate the power of adversarial machine learning. It's a model turtle.

To you or me it looks normal, but to a drone or a robot running a particular deep-learning vision algorithm, it seems to be … a rifle. In fact, at one point the unique pattern of markings on the turtle's shell could be recrafted so that an AI vision system made available through Google's cloud would mistake it for just about anything. (Google has since updated the algorithm so that it isn't fooled.)

The turtle was created not by some nation-state adversary, but by four guys at MIT. One of them is Anish Athalye, a lanky and very polite young man who works on computer security in MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL). In a video on Athalye's laptop of the turtles being tested (some of the models were stolen at a conference, he says), it is rotated through 360 degrees and flipped upside down. The algorithm detects the same thing over and over: "rifle," "rifle," "rifle."

The earliest adversarial examples were brittle and prone to failure, but Athalye and his friends believed they could design a version robust enough to work on a 3D-printed object. This involved modeling a 3D rendering of objects and developing an algorithm to create the turtle, an adversarial example that would work at different angles and distances. Put more simply, they developed an algorithm to create something that would reliably fool a machine-learning model.

The military applications are obvious. Using adversarial algorithmic camouflage, tanks or planes might hide from AI-equipped satellites and drones. AI-guided missiles could be blinded by adversarial data, and perhaps even steered back toward friendly targets. Information fed into intelligence algorithms might be poisoned to disguise a terrorist threat or set a trap for troops in the real world.

Athalye is surprised by how little concern over adversarial machine learning he has encountered. "I've talked to a bunch of people in industry, and I asked them if they are worried about adversarial examples," he says. "The answer is, almost across the board, no."

Fortunately, the Pentagon is starting to take notice. This August, the Defense Advanced Research Projects Agency (DARPA) announced several big AI research projects. Among them is GARD, a program focused on adversarial machine learning. Hava Siegelmann, a professor at the University of Massachusetts, Amherst, and the program manager for GARD, says these attacks could be devastating in military situations because people cannot identify them. "It's like we're blind," she says. "That's what makes it really very dangerous."

The challenges presented by adversarial machine learning also explain why the Pentagon is so keen to work with companies like Google and Amazon as well as academic institutions like MIT. The technology is evolving fast, and the latest advances are taking hold in labs run by Silicon Valley companies and top universities, not conventional defense contractors.

Crucially, they're also happening outside the US, particularly in China. "I do think that a different world is coming," says Kanaan, the Air Force AI expert. "And it's one we have to combat with AI."

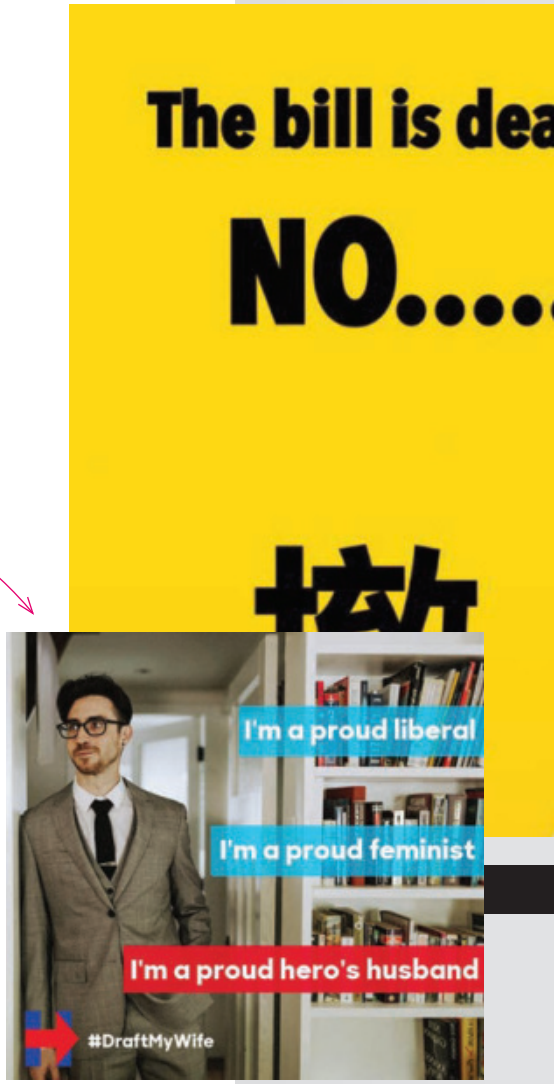
The backlash against military use of AI is understandable, but it may miss the bigger picture. Even as people worry about intelligent killer robots, perhaps a bigger near-term risk is an algorithmic fog of war—one that even the smartest machines cannot peer through.

Will Knight was until recently senior editor for AI at MIT Technology Review, and now works at Wired.

Memes come off as a joke, but some people are starting to see them as the serious threat they are.

By **Joan Donovan**

Drafted into the meme wars



In October 2016, a friend of mine learned that one of his wedding photos had made its way into a post on a right-wing message board. The picture had been doctored to look like an ad for Hillary Clinton's campaign, and appeared to endorse the idea of drafting women into the military. A mutual friend of ours found the image first and sent him a message: "Ummm, I saw this on Reddit, did you make this?"

This was the first my friend had heard of it. He hadn't agreed to the use of his image, which was apparently taken from his online wedding album. But he also felt there was nothing he could do to stop it.

So rather than poke the trolls by complaining, he ignored it and went on with his life. Most of his friends had a laugh at the fake ad, but I saw a huge problem. As a researcher of media manipulation and disinformation, I understood right away that my friend had become cannon fodder in a "meme war"—the use of slogans, images, and video on social media for political purposes, often employing disinformation and half-truths.

Joan Donovan is a researcher at the Shorenstein Center for Media, Politics, and Public Policy at the Harvard Kennedy School of Government.

While today we tend to think of memes as funny images online, Richard Dawkins coined the term back in 1976 in his book *The Selfish Gene*, where he described how culture is transmitted through generations. In his definition, memes are "units of culture" spread through the diffusion of ideas. Memes are particularly salient online because the internet crystallizes them as artifacts of communication and accelerates their distribution through subcultures.

Importantly, as memes are shared they shed the context of their creation, along with their authorship. Unmoored from the trappings of an author's reputation or intention, they become the collective property of the culture. As such, memes take on a life of their own, and no one has to answer for transgressive or hateful ideas.

And while a lot of people think of memes as harmless entertainment—funny, snarky comments on current events—we're far beyond that now. Meme wars are a consistent feature of our politics, and they're not just being used by internet trolls or some bored kids in the basement, but by governments, political candidates, and activists across the globe. Russia used memes and other social-media tricks to influence the US election in 2016, using a troll farm known as the Internet Research Agency to seed pro-Trump and anti-Clinton content across various online platforms. Both sides in territorial conflicts like those between Hong Kong and China, Gaza and Israel, and India and Pakistan are using memes and viral propaganda to sway both local and international sentiment.

In 2007, for example, as he was campaigning for president, John McCain jokingly started to sing "Bomb bomb bomb, bomb bomb Iran" to the tune of the Beach Boys' popular song "Barbara Ann." McCain, an Iran hawk, was talking up a possible war using the well-worn tactic of humor and familiarity: easy to dismiss as a joke, yet serving as a scary reminder of US military power. But it became a political liability for him. The slogan was picked up by civilian meme-makers, who spread and adapted it until it went viral.

His opponent, Barack Obama, in essence got unpaid support from people who were better at creating persuasive content than his own campaign staff.

The viral success of memes has led governments to try imitating the genre in their propaganda. These campaigns are often aimed at the young, like the US Army's social-media-focused "Warriors Wanted" program, or the British Army campaign that borrows the visual language of century-old recruiting posters to make fun of millennial stereotypes. These drew ridicule when they were launched earlier this year, but they did boost recruitment.

However, using memes this way misses the point entirely. As mentioned, great memes are authorless. They move about the culture without attribution.

Much more authentic military meme campaigns are coming from soldiers themselves, such as the memes referencing the bungling idiot known simply as "Carl." US service members and veterans run websites that host jokes and images detailing the reality of military life. Yet these serve a purpose not so different from that of official propaganda. They often feature heavily armed soldiers and serve to highlight, even in jokes, the tremendous destructive capacity of the armed forces. In turn, such memes have been turned into commercial marketing campaigns, such as one for the veteran-owned clothing company Valhalla Wear.

Recognizing this power of memes generated by ordinary people to serve a state's propaganda narrative, in 2005 a Marine Corps major named Michael Prosser wrote a master's thesis titled "Memetics—A Growth Industry in US Military Operations," in which he called for the formation of a meme warfare center that would enroll people to produce and share memes as a way of swaying public opinion.

Prosser's idea didn't come to fruition, but the US government did come to recognize memetics as a threat. Beginning in 2011, the Defense Advanced Research Projects Agency offered $42 million in grants for research into what it called "social media in strategic communications," with the hope that the government could detect "purposeful or deceptive messaging and misinformation" and create countermessaging to fight it.

Yet that research didn't prepare DARPA for Russia's 2016 disinformation campaign. Its extent was uncovered only by reporters and academics. That revealed a fatal flaw in national security: foreign agents are nearly impossible to detect when they hide within the civilian population. Unless social-media companies cooperate with the state to monitor attacks, this tactic remains in play.

My friend's wedding photo provides a good illustration of how something as seemingly trivial as a meme can be turned into a powerful political weapon. In 2016, a Reddit message board, r/The_Donald, was a well-known meme factory for all things Trump. Imagery and sloganeering were beta-tested and refined there before being deployed by swarms of accounts on social-media platforms. Famous viral slogans launched from The_Donald included those having to do with "Pizzagate" and the Seth Rich murder conspiracy.

My friend's picture was appropriated for a memetic warfare operation called #DraftMyWife or #DraftOurDaughters, which aimed to falsely associate Hillary Clinton with a revival of the draft. The strategy was simple: the perpetrators took imagery from Clinton's official digital campaign materials, as well as pictures online like my friend's, and altered them to make it look as if Clinton would draft women into the military if she became president. Someone who saw one of these fake campaign ads

My friend's picture was appropriated for a memetic operation that aimed to associate Hillary Clinton with a revival of the draft.

and then searched online would find that Clinton had in fact spoken in June 2016 in support of a bill that included a provision making women eligible to be drafted—but only in case of a national emergency. The bill was passed, but it was later changed to remove that requirement. This is what made #DraftMyWife sneaky—it was based on a kernel of truth.

Memes like this often use a process called "trading up the chain," pioneered by media entrepreneur Ryan Holiday, who describes the method in his book *Trust Me, I'm Lying*. Campaigns begin with posts in blogs or other news outlets with low standards. If all goes well, somebody notable will inadvertently spread the disinformation by tweet, which then leads to coverage in bigger and more reputable outlets. #DraftMyWife was outed fairly early on as a hoax and got debunked in the Washington Post, the Guardian, and elsewhere. The problem is, taking the trouble to correct disinformation campaigns like these can satisfy the goal of spreading the meme as far as possible—a process called amplification.

Memes online make hoaxes and psychological operations easy to pull off on an international scale. We should view them as a serious threat. The good news is that a bill in the works in the US Congress would form a national commission to assess the threat posed by foreign and domestic actors manipulating social media to cause harm.

Just focusing on those actors misses the point, though, for much the same reason those meme-inspired military recruiting campaigns missed the point. Memetic warfare works only if those waging it can rely on massive public participation to spread the memes and obscure their original authors. So rather than going after the meme creators, politicians and institutions looking to counter meme war might do better to strengthen the institutions that create and distribute reliable information—the media, academia, nonpartisan government agencies, and so on—while US cyber-defense works with the platform companies to root out influence operations.

And if that doesn't work, blame Carl.

THE US IS UNDER CYBERATTACK. WHAT HAPPENS NEXT?

{

AN ORAL HISTORY OF A DEVASTATING STRIKE THAT HASN'T HAPPENED YET.

}

This moment had been 10 months in the making. But no one noticed until last week.

A group of well-resourced hackers have been combing through the networks of the gas pipeline operator for almost a year, harvesting crucial information. Now the hackers know the network better than the pipeline company does: every piece of equipment, the company's entire workforce, usernames and passwords. They have the privileges needed to access both the firm's desktop computers and the machinery of the pipeline itself. Now they are ready to strike.

<!-BY PATRICK HOWELL O'NEILL->

THE US

has a lot of cyber-enemies. It trades blows with China, Russia, Iran, and North Korea on a daily basis. A full-blown cyberwar, thankfully, remains the stuff of theory and tabletop exercises. But what happens when one breaks out for real?

To better understand how it would play out, we talked to a number of experts in cybersecurity and national security. We asked them to consider hypothetical scenarios, including the one on the opposite page in which unknown hackers have accessed the computers, networks, and hardware of gas pipelines in New England.

The potential consequences would range from espionage and intellectual-property theft to more devastating attacks that could leave Boston without power or, in the worst case, cause fires and life-threatening damage. What happens next—and whether it escalates into a real cyberwar—depends on who is on the attack, what their goals are, and how the US responds.

The variables at play mean there's no telling exactly how this would go. But imagining the worst might help us better understand how conflict is changing, and let us plan how to act when cyberwar lands on our doorstep.

Our panel was made up of some of the US's leading experts in cyberwarfare. →

SANDRA JOYCE is vice president of global intelligence at the cybersecurity firm FireEye, the first company to openly name Chinese government hackers working against US companies.

RICHARD CLARKE has worked in the administrations of Bill Clinton, George W. Bush, and Barack Obama. He was among the first high-level White House officials to focus on cybersecurity.

MICHAEL DANIEL was cybersecurity czar under President Obama. He now leads the Cyber Threat Alliance, a team of cybersecurity companies sharing information on threats.

ERIC ROSENBACH was the chief of staff to former secretary of defense Ash Carter. He led the Defense Department's cyber activity and crafted the military's cyber strategy.

JOHN LIVINGSTON is the CEO of Verve Industrial Protection, a company that handles management of industrial cybersecurity for projects including natural-gas pipelines and other critical infrastructure.

REPRESENTATIVE MIKE GALLAGHER is a former counterintelligence officer in the US Marine Corps and now cochair of the Cyberspace Solarium Commission, a panel of experts charged with formulating a US cybersecurity doctrine.

SENATOR ANGUS KING is a member of the Senate Select Committee on Intelligence and cochair of the Cyberspace Solarium Commission.

We spoke to all of our panelists individually, and their responses have been edited for length and clarity.

Senator Angus King | Sandra Joyce | Richard Clarke | Michael Daniel | Eric Rosenbach | John Livingston | Rep. Mike Gallagher

ROSENBACH: The first thing that would happen is the NSA [National Security Agency] collecting intelligence abroad. When this first comes through there's just kind of a fuzzy gray picture that someone is operating in natural-gas infrastructure. And you don't know necessarily whether they intend to immediately pull the trigger on the attack.

KING: The first problem is attribution [i.e., who is behind the attack]. That's one of the key challenges in this field, because the adversaries are getting smarter all the time about their tracks.

I'm proposing to the Cyberspace Solarium Commission that the US government should have an attribution center that would combine resources from NSA, FBI, CIA, and other intelligence agencies so that there'd be one central place to go.

CLARKE: The attribution problem is not as bad as people think it is. With regard to cyber, if you are in the enemy systems, then you'll know who did it because you'll see them doing it. If you can see it live, you've got a very good chance to figure out attribution. If it's a post hoc analysis or forensic analysis, then attribution can be harder, especially since we know now that many nations, possibly including the US, are using attack tools created by other countries. What if they used a computer with a certain kind of keyboard, or used other techniques that fingerprint to another country? That creates a problem.

ROSENBACH: Next, you would see whether there could be a cooperative relationship between [various US government agencies] to try to figure out where the attack might occur, look for certain types of malware that adversaries may have used in the past.

You see whether you can get more granular intelligence about that. The whole time that you're working on all those kinds of domestic mitigation issues, you can try to think about what would happen in the case that the attack is successful and what you do. What is incident response during winter if there are hundreds of thousands of people, or millions of people, without heat?

You think about what you would say about that. At the same time, you're thinking about whether or not you would confront the adversary nation with this information. Do you go to them and say, "We know that you have malware in the natural-gas infrastructure and grid"? Do you actually threaten them? And then, just like in the case of the 2016 elections, and also for the first time during the [2014] cyberattack on Sony [Pictures], the president would have to talk to all the senior advisors and staff about whether he goes public with this information. Is it fair to the public, if you know that there's an attack about to occur, that you keep it to yourself? What are the pros and cons of publicly attributing?

GALLAGHER: One problem we have to deal with in cyber is whether the difficulty of attribution creates deterrence problems and deterrence failures. If you're trying to deter an adversary from conducting a cyberattack, you need to be able to establish who the adversary is and also signal clearly what your response will be. There's an open debate as to whether we should have such a declaratory policy in cyber or whether that would incentivize that behavior just below whatever threshold we determine is acceptable or unacceptable.

CLARKE: Around four years ago, the intelligence community wanted to know who these [hackers] were. Once the [Justice Department] realized that knowledge was available, they then asked the intelligence community if it could be unclassified. Somewhat remarkably, the Justice Department won that and persuaded the intelligence community to declassify. I was surprised. Some of it is part of a name-and-shame strategy. Some people say the value is low because the hackers will never be arrested, but actually a couple have been. They have to be very careful about where they travel.

ROSENBACH: After that you start to move into a phase where you're trying to collect more intelligence. You're trying to come up with options for the president or, if you're in a specific department or agency, for the secretary, in order to figure out how you could mitigate the risk and the impact of an attack like that. That's when it starts to get really complicated.

CLARKE: Cyber can speed war up. I think it provides an attacker with the ability to do significant damage to the enemy's homeland. And it provides the ability to do damage with speed. That's true in cyber along with other things that are happening in warfare, like hypersonic missiles and AI-driven weapons, that could result in a war coming to a pretty quick conclusion—or at least the first phase of a war coming to a pretty quick conclusion.

This is part of what I think a lot of people in the Pentagon are worried about. They talk a lot over there about the "decision loop" and getting inside the other guy's decision loop. They realize that cyberweapons mean there may not be a lot of time to decide how to react. That creates the possibility of greater instability. It might give you an incentive to attack first. You might have to make decisions about reacting before you really have good intelligence about what the hell is going on. Fast wars are something that we haven't really understood yet.

DANIEL: Just like how air power changed the nature of how militaries applied force and opened up options, I think cyberspace does the same thing in that it offers new channels for conflict. Some of the new physics and math of cyberspace mean that, for example, distance doesn't mean the same thing. You can cause a physical effect all the way on the other side of the planet without nearly the kind of investment you have to make to do that in a physical domain.

JOYCE: When you think about the type of conflict that is military against military, the United States has a clear advantage. We have near peers, but essentially the US outspends everybody. When countries want to challenge the US, they cannot do it in the ways the US is strong. So they'll opt for other avenues.

ROSENBACH: Nations who are adversaries to the United States have realized that the asymmetry of cyber and information operations is a huge advantage to them. The biggest and the clearest example would be North Korea. Think about how skilled they are as a cyber operational unit. Think about some of the attacks they've done in the past. Think about some of the things they're doing now in terms of using ransomware to raise money through cryptocurrencies to get around economic sanctions.

The fact that they have very little telecom and IT infrastructure, and are therefore not vulnerable, [makes cyber] an even better tool for them. That means [that] if the US or other countries were trying to figure out how to mitigate the impact of North Korean cyber operations, they would have to go to either economic sanctions, where there aren't a lot of options left, or outright military operations, where you risk too much escalation.

Then the Russians, of course, have totally perfected this by using pretty aggressive cyber and info ops and hybrid warfare. Ukraine is a great example. There they are attacking both the grid and elections. Of course, they're attacking American elections as well.

A more recent example is what US Cyber Command did against Iran's Islamic Revolutionary Guard Corps to try to have an impact on them, limit the effectiveness of that Iranian military organization, and at the same time control escalation so it might not grow into a broader conflict.

KING: I'm very worried about gas pipelines. Our gas pipeline system does not have the same kinds of controls and requirements as the electric grid, although as far as I'm concerned, the gas pipeline system is part of the electric grid because so much of our power comes from natural gas.

GALLAGHER: Around 85% of critical infrastructure [in the US] is owned by the private sector. That's a very difficult challenge. That is unique to cyber, in many cases, and requires the Department of Defense and the intelligence community to operate a little bit differently. Perhaps be a bit more forthcoming in terms of the information they're willing to share with the private sector.

LIVINGSTON: When you have historically thought about national defense, it has been a government responsibility. You build a navy, you build an army, you defend the borders. The private sector's role in that has largely been to supply that army or navy with whatever it needs. It has not been defending itself. But if we go forward 20, 30, 50 years, suddenly you have a world where the security of the nation depends on the private sector and not the government. What is the role of government in a world where my security is dependent on what my utility decides to spend money on? Or what that for-profit gas pipeline decides to spend money on? Or what that chemical plant that's 50 miles away from me decides to spend money on? That is a very difficult public policy issue, and we won't get there, I don't think, until—unfortunately—there is a major incident.

KING: It has become apparent to me that we have no doctrine, we have no strategy, and we have no policy that will in any way deter adversaries from coming after us. We're a cheap date. Why wouldn't you attack us in the cyber realm if you can do so with relative impunity? Until we develop some deterrent capability and also better resiliency, this is going to keep happening.

The good news is we're the most wired country in the world. The bad news is we're the most wired country in the world. That makes us the most vulnerable.

"We have no doctrine, we have no strategy, and we have no policy that will in any way deter adversaries from coming after us. We're a cheap date. Why wouldn't you attack us in the cyber realm if you can do so with relative impunity?"

Patrick Howell O'Neill is MIT Technology Review's senior editor for cybersecurity.

America's longest war has been shaped by technology—as the people of Afghanistan know only too well.

By Ali M. Latifi

Khalid still remembers the first time he heard about drones. He was 10 years old, sitting in his school classroom in Khogyani, a district near the Durand Line in eastern Afghanistan's Nangarhar province. A group of his friends animatedly discussed the recent death of a local man.

"Then the drone came," one of them said, imitating the whistling noise of an unmanned aircraft, "and he was dead."

Khalid didn't understand what they were saying. It was as if he was the only one left out of a secret. He finally decided to ask his teacher. What did the other boys mean? What was a *drone*?

The teacher's response was both ominous and prescient. "It's something that, once you come to its attention, you will not be left to live," he told Khalid.

That was in 2007. Khalid is 22 now, a young man. American military involvement in Afghanistan—sparked by Al Qaeda's attacks on September 11, 2001—was already six years deep by the time he learned about drones, but the strikes go back nearly as far.

The first instance of a drone killing civilians in Afghanistan was in 2002, when a man by the name of Daraz Khan was killed by a Hellfire missile dropped by a Predator drone in the eastern province of Khost. The US suspected that he was Osama bin Laden; residents maintain that Khan was merely out searching for scrap metal.

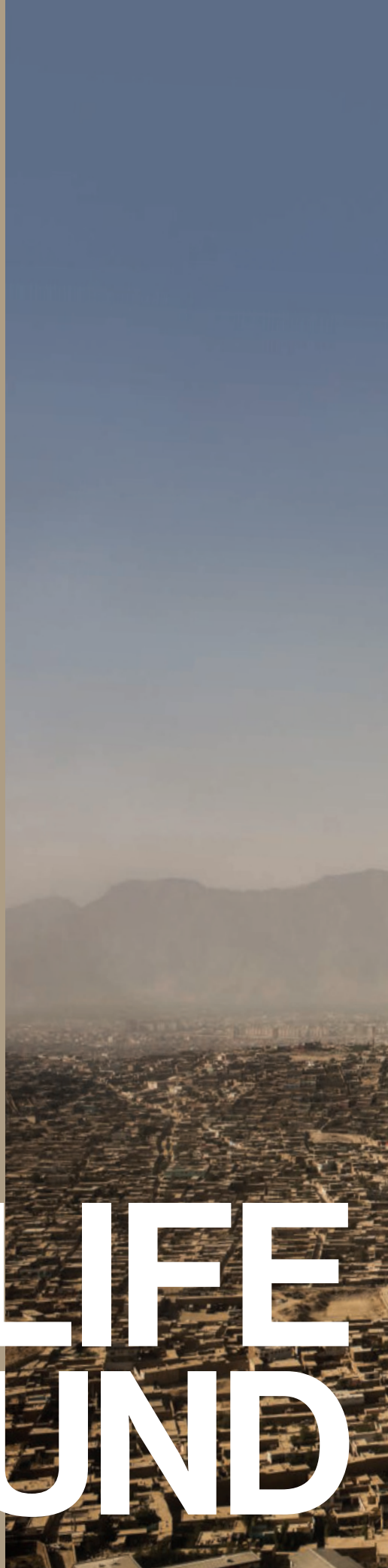
Since then, Khalid's province of Nangarhar has become a hub for armed groups—first the Taliban, and later forces claiming allegiance to ISIS—and a bustling drug trade. It has also become one of the most drone-bombed provinces in the most drone-bombed country in the world.

The American public, though, has largely forgotten this. The war in Afghanistan has been running for 18 years, making it the longest conflict in American history (it passed the previous milestone, set by the Vietnam War, in February 2019). Over the years, press coverage has fallen dramatically. According to the Pew Research Center for Journalism and the Media, Afghanistan accounted for 1% of all media coverage in the US in 2007 and just under 4% in 2010, when the Pentagon deployed 100,000 troops and dropped 5,101 bombs on the country. Today, the level of coverage is insignificant: Pew no longer even tracks it as a topic.

In fact, military activity in Afghanistan is on the increase again. The number of US troops there started rising again under the Trump administration; there are now 15,000 American military personnel officially deployed in the country. Air strikes are at a record high, according to the US Air Forces Central Command: 2018 saw 7,362 bombs dropped by US forces in Afghanistan.

As of August 31 this year, the Bureau of Investigative Journalism had documented at least 4,251 aerial strikes in Afghanistan for 2019, more than double the total for the whole of 2018. Most of these, it says, are thought to be by drones. These attacks are exacting an increasing toll on the Afghan people. This year, according to the United Nations, foreign coalition forces were responsible for more civilian deaths than the Taliban or ISIS-allied forces for the first time since its Afghanistan mission began recording civilian casualties in 2009. Between January 1 and June 30, international military forces were responsible for 89% of the 519 civilian casualties—363 deaths and 156 injuries—caused by aerial operations.

It's not just drone warfare that has expanded dramatically, however. The US military has used the war to test and improve other tactics, too.



A DRONE SKY

ER

Information warfare

In 2007, American forces began taking photographs, fingerprints, and iris scans of almost every Afghan they came across. By 2011, almost two million people—more than 5% of the population—had had their biometric details captured by the US military. In most cases it was claimed that this was done in a check for suspected militants, or as part of the application process for jobs with government security forces or on coalition bases, but it could happen at any time, and for almost any reason.

The Pentagon said the move, a tactic it calls "identity dominance," was intended to spot insurgents and prevent infiltration. But it's believed that US Navy Seals used their identity system to confirm that they had found Osama bin Laden during the raid on his compound in Pakistan in 2011. And in Iraq, where the US had previously tried biometric capture, it was used to control people's movements, especially in high-conflict areas like Fallujah.

Unsurprisingly, perhaps, the fear of surveillance is pervasive among ordinary Afghans. Rumors circulate about new techniques being used to spy on people: Khalid and his friend Naimatullah tell stories about a substance that can be rubbed on your clothes to make you more easily traceable. These tales have apparently led to a new defense mechanism among Nangarharis. "You just take off your clothes and run into some water. They say that somehow jams the signals," said Naimatullah.

Obaid Ali, a Kabul-based analyst at the Afghanistan Analysts Network, who has written extensively on aerial operations, says he has been told about physical tracking devices—albeit slightly more traditional ones. "They're really small electronic devices that are slipped into someone's clothing," he told me.

A Department of Defense spokeswoman said the Pentagon could not comment on tactics, techniques, or procedures for operational security reasons. Rahmatullah Nabil—a presidential candidate who twice served as Afghanistan's chief of intelligence during 2010 to 2015—says people are definitely tracked: but that most of that is done through mobile-phone signals. This, says Nabil, has led the Taliban to rely on some familiar tactics to keep them from being traced: "They use the simplest possible mobile phones and are constantly changing their locations every few hours. They never spend more than 48 hours in a single area."

In many areas of the country, phone service is cut off, usually by the Taliban, at sundown. And in August, the Taliban announced that they would begin targeting employees of the state-run provider Salaam Telecom, saying the company's workers are "tied to intelligence agencies."

In many areas under Taliban control, simply owning a smartphone can create suspicion that someone is an intelligence agent. That means even though people often use phones to check on loved ones after a terrorist attack or security operation, some have chosen to give up on them altogether.

But even if you throw away your mobile phone, avoid bumping into a US soldier on patrol, and can keep your biometric information to yourself, you can still get caught up in the war.

Mother load

The device that fell on a small village in Nangarhar's Achin district, an hour's drive along a treacherous road from Jalalabad, in April 2017 wasn't just any bomb. The GBU-43/B Massive Ordnance Air Blast Bomb, or MOAB, weighed 21,600 pounds (9,800 kilograms) and cost $170,000. It was the most powerful non-nuclear weapon ever used, capable of destroying an area the size of nine city blocks. It quickly became known as the "Mother of All Bombs."

The Afghan government tried to justify the strike by saying it had killed at least 94 ISIS fighters. But former president Hamid Karzai called it a prime example of how the US was using Afghanistan for what amounted to experimental warfare. "This is not the war on terror but the inhuman and most brutal misuse of our country as testing ground for new and dangerous weapons," he wrote on Twitter.

Nabil, the former intelligence chief, agrees. "Did they ever use such a weapon anywhere else in the world? No," he told me. "It's clear that Achin was just a convenient place for them to test out their weapons."

The government claims that the bomb killed foreign fighters from a number of countries. But in the days and weeks following the bombing, the village itself was still under the watch of the US military. Journalists were not allowed within 10 kilometers, and it became clear that local military and government officials had not been given access either. In the two and a half years since, journalists and investigators have still not been able to get to the exact site of the attack in order to decipher what happened.

So why was such a large bomb used? A few days after MOAB dropped, Vice President Mike Pence suggested one motive: as a demonstration of power. "Just in the past two weeks," he said in an address in Seoul, "the world witnessed the strength and resolve of our new president in actions taken in Syria and Afghanistan. North Korea would do well not to test his resolve or the strength of the armed forces of the United States in this region." He added, "The era of strategic patience is over."

Uninvestigated

All this is made worse because the US military has not always been transparent about its operations. Human Rights Watch said in a 2018 report that neither the American nor Afghan governments have been doing enough to investigate possible violations of the laws of war.

AP PHOTO/MARCO DI LAURO; PREVIOUS SPREAD: ANDREW RENNEISEN/GETTY IMAGES

At left, smoke rises from the village of Esferghich after a US air strike. Below, Afghan residents clear rubble from their homes.

NOORULLAH SHIRZADA/AFP/GETTY IMAGES

Afghans on the ground agree. I have spoken to hundreds of people since 2015, in provinces all over the country. Each time, they have said that not enough people have inquired about strikes in their areas. And even when there are independent reports, they are accused of political bias by officials in Kabul and the US-led coalition.

Emran Feroz, an Afghan-Austrian journalist and author who has been tracking aerial operations in Afghanistan since 2011, concurs: "The central problem is most of these strikes are conducted under the cover of night in hard-to-reach areas, often under the control or influence of groups like the Taliban, which makes it very difficult for anyone to go and investigate in a timely manner."

Nearly 20 years in, and with the conflict once more intensifying, there are no signs of an ending. Diplomacy between the Taliban, the Afghan government, and the Trump administration seems to be making little progress. Trump, who claimed to have canceled a secret meeting with the Taliban on US soil planned for September, has vowed to halt talks so long as Taliban fighters keep attacking Afghan civilians and US forces.

As long as military intelligence is weak, however, it is not just the Taliban that Afghans have to fear. In July, the deaths of at least seven civilians, including three women, led to protests in the Eastern province of Maidan Wardak, where residents threatened to boycott the upcoming presidential election unless action was taken. But the outcry has done little to change military action. In September, at least 30 civilians were killed in a US drone strike near a pine nut field in Khogyani. Provincial officials say the attack was meant to target a hideout of ISIS forces, but residents say it was civilians who paid the price once again.

Nabil, the former intelligence chief, says the best way to improve things is to shift away from technology and back toward proper intelligence gathering. "We have to be better than the Talibs—we must ensure that we protect civilian life at all costs," he says. During his tenure at the National Directorate of Security, he says, aerial operations were allowed to take place only when he had verified information on suspected targets. "You can't go from the word or suspicions of just one or two people. You must do your due diligence, otherwise you end up in a situation like today where civilians are constantly being killed by our own forces," he told me.

Khalid and Naimatullah agree that the increasing frequency of strikes serves no purpose. "Even people in the villages know where the Taliban and Daesh [ISIS] are, but why is it that civilians keep dying in these attacks?" they asked.

"I was 16 when I saw someone die from a drone strike," said Naimatullah. "Since then I've cleaned up so many bodies, their blood, their brains. My heart is stone now, because it's always innocent people dying."

Ali M. Latifi is a journalist based in Kabul.

Documenting drones with data

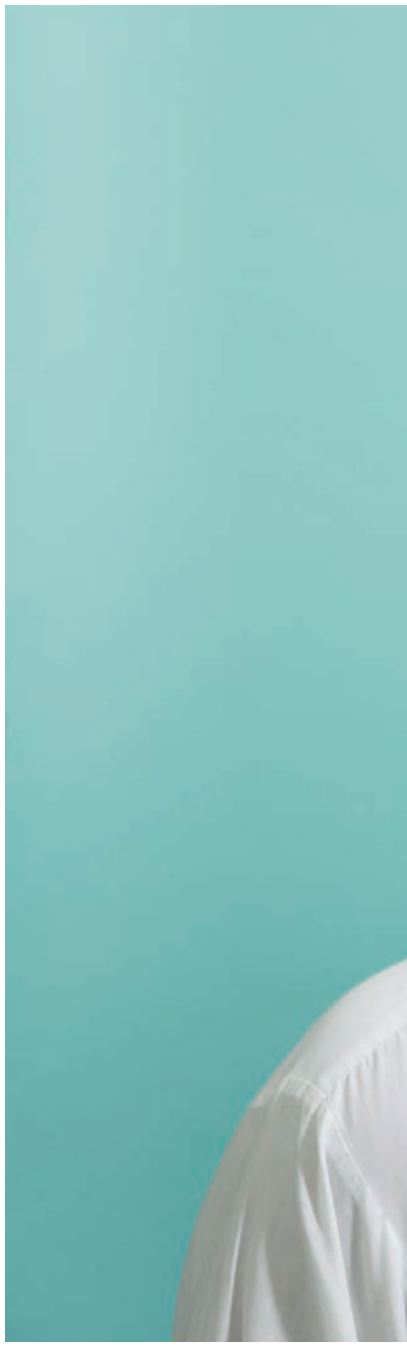
Nearly a decade ago, we started recording US air and drone strikes in Yemen, Somalia, and Pakistan, and we added Afghanistan to the list in 2015. We did this in response to the official silence that surrounded these operations. And while American counterterrorism operations have become somewhat less secretive over time, the level of transparency is constantly in flux. In September 2016, after more than a year of pressure, we started to get official military figures on how many strikes were taking place in Afghanistan each month. A year later, however, that same information was suddenly deemed too sensitive for public release.

When it was reinstated another year later, we were happy to see important details included—such as where and what the strikes hit. This showed a high number of strikes on buildings, described by one expert as the riskiest kind of strikes for civilians. But two weeks after we published a story raising these concerns, that level of detail was stripped out of the data.

Transparency, or the lack of it, can have a very real impact for civilians on the ground. In Wardak, one Afghan province, a strike killed one man's entire immediate family, including his seven children. The US military denied responsibility on three separate occasions, even telling us that they carried out no strikes in that area. Only after we found weapon fragments from the site conclusively proving US responsibility did they admit dropping the bomb (although they still deny civilian casualties). Had those fragments not been found, the US role in this incident might never have been uncovered.

Jessica Purkiss is a reporter at the Bureau of Investigative Journalism covering drone strikes.

“The West is divided. This is the worst of all worlds.”



TR: Q+A

Split strategies over nuclear proliferation could spell disaster, says one of the world’s most decorated soldiers.

By **Janine di Giovanni** / Photograph by **David Vintiner**

General David Richards is one of Britain’s most influential soldiers: he served as head of the British Armed Forces and NATO commander in Afghanistan. But he is perhaps most renowned for his humanitarian intervention in Sierra Leone in May 2000, when he unilaterally took decisions on the ground to protect the capital, Freetown, saving the country from sliding into genocide.

He spoke with war reporter Janine di Giovanni, who has covered conflicts including those in Bosnia, Iraq, Afghanistan, and Syria.

Q: In Sierra Leone you evacuated hundreds of people and blocked rebels from entering Freetown. This operation was extraordinary. Did you ever think that it could fail?

A: I knew that it was possible to fail because of the number of tactical challenges. And of course I had to persuade London to back me. But I had been to Sierra Leone three times before, and I had a good grasp of the issues and the nature of the enemy, the Revolutionary United Front (RUF). With a bit of luck, I would pull it off. Napoleon said “Give me lucky generals.” That said, without good people in key positions, I never could have managed. If I really thought I was going to fail, I wouldn’t have tried it. It was a risk, but not a gamble.

Q: But you didn’t have any orders to do this, did you?

A: I was conscious that the genocide in Rwanda had happened not long before—military commanders had been too cautious and followed bad orders. In Sierra Leone, I was determined that I would avoid such an outcome. If I played my cards right, at a minimum I could prevent the RUF from getting into the city. But yes, you’re right, I had no orders to do this.

Q: And what lessons did you learn from leading NATO in Afghanistan?

A: The primary difference was that Sierra Leone involved the British collaborating with others but calling all the shots. In Afghanistan, everyone took orders primarily from their own capital. If they felt like it and it suited their national priorities, they would also take orders from me. People did their best, but one or two nations were very difficult. Subordinate commanders, usually put up to it for political reasons

by their national bosses, would second-guess me. They could undermine perfectly sound military logic. In Sierra Leone, everyone was indisputably on the same side and wanted the same outcome.

Q: What do you think about the current arguments over nuclear proliferation?

A: At a conference a few years ago, I heard a serving US officer discuss nuclear weapons as if they might be used as an integral part of modern war. I and a few other Cold War diplomats and politicians were horrified. They are the most dreadful weapon: if we use them, we have failed. They must be seen as a deterrent—something whose possession makes war less likely, not more.

For that reason, we need to persuade Iran not to develop nuclear weapons. President Trump is now using a very harsh sanctions regime to achieve this, but I worry that he is underestimating and misreading the Iranians. Like the Russians, they will sustain a great deal of pain to achieve their goals. It would have been better to stick to the nuclear deal and play the long game. The trouble is the West is divided. This is the worst of all worlds. We need to be united around the nuclear deal or the president's alternative. The Iranians are sophisticated, and they will exploit that wedge.

Q: Do you think war will become more technological over time? What about the role of AI?

A: It's inevitable. These things will change the character of war, but not the nature. After the tank was invented, for many years it was very successful and dominated warfare; today its utility is more limited. And as we go through this tech revolution, this doesn't necessarily mean that conventional armed forces and weapon systems will become redundant. You can probably never have enough technology to deal with a million people and 50,000 tanks. The new systems have to be capable of defeating old forms of industrial warfare.

Q: Is war inherent in man? Can we ever escape it?

A: My instinct is that war is sadly inevitable. We should always assume that there are people out there who are prepared to achieve their goals through war. Even if we don't want to go to war, others may in order to achieve their aims. The best defense against this is to be strong enough to deter it. But when no alternative exists, we must be prepared to root out evil in its infancy and before it becomes endemic.

Additional research by Misia Lerska.

Aftermath

3

ZUMA PRESS

Under cover: Even when the fighting is over, peace needs to be maintained—and sometimes it requires taking unusual steps. In Afghanistan, female police officers are trained by foreign military personnel, but the drills must take place in secret to protect the officers' identities from insurgents.

Photograph by Louie Palu


1
2014 04 24
3
Heading
355°
Orientation
N
32/46/5°
1.06
0.0
Last Fix
19:09:12
36°44.557'E
84%
Brightness (Sun)
167
32
Error (m)
2
4
5

DIGITAL TECHNOLOGIES
ALLOWED SYRIAN WAR CRIMES
TO BE DOCUMENTED IN
UNPRECEDENTED DETAIL.
WHAT GOOD HAS IT DONE?

Hard evidence

BY ERIC REIDY

ILLUSTRATIONS BY
EMILY HAASCH

On April 23, 2014, Houssam Alnahhas slid into the back seat of a car in the southern Turkish city of Gaziantep and headed for the Syrian border, about 30 miles (48 kilometers) away. A tall 26-year-old medical student with striking gray eyes, he had escaped Syria two years before and was working for a task force training medical personnel in opposition-held areas. But now he was heading back with a mission: to collect evidence of war crimes.

Two weeks earlier, Alnahhas had started receiving reports that barrel bombs were being dropped on towns in the country's rural northwest. He was used to such news in his work, but this time was different. Usually the crude devices were packed with explosives and shrapnel. But doctors were telling him these latest bombs were releasing poisonous clouds of chlorine gas.

Chlorine gas had rarely been used as a weapon since World War I, and its use in Syria would be a major violation of international norms. Western governments wanted to know if there was proof. And so, over the next two days, he and two of his friends visited two villages that had allegedly been hit—Kafr Zita and Talmenes—to see what had taken place.

The trip was dangerous. They were close to the front lines of the civil war, where rocket, mortar, and sniper fire were common. If agents of the Syrian regime got word of what they were doing, their lives would be in peril: Alnahhas had heard rumors that someone who'd collected evidence from a chemical attack a year earlier had been assassinated while attempting to bring it to Turkey.

But the threat of violence wasn't the only thing weighing on his mind. Alnahhas knew that many groups—supporters of Syrian president Bashar al-Assad, the Russian and Iranian governments, online conspiracy theorists—would use any opportunity to insist that chemical-weapons attacks were false-flag operations or outright hoaxes. And since he was acting on his own, without institutional backing, he wanted to make sure the evidence he collected was unimpeachable.

As soon as he crossed the border, Alnahhas started tracking his coordinates using GPS and recording the trip on video. In the two villages, residents described witnessing yellowish-orange smoke rising after helicopters dropped barrel bombs. Doctors explained how they treated victims—women, men, young and elderly people—who were terrified, coughing violently and struggling to breathe. They handed over blood, urine, saliva, and hair samples they had collected.

At the spots where the bombs had fallen, Alnahhas recorded 360-degree video of the surroundings, focusing on identifiable landmarks so the locations could be independently verified. He collected soil samples in small plastic containers, triple-sealing them in clear plastic bags and labeling them in front of the camera.

In Kafr Zita, he gathered pieces of shrapnel and measured heavy, rusted barrels bent, mangled, and peeled apart by the impact and detonation. There were three long canisters, two still lodged inside the barrels, covered in chipped yellow paint, the color often used to mark industrial chlorine gas. The chemical symbol Cl_2 was still clearly visible on the ruptured nose of one.

In Talmenes, in the dimming evening light, Alnahhas filmed an impact crater in the backyard of a house. There were dead birds scattered across the ground, and the leaves on the plants and trees were dead, even though it was springtime. The smell of chlorine still hung in the air, causing him to cough and his eyes to water.

"To be honest," Alnahhas says, "this was the scariest time of my life."

Syria was one of the first major conflicts of the social-media era. Local access to Facebook had been restricted since 2007 as the government tried to limit online political activism. But by February 2011, when the Assad regime unblocked many social-media sites—either as a nod toward reform or as a way to track its opponents—they had become major forces across the globe, and many Syrians had cell phones with cameras and access to high-speed internet.

There were dead birds scattered across the ground, and the leaves on the plants and trees were dead, even though it was springtime. The smell of chlorine still hung in the air, causing him to cough and his eyes to water.

Soon afterwards, protests broke out in the south of the country and quickly spread. The government cracked down brutally, and activists, lawyers, medical workers, and ordinary citizens started using Facebook and YouTube—often at great personal risk—to record the violence and show it to the world.

Initial efforts were haphazard, and mostly involved people uploading shaky cell-phone video and using accounts with fake names to protect themselves. But before long the push to document what was happening became more organized and sophisticated. Media offices and local news agencies mushroomed. By early 2012, international organizations had begun training local activists on professional production standards and online security and helping them to record their videos. The idea wasn't just to release clips to the media, but to gather evidence that could be used to pursue justice in the future.

Volunteers took videos and photos at the scenes of attacks and potential war crimes, compiled detailed medical reports, recorded victim and witness statements, and smuggled reams of documents out of captured government buildings. Civil society groups such as the Syrian Archive and the Syria Justice and Accountability Centre collected millions of pieces of potential evidence—some of it made public, some filed away in protected archives.

The material collected by Syrians allowed people far away from the actual fighting to take part in the investigative efforts too. In 2012 Eliot Higgins, then an unemployed British blogger, began sifting through videos and photos posted from Syria, trying to identify the weapons being used; later he started a website, Bellingcat, and assembled a team of volunteer analysts.

Pioneering the technique of "open-source investigation," Higgins and his team pieced together evidence suggesting that Syrian government forces were using chemical weapons and cluster bombs, that Russian forces had attacked hospitals in

PREVIOUS SPREAD: ILLUSTRATION SOURCE IMAGERY COURTESY OF THE AUTHOR

Obama declared the use of chemical weapons in Syria to be a "red line," but after government forces used them, he backed off from action and settled for a deal brokered by Russia.

the country, and that ISIS was using small, commercially available drones to drop 40mm grenades onto targets.

Back then, many people working at the intersection of technology and human rights shared a belief in the power of social media and digital connectivity to do good, according to Jay D. Aronson, head of the Center for Human Rights Science at Carnegie Mellon University. People thought that "if we're able to document these war crimes and these human rights violations and we're able to share them with the world, then that will create political will that will lead countries to intervene and protect vulnerable populations," he says.

Spurred on by such optimism and the encouragement of Western politicians, such efforts made the Syrian conflict the most thoroughly documented in human history.

Thanks to frontline investigators like Houssam Alnahhas, local outfits like the Syrian Archive, and online analysts from Bellingcat, detailed information about what was happening on the ground was there. Someone just needed to act on it.

When Alnahhas returned to Turkey with the evidence he'd collected in Kafr Zita and Talmenes, he met up with a British chemical weapons expert who tested some of the samples. The analysis confirmed that they contained a high enough concentration of chlorine to kill people. The evidence clearly showed that the Syrian government, the only fighting force with helicopters at the time, had indiscriminately bombed civilians with chlorine gas—a war crime.

International media picked up on the story; human rights organizations published reports; the Organisation for the Prohibition of Chemical Weapons launched a fact-finding mission. The remaining samples were given to the Western governments who were interested, and then Alnahhas waited.

Nothing.

Last summer I met Ahmad al-Mohammad, a soft-spoken activist and communications director of the Syrian Institute for Justice, in Istanbul. He had been a 19-year-old agriculture student at Aleppo University when the uprising began in 2011.

The Syrian protesters were optimistic back then. The US had just led an international military intervention to protect civilians in Libya from the advancing army of former leader Muammar Qaddafi. "We listened to a lot of speeches from the president of America, Obama," said al-Mohammad. "We had hope, honestly, that the West would intervene and remove Bashar al-Assad."

And in 2012, Obama declared the use of chemical weapons in Syria a "red line." "The world is watching," he warned Assad. "If you make the tragic mistake of using [chemical] weapons, there will be consequences, and you will be held accountable."

Obama's resolve was put to the test on the morning of August 21, 2013. Syrian government forces launched rockets loaded

with sarin gas, a deadly nerve agent, at the rebel-held enclave of Ghouta, on the outskirts of Damascus. It was by far the deadliest and most visible chemical attack of the war. Syrian activists quickly uploaded photos and videos of the casualties, many of them women and children, their faces blue from suffocation. The estimated death toll ranged from around 350 to more than 1,400.

The US—driven forward by the "red line" rhetoric—prepared to launch military strikes. The regime hunkered down. But at the last minute, Obama pulled back. Instead of using force, he opted for a deal brokered by Russia, which resulted in the Syrian government's signing on to the Chemical Weapons Convention and agreeing to declare its stockpiles and destroy them by mid-2014.

For people in opposition-held areas, the decision was crushing. "We lost hope that anyone would [stand] up and say enough … killing civilians inside Syria," Mohammed Abdullah, a Syrian photographer who goes by Artino and who was in Eastern Ghouta at the time of the attack, told me.

And then, despite its promise to dismantle its chemical weapons program, the Syrian government launched chlorine gas strikes in April 2014—the ones Alnahhas documented. They were another clear violation of Obama's red line. When the outside world again failed to take strong action, Assad's government continued to push the envelope. According to a report by the Global Public Policy Institute (GPPi), a think tank in Berlin, this was when the Syrian government began integrating the use of chemical weapons, especially chlorine gas, into its "arsenal of indiscriminate violence."

Assad's strategy was directed against civilians living in opposition-held residential areas far from the front lines. Life-sustaining social institutions—bakeries, hospitals, and markets—were often targeted with a brutality that forced people to choose between surrender, exile, and death. Tobias Schneider, one of the GPPi report's authors, refers to it as the "military utility of crimes against humanity." The use of chemical weapons was "the last couple of meters," he told me.

Heavier than air, poison gas sinks into basements and bunkers, suffocating and terrifying people sheltering from conventional bombs and weapons. Even if the chemical attacks often didn't kill large numbers of people, they showed that "there is absolutely nowhere you can hide and there's absolutely nothing [the regime] can do that will make the international community stop [the violence]," Schneider added.

The Syrian government has used chemical weapons more than 330 times so far, according to data collected by GPPi. The vast majority of these incidents—more than 300 of them—took place after the attacks in Ghouta, Kafr Zita, and Talmenes.

For Alnahhas, the lesson was clear.

"After providing evidence all the time, at a certain point you stop to believe that it will be effective," he said. "The main thing that I know is that neither I nor the people inside Syria trusted the international community anymore."

Activists in Syria have documented the presence of chemical weapons' shell casings with photos like this one, in the hope that they'll provide evidence of war crimes.

Many people who had been documenting the war were forced to leave Syria as it grew more violent. Some decided to focus on putting their lives back together, to finish their studies or start families. For many of those who remained in Syria, the work of documentation became too dangerous as the areas they were in fell under regime control.

But other activists have decided to take a longer-term view. Although the documentation efforts have failed to shift the course of the war, Syria has produced arguably the largest evidence base on war crimes ever recorded. Civil society organizations are sifting through the data, organizing it, and using it to build case files for prosecutions. Courts in Germany, France, and Sweden are already trying cases. Arrest warrants have been issued for several high-ranking members of the Assad regime, and charges have been brought against European companies for violating sanctions imposed on the Syrian government. The Open Society Justice Initiative (OSJI), a human rights litigation team, is working with the Syrian Archive to develop case files on a number of attacks, including the attack in Talmenes that Alnahhas documented.

"Open-source information has radically transformed how we investigate, collect, and analyze information," Steve Kostas, a lawyer with OSJI, told me by email. "We use it to establish a factual narrative of the attacks, to identify possible witnesses, [and] to identify and learn about suspected perpetrators." Still, says Beth Van Schaack, a visiting professor at Stanford Law School who previously worked on Syria at the US State Department, the prosecutions so far have been "mostly against lower-level individuals, opposition figures, [ISIS] members, and not the kinds of war crimes that have really come to characterize this war."

Holding the true architects of the Syrian government's war strategy responsible would require unity from other governments. But Russia has repeatedly blocked efforts to start an international process of justice and accountability; for example, it vetoed a 2014 UN Security Council resolution referring Syria to the International Criminal Court. The UN created a body called the International Impartial and Independent Mechanism to gather evidence for future cases, but "until this moment, we don't have any court or entity that has jurisdiction over crimes committed in Syria," says Deyaa Alrwishdi, a Syrian lawyer who has been involved in accountability efforts since 2011.

It now seems all but inevitable that the Assad regime—helped by Russia and Iran—will emerge victorious from the war. It may be decades, if ever, before it's truly held accountable.

"We get hope when we look at the former Yugoslavia and how victims and survivors from Bosnia and Herzegovina did eventually get justice. That gives us hope to keep holding on," al-Mohammad, from the Syrian Institute for Justice, told me in Istanbul.

He has scars on his face from having his jaw fractured in seven places when security forces threw him from the second story of a building during a protest in 2012. Two members of the documentation team he manages in Syria were killed while carrying out their work. And he has watched countless hours of video showing one brutal atrocity after another, giving him nightmares. His family is still in Syria, and he worries that they will be punished by the regime as retribution for his actions.

Al-Mohammad has scars on his face from having his jaw fractured in seven places when security forces threw him from the second story of a building during a protest in 2012.

It's hard for him to see a path forward or a way to return home. "Me and my friends, we sit down and we talk about it a lot … we don't really know where we are going," he says. "At the end of the day, people like us—our future in a Syria without justice is just death or prison."

Yet al-Mohammad and others have continued to record evidence of the crimes taking place. At some point, he says, it stopped being about what the international community would or wouldn't do; it became about Syrian people taking control of their own stories. "My goal became to document my country's history," he says.

When I met Alnahhas in Gaziantep earlier this summer, he told me he felt the same way. We talked at an outdoor café, surrounded by the mundane bustle of a busy town. Syria, just a few miles down the road, seemed far away. In the years since his dangerous trip to document the chemical weapons attacks, he had gone to a Turkish university to finish his medical degree, married, and started a family. He couldn't imagine returning home.

He told me about three of his friends, young students who had volunteered to provide care to injured protesters in the early days of the uprising. They were stopped at a regime checkpoint, and medical supplies were found in their car. Days later, their bodies were returned to their families, burned beyond recognition. Years later, his efforts to document the chemical attacks in Kafr Zita and Talmenes hadn't changed anything; people were still being murdered with impunity.

"At the same time," he said, "you cannot simply say that I'll not continue." If nothing else, documenting has given him and others like him a certain mission. "History is written by the strongest," he said, echoing the familiar adage. "Without proper evidence … the regime will be able to, at a certain point, say 'No, this never happened'; [it] will be able to manipulate the history of the Syrian crisis maybe to avoid punishment. So this is our responsibility."

Eric Reidy is a journalist based in the Middle East.

ILLUSTRATION SOURCE IMAGERY COURTESY OF THE AUTHOR

By
ANDREW ZALESKI

Photographs by
JARED SOARES

Becoming whole

Modern medicine has saved war veterans with horrific genital injuries from dying. Now it's finally giving them hope of a normal life as well.

Ray almost missed it, the message that would change his life. On a Saturday in March 2018, just as he was about to take his dog for an afternoon walk, he pulled his phone from his pocket and discovered a string of voicemails. Eight years had passed since the bomb had blown up underneath him while he was on patrol in Afghanistan, five since he'd first met his doctor. He'd been on the waiting list a year. He was getting impatient.

He dialed back. This is it, he thought. It has to be.

A nurse picked up. Ray needed to come to the hospital immediately, she said. They had a donor. He was getting a new penis.

Ray had carried his unseen injury for years—always furtive, always anxious, always wondering how anyone who found out might react. Having lost both legs in the blast didn't bother him that much; Ray often left the house in the summertime wearing shorts, his prosthetics shining in the sun. But his other injury? Aside from his parents, hardly anyone knew—not even the guys he went to war with.

For men like Ray who lose their genitals, the usual treatment—if there was any—was phalloplasty: a rolled tube of tissue, blood vessels, and nerves taken from the forearm or thigh and transplanted to the groin, an ersatz penis that needs an external pump to get erect. When he first met with plastic surgeon Richard Redett, an expert in genital reconstruction at Johns Hopkins Hospital in Baltimore, phalloplasty was what he was offered. But soon after, Redett decided Ray could be a candidate for one of the world's first full penis transplants. Not a crude substitute; the real thing.

"This was actually something that could fix me," says Ray. "I could go back to being normal again."

PENIS TRANSPLANTATION IS a radical frontier of modern medicine: extremely rare, expensive, and difficult to perform. Replacing a major organ like a damaged liver is one thing: it contains just one type of tissue. But grafting a penis from a deceased donor onto a living recipient is a chaotic amalgamation that entails stitching millimeters-wide blood vessels and nerves with minuscule sutures.

In 2013, when Ray first went to Johns Hopkins, there was no precedent for such a transplant. Since then, only four patients have had one.

South African urologist Andre Van der Merwe completed the first-ever successful transplant in 2014, sewing a donor penis onto a 21-year-old whose own had turned gangrenous after a grisly circumcision. In 2016, doctors at Massachusetts General Hospital transplanted a donor organ onto 64-year-old Thomas Manning, who had lost his penis to cancer. A year later, Van der Merwe and his team at Tygerberg Academic Hospital in Cape Town repeated their procedure on a 41-year-old victim of another circumcision gone wrong. Ray became patient number four.

After getting off the phone with the nurse that Saturday afternoon, he went into action. With military precision, Ray called his parents, packed the items he would need, boarded his dog, and made his way to the hospital. He checked in, as requested, at 1:30 on Sunday morning. At 2 a.m. Monday, he lay anesthetized on an operating table. And 14 hours after that, Redett and his team had completed the procedure. It was the most extensive penis transplant ever performed, and the first for a military veteran anywhere in the world.

RAY HAD BEEN a US Navy corpsman trudging through Afghanistan when Taliban fighters ambushed his squad in 2010. As he rushed to give first aid to a downed soldier, he stepped on a roadside bomb.

"I remember everything froze and I was upside down," he says. "I remember thinking a quick thought: 'This isn't good.' And then I was on my back."

The butcher's bill was steep: both of his legs up to and including the thigh were blasted off, along with his penis, his scrotum, and an upside-down-U-shaped chunk of his abdominal wall. Only a handful of people know the full extent of his injuries.

Two years later, while he was learning to walk on prosthetic legs, his urologist at Walter Reed National Military Medical Center referred him to the reconstructive surgery group at Johns Hopkins.

At the time, Hopkins was a leader in vascularized composite allotransplantation, more commonly called VCA surgery. It's used in face, hand, arm—and penis—transplants, taking multiple types of tissue from a donor and hooking up blood vessels and nerves so they work for the recipient. In December 2012, Hopkins surgeons completed their first bilateral arm transplant, on an infantryman who had lost both his arms and legs to a roadside bomb. If anyone could help Ray, it was these surgeons.

At their first meeting, Redett talked about phalloplasty, which didn't excite Ray much. He resolved to go through with it, thinking it was the only choice. Yet Redett soon changed course, deciding that Ray was a better candidate for a transplant.

Johns Hopkins surgeon Richard Redett first suggested phalloplasty before realizing Ray made a good transplant candidate.

In fact, it was probably the only surgical fix given the extent of the damage. Van der Merwe calls Ray's procedure "the most complex to date," largely because of the scope of his injury. To repair it, Hopkins doctors didn't just transplant the penis itself. They also transplanted the donor's scrotum and extensive amounts of tissue from the thigh and lower abdomen.

"When I heard they wanted to do it, I felt this huge sigh of relief," says Ray.

"For him, it was almost either you do this transplant, or you live the rest of your life with your defect," Redett says.

RAY, WHO IS now in his mid-30s, is a thin man of average height, with touches of gray in his beard and a wobbly gait, a result of the prosthetics he now calls his legs. He hasn't discussed his surgery since April 2018, when he gave a short interview to the New York Times. But this March, one year after his surgery, he agreed to talk to me so long as MIT Technology Review protected his identity. (His name has been changed in this article.) He did so, he says, because he wants other veterans to know about their options.

And many others are affected. A total of 1,367 American infantrymen sustained significant genital injuries in Iraq and Afghanistan between 2001 and 2013. Such hidden wounds of war represent a relatively new problem. Bombs from below used to be a death sentence, but better body armor and modern casualty care ensure that more wounded soldiers survive—and more of them with devastating genital-urinary trauma. In a report last year, military urologists wrote that groin injuries have increased "to a level never before reported in the history of war."

The US Department of Defense recognized the problem as long ago as 2008, when it set up an institute to research various reconstructive transplants. Eventually, the TOUGH Project—Trauma Outcomes and Urogenital Health—placed a figure on it: among infantrymen with genital-urinary injuries from Iraq and Afghanistan, 502 were injured so severely that a penis transplant might be their only recourse.

Quantifying the number of such injuries is easy. Outlining the psychological toll they take on guys in their 20s and 30s is much harder.

Even those closest to the trauma, like Timothy Tausch, have to use anecdotes to explain. He's an Army lieutenant colonel and director of trauma and male reconstructive urology at Walter Reed. "As soon as they wake up, they're not asking about where their legs are," he says. "They're asking where the testicles and the penis are. You can't put a number on how significantly this affects one of these wounded warriors' lives."

Yet some experts wonder if the procedure is really necessary. Kidney and heart transplants save lives, but someone who lost a penis isn't going to die without a new one. Getting one may even be inviting a different set of psychological issues. (It bears mentioning that a poorly documented transplant attempt happened in 2006 in China, but the 44-year-old recipient apparently demanded reversal after his wife panicked, shocked at the idea he had someone else's penis.) In the months following Ray's surgery, Hiten Patel, a chief resident at the Johns Hopkins Brady Urological Institute, wrote that a penis transplant "lacks both life-saving and life-enhancing properties when compared to a readily available alternative in phalloplasty."

Others argue that for young men devastated by their wounds a transplant is, in fact, both life-saving and life-enhancing. Suicide risk among US veterans is already high: one study found that those deployed between 2001 and 2007 were 41% more likely to take their lives than civilians. Ray himself entertained thoughts of suicide after his injury. The idea gradually faded once he realized he could have gone to war and died; instead he was alive, on the first step of a long climb back.

"Even though we do a pretty good job with phalloplasty reconstruction, it's still a quantum leap to put on a real penis," says Curtis Cetrulo, one of the surgeons who operated on Thomas Manning in 2016. Phalloplasty recipients, for example, may regain some erotic sensation, but they must use a pump to achieve an erection or have intercourse.

Ray wouldn't say the transplant saved his life, exactly, but it has improved it.

"This surgery was a way for me to overcome that little subconscious voice or whatever it was that would always keep me feeling different from everyone else," he says. "It was one of those injuries that really stresses you out and you think, 'Why would I keep going?' I guess I always just kept this real hope that there's an answer out there."

SEVERAL HOURS BEFORE the hospital contacted Ray, Richard Redett had received a phone call of his own. He had gotten it enough times before to know the words by heart: *We may have a donor.*

Usually such calls were dead ends: the potential transplant almost never met Redett's strict criteria. For Ray's surgery to stand a chance, the donor had to be a young, healthy guy; the organ had to be a good color match and average in size; and, crucially, it had to be no more than two hours away, so that once it had been removed from the donor's brain-dead but still living body, it could be brought to Johns Hopkins before it started decaying.

"If you do an arm transplant, we know exactly how long that will hold up on ice. But nobody really knows that for a penis," he says.

This particular call on that Saturday in March was more promising. There was a brain-dead patient nearby who was donating his organs, including his penis. Over a rapid string of conversations, Redett evaluated the patient's medical history and determined when his team could get there. By the afternoon, Redett knew he had his donor.

Still, no doctor had ever worked with a graft as large as the one Ray required. To transplant a penis, you need the two dorsal arteries and the two dorsal veins from the donor. Fortunately, Ray's two penis nerves were intact. But to transplant the abdominal wall and scrotum, even more veins are necessary. Fail to take those, and the new scrotum and abdominal tissue will die, along with much of the skin of the penis.

Over five years, Redett and his team had deciphered the topography of penis transplantation with cadavers and food coloring. It was basically a grand perfusion experiment: inject dye into the blood vessels of a dead man, and watch for blush on the skin to know which vessels are required as part of the transplant. "We were injecting

every blood vessel we could find down in the region with blue and red food color," he says. "We just needed to know which vessels, and we needed to get very quick, very efficient, and very safe. We knew this had the potential to be a very long operation."

On the Sunday afternoon, his team boarded a chartered jet to meet their donor (the donor's identity and the state he's from can't be disclosed). At 6 p.m., they entered the procurement room. Other doctors and medical staff, 25 in all, were there grabbing solid organs: lungs, heart, kidneys, liver. It's a bloody choreography, finding your place in an organ procurement. Redett and his team sliced into and isolated the lower abdominal wall, thigh tissue, scrotum, and penis, dissected out the requisite arteries and veins, and let the other doctors take what organs they needed before finishing.

Once they had removed and packed Ray's graft, nothing else mattered except speed. Bodily tissue begins to break down the instant it's deprived of blood. If enough toxins are released, the tissue can swell so much it asphyxiates. It's why you throw transplants on ice, as Redett's crew did for their Learjet flight back to Baltimore—it delays the breakdown process.

It's also why surgeons train, practice, and visualize their maneuvers. Redett's team had already run dry rehearsals of their procedure. In the operating room, they had set up the table where Ray would lie, figured out where the ice machine went, placed the optical microscope Redett would use, and even tested every power outlet to make sure they wouldn't short a circuit.

As the team ate snacks from their go-bags on the plane back to Hopkins, other surgeons wheeled Ray into the operating theater. By this time it was 11 p.m. on Sunday, almost 24 hours after he had arrived at the hospital. They prepared him by removing all the diseased tissue and exposing the blood vessels, nerves, urethra, and penile stump. At 2 a.m. Monday, Redett and his fellow surgeons took their places—some standing above Ray, the rest tending to the graft at another table—and steeled themselves. The gravity of his mission consumed Redett's thoughts.

"I remember

everything froze

and I was upside down."

"We felt very confident we could do it, but we had never done it," he says. "If you're not anxious for something like that, you're not thinking hard enough."

In the Johns Hopkins operating room, a surgical microscope with a craned neck like a brachiosaurus magnified the view by up to 20 times, enabling Redett to see the very tip of the needle-point instruments that hold the sutures for stitching together vessels barely two millimeters thick.

"The threads are smaller than a human hair," he says. "Unless you're under a 'scope, you can't really even see it."

They began by sewing Ray's urethra onto the donor's. Then came the arteries and veins that bring blood to the skin of the abdominal wall, scrotum, and penis shaft. Next they sutured Ray's penile nerves, which were buried deep underneath his pelvic bone, to the nerves of the donor penis. Finally, Redett's team stitched together the skin.

"You know how to do it, but until that last blood vessel is hooked up and you release the clamps and blood flows through it—I mean, that's a huge sigh of relief," says Redett.

A kidney transplant usually takes three hours. The first penis transplant surgery in 2014 took nine. Redett's team needed an additional five hours to complete Ray's transplant. In a surgery that long, doctors are allowed to take bathroom breaks, and even slug some coffee. Redett did neither.

RAY'S FIRST MEMORY after he came out of the anesthesia was the heat. His room was warm to help keep his transplant at body temperature. It wasn't until two days later that Ray looked down and saw his new penis for the first time.

"It was swollen and still had a lot of healing to do," he says. "In the back of your mind, you know this is a transplant, and you wonder if it's going to be too much for you to handle. Once I went through with the surgery, all of those concerns just went away."

The surgery wasn't just technically complex; it also required weighing various ethical questions. For example: if they were giving Ray a scrotum, should they give him

testicles too? The answer was no: transferring sperm-generating tissue might have made it possible for Ray to have the donor's genetic kids. (In the end, the donor had not given consent to use his sperm.)

Another matter was the prospect of lifelong immunosuppression. In penis transplant surgeries, it's critical: Van der Merwe had to cut off half of the penis he transplanted in 2014 because the patient stopped taking his medication and rejection set in.

The team came up with a novel answer to this problem. In a procedure spearheaded by Gerald Brandacher, scientific director of the reconstructive transplantation program at the Johns Hopkins School of Medicine, bone marrow and stem cells from the donor's vertebral bones were isolated in the lab. Two weeks after his transplant, Ray was injected with a large amount of the donor's bone marrow cells.

In organ transplants of any type, recipients are typically given a cocktail of immunosuppressant drugs every day. Ray, on the other hand, requires just one pill.

"It's kind of like reeducating the immune system," says Brandacher. "It allows us to minimize the need for immunosuppression but not completely stop it."

Minimizing the drugs needed after a transplant, in fact, may be what really got the US military interested in surgery like Ray's. Immunosuppressants ensure that the body doesn't attack a new organ, but they also weaken the immune system and can lead to toxic complications like kidney failure. For a heart or lung, the trade-off is obvious: immune problems versus death. For a penis, the question is more muddled.

"If we can get to a point where we have therapy that doesn't require that level of toxicity, the calculus changes completely," says Lloyd Rose, a former program manager for rehabilitative medicine research in the US Army. "Then a transplant can become a surgery for anybody who's missing a hand or a foot or a face or a penis—or anything."

If vets with transplants have to take fewer pills, it means fewer complications as they get older, and an easier life. It also saves the government money in the long term. The issue is so important to the military that the $12 million Congress appropriates each year for the Armed Forces Institute of Regenerative Medicine is now spent primarily on immunosuppressive research—not on paying for things like penis transplants.

ON A HOT afternoon last April, a year after his surgery, I met Ray for the first time. He balanced his modest frame on his part-metal, part-polymer prosthetic legs, and in his left hand he carried a cane. Even with the support, he picked his way gingerly along the sidewalks until we made our way over to a public bench near a coffee shop.

"When I got hurt, one thing I did realize is that the world is not designed for a guy like me, being blown up," he told me matter-of-factly. "I knew then I would have to change myself to fit the world."

While he doesn't hide his prosthetics—when we met, he wore gym shorts—his unseen injury still causes him some consternation. It's not that he hasn't accepted his new penis. On the contrary, Ray doesn't seem to think about it as a donor organ at all. It's just that so few people know what happened to him, and he's not quite ready, and may never be ready, to identify himself.

"It may not necessarily be that people are going to say bad things about it," he says. "But it's just one of those things. It's a private thing."

Still, those around him recognized a change. A close friend of Ray's, one of the few who know, says she noticed "a little boost" following the procedure. "It was such a profound wound, there was a no-light-at-the-end-of-the-tunnel kind of feeling," she says. "Now he's much more confident … It's this feeling of being whole again."

In some ways, Ray is still figuring out how his transplanted organ will shape the contours of his life. He's not dating at the moment, and knowing that he can't be a biological father, he wonders if that will deter women who may want to start a family.

In other ways, the surgery has made a huge difference to his daily emotional state. He's more outgoing, less afraid to meet new people, and more fit, mentally and physically, piecing back together a life interrupted. Important questions—such as whether he's able to pee standing up (he can), whether he gets erections (he does)—already have answers.

"He told me, which was the best news I could hear, that it feels normal," says Redett.

It took six months before the nerves of his transplanted penis started firing. Stitching nerves together isn't like splicing a wire; a nerve cell's axons, the long threads along which impulses are sent from one cell to another, have to grow all the way out to the organ they're supplying. Now, more than a year removed from surgery, those nerve signals have grown only stronger. "I'm still getting sensation back. It's pretty close," Ray says. "This is not going to be a quick fix, but I've seen improvement over time."

"The world is not designed for a guy like me," says Ray.

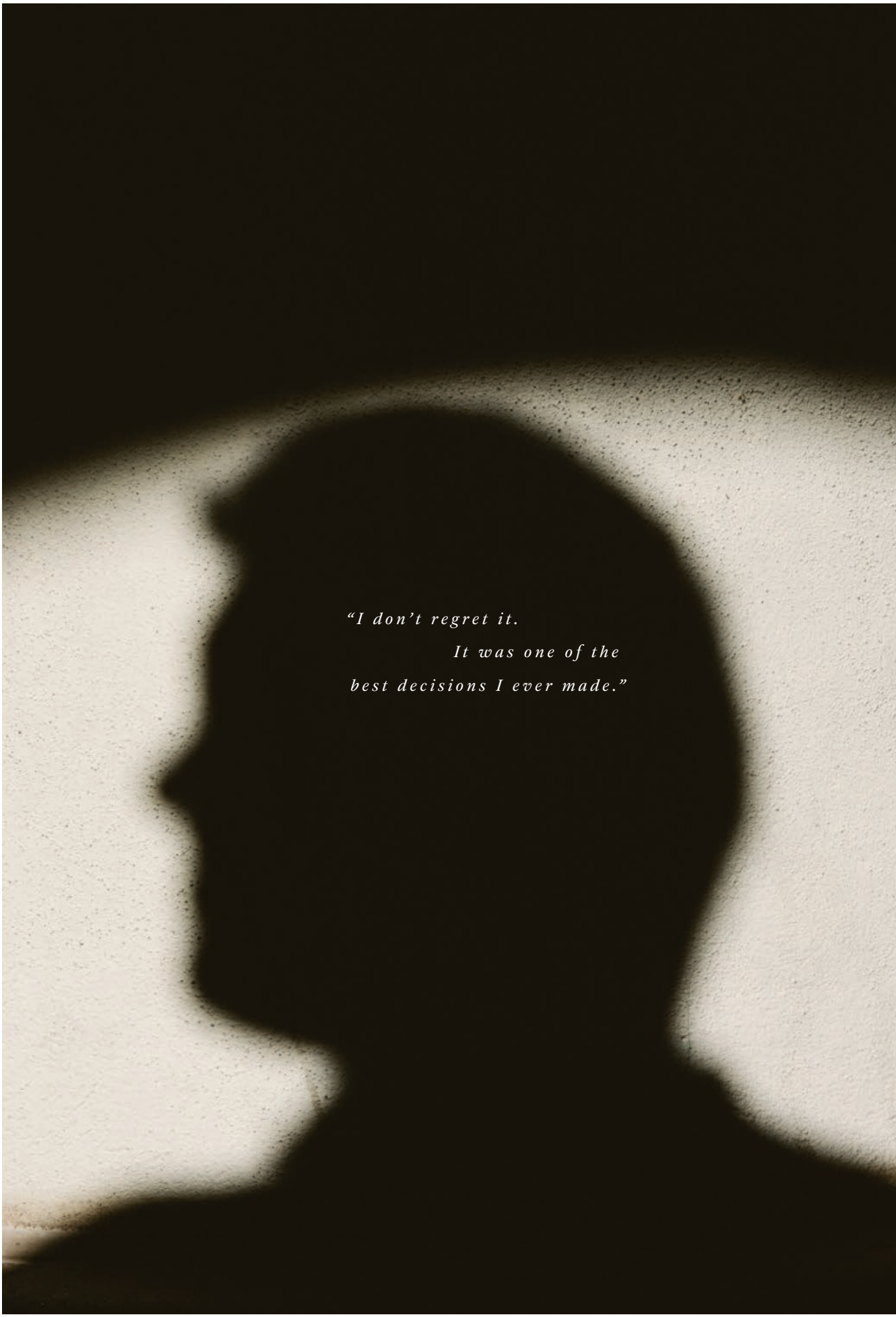
Where penis transplant surgery for wounded veterans goes is still up in the air. South Africa's Van der Merwe, the originator of the transplant, says the VCA procedure itself is now proven; its future depends on other matters. There's the problem of who pays, and of finding appropriate donors. And then there's the immunosuppression issue that the military is trying to solve.

"The risks of immunosuppression in many people's minds also outweigh the benefit of doing an arm, or a face, or a genital transplant," Redett says. "We disagree, but that will slow down progress."

Ray barely blinked when I asked him some of these questions at our second meeting, in July. Dealing with immunosuppression, he says, is easy: he takes a pill and washes his hands frequently. Guys who need it and can handle it, he says, should get a transplant. He feels no ambivalence about that phone call, when doctors told him they were ready to sew on the donor penis for which he had waited five years.

"I don't regret it," Ray says. "It was one of the best decisions I ever made."

Andrew Zaleski, a writer based near Washington, DC, covers science, technology, and business.


“I don’t regret it.
It was one of the
best decisions I ever made.”

Fiction

AN41

You never actually heard the rounds that hit closest to you. You definitely felt the change in pressure every time a bullet slapped into the far side of the wall, though. Jack looked back at his squad. They were nervous and holding tight to their cover, but craning their necks around looking for an opportunity to return fire.

Something caught his eye to the right. AN41 was moving their way. She scooted over, dropped to a knee, and popped her visor up. She did not need the augmented-reality display—she was "chipped," like all other Legionnaires—but she had joked that the visor screened the sun out better than sunglasses. Dust clung to the exterior of her armor. Her exo had been "tuned up," as the soldiers say: she'd taken rounds on her way across the open ground. The impact points were visible on the shoulder and chest, but she didn't look fazed. A heavy machine gun started thumping away, and the unmistakable sound of quadcopters could be heard from above. She grinned at Jack and the squad, looked up toward the top of the hill, and said, "Here's the plan."

~

That morning Jack had been sitting with the squad during breakfast when his platoon sergeant called to him from across the room.

"Need you to take 3rd Squad and kit up. Meet by the flagpole in twenty—you are picking up security and reaction force duties for a Legionnaire element going up north."

Legionnaires on the patrol added a layer of stress for everybody. Higher took a major interest in any operation where general-purpose infantry like 3rd Squad were mingled in with members of the Legion.

Twenty minutes later, the squad was by the flagpole in full kit. It had been "on call" for Legionnaire missions twice before, but never gone forward with them on patrol. This would be different.

BY JASPER JEFFERS
ILLUSTRATIONS BY YOSHI SODEOKA

The US knew humans were always the weakest and slowest point of decision-making.

It would also be their first trip up north toward the Donovian border.

Jack looked up as a young Army major, in multi-cam with sleeves rolled up at the cuffs and a bright smile on her face, walked over to them. This was a thing with Legionnaires; they were such disgustingly nice people.

"Sergeant Adams, I'm AN41." Another thing about these guys; Legionnaires only introduced themselves by call sign. This did not help eliminate the image that they were mostly robots.

"But most of my crew calls me Annie." She smiled and extended her hand. Jack shook it.

"We'll keep it at Forty-One, ma'am." He wanted to display the highest professionalism.

"Thanks Sergeant A, appreciate your helping us on this one—we're not expecting any drama, but once we get up into Otso, never hurts to have the extra help."

Jack knew these super-soldiers didn't need his squad as extra help, but he appreciated the gesture. Many years ago, Jack's brother had been a Legionnaire. Jack himself had gone through the assessment, but it hadn't worked out. Fewer than 200 Legionnaires existed in the force; the rate of selection was ridiculously low.

But it meant Jack had a pretty good idea of the capabilities and type of people that ended up with the chip. He was looking at three of them right now. Just behind AN41 were the other two Legionnaires on the team; there were always three. And just behind them, he could see the folded legs of three quadrupeds on a trailer being pulled by their support vehicle. He could guess what was inside the housing bumps on the back of each q-ped, and doubted these Legionnaires needed anyone to be watching their back.

"No sweat, ma'am ... We are ready to roll."

"Sounds good. Split up between the lead and trail truck, and if you can ride up front with me, we can get caught up before we get outside the bubble. We'll real-time distro the guidance to your team's internal channel and visors."

The squad split up, and Jack walked to the lead vehicle. It was built for speed more than for protection—a mashup of a five-ton truck and a dune buggy, with a minimum of armor. AN41 was adjusting her exo and helmet when she looked up without a smile.

"Jack, I apologize ... The MIND just passed me your background. I wanted to let you know your brother was an amazing individual and leader. He put me through the course. It is truly an honor to meet you—he was a hero."

~

It had started with driverless cars. The first ones were a novelty, but it was the ability to network them, and the resulting decrease in accidents, that led to the opening. Who doesn't want their kids to be safer? And if you have a million autonomous and semi-autonomous vehicles, wouldn't you want a powerful AI to help coordinate them? Simple but large-scale AI systems, mandated by governments as a public safety measure, became a natural overlay of the social and political environment.

But the well-intentioned regulations of Western governments also created an impetus to "democratize" AI development, to reduce the risk of any one political power using it as a weapon. And democratization made it free and available for actors who would use the technology for their own agendas.

That created the perfect conditions for what folks now call the Continental Wars between Donovia and Otso. With powerful and free AI crunching numbers, probabilities, and potential strategies instantaneously, a billion regressions on a particular course of action could lead you to some pretty confident and horrible decisions. It was only a matter of time until a weakened state was told by its AI that outcomes could only be changed by acting with violence.

The war came to a stalemate: a long DMZ along the "new" border of Donovia. In the meantime, both sides patrolled, competed, and wrestled in a buffer zone. It was not quite full-on war, but it certainly included plenty of small-unit skirmishes.

During the conflict's decisive action phase, the United States learned the hard way about the strengths and weaknesses of AI-networked systems. The US built the world's most powerful AI entity, referred to as the MIND. The MIND had to represent the best of the values of the American Republic. The US knew humans were always the weakest and slowest point of decision-making, but they could not just turn over power to machines. So it created the Legion.

The concept was simple. The best way to ensure the MIND did not become a tool for efforts fundamentally incompatible with human values was to embed and meld the MIND with humans themselves. Soldiers made the ideal first

candidates for incorporation of the MIND. The American people generally had more confidence in the military than in other political institutions, and you needed a group of young, willing humans to actually execute the concept.

A specially selected set of individuals would take on this responsibility and ensure that the power of the MIND was kept out of the hands of the wrong people. It would be a military organization made up of the best leaders, with exceptional character. The candidates could come from anywhere—college, the State Department, nonprofits, or within the armed services—and were chosen in a selection process that forced hard decisions under stress. The system was designed to allow an individual's moral and essential values to bubble to the top. Legionnaires had networked devices implanted into them, and the two forces—man and machine—balanced out as one. Near-omniscience from access to the MIND, and an ethical code that prevented purely mathematical decision-making: this was the Legion.

The chipping process required months of surgery. Small scars around all of the Legionnaires' ears indicated augmentation for their hearing; Jack had heard they now had an enhanced sense of smell too. But the technological game-changer was the integration directly with the human brain.

Of course, you had to hope the selection process picked individuals with the right core values. The chance of selecting the wrong person was always present. So a failsafe was built in: only three living Legionnaires, acting in concert, could access the resources of the MIND. This tactical check-and-balance theoretically reduced the risk of any single Legionnaire becoming compromised by the power or becoming an unwitting servant of the MIND.

~

The vehicles bounced down the road, but active suspension eliminated the jouncing. Everyone still instinctively leaned left and right when the vehicle mounted difficult terrain, even though the crew compartment barely moved at all.

AN41 turned to look at Jack. She didn't need to drive—or at least she wasn't looking at the road. Jack didn't understand how, but he knew the MIND guided the vehicle and would alert AN41 to certain parameters or environmental changes that required her to return her eyes to the road.

In fact, Jack wasn't even sure how much she needed her human eyes. The vehicle was packed with sensors of all varieties: visual, electromagnetic, short-range radar. All were constantly analyzed and integrated through the MIND, which alerted human attention to anything above a certain suspicion threshold.

New York-based artist Yoshi Sodeoka's work is characterized by its neo-psychedelic view of the world.

"Sergeant Adams, let's lay out the plan here," AN41 said. "We are headed north, just inside the contested area of Otso." She pulled over a map board and highlighted a location in the valley.

"We know there is an ongoing effort to disrupt the current ceasefire by our adversary. We also know that somehow this valley, this town in particular"—she pointed at the map again for emphasis—"is a major focus for their recce efforts."

He knew AN41 could use her chip to sort of see the feeds in her brain.

Legionnaires commonly said things like this: "We *know.*" It meant the MIND had run the sims, billions of regressions, and identified a place on the map like this town, with a population of fewer than 7,500 people, that might be identified as crucial to the outcome of something.

"We'll run a multi-day patrol there, identify the methods the adversary is using to influence the population, stop them if possible, but also bolster confidence in the community that the coalition can protect them and ensure basic security and governance."

Jack nodded and made notes he could pass on to the squad. Everything she said was being piped into his soldiers' helmet comms two vehicles back, but the squad had two brand-new privates, and there was no technology solution to prevent soldiers from falling asleep immediately upon seating themselves inside a vehicle.

"The surrounding area is heavily contested," AN41 said.

This was Legionnaire-speak for high-intensity conflict and violence. The Continental War itself had been incredibly lethal: new weapons, new technology, employed at speed. But it had also been quick. In the current political stalemate, the "heavily contested" areas could go to high-end lethality almost instantly. AN41 meant this could get sporty, but not a small-arms gun fight. She was saying they could get thumped by rockets and high-end killer quadcopters.

"We'll stay along this route until just outside the main population center in the valley. Then we'll dismount the q-peds and move up separate from the vehicle and isolate from the high ground. Once set, we'll go into the village and see what we can sort out."

Jack nodded and looked to her for more guidance, but her eyes glazed over. Something coming across the network was chewing up her human bandwidth.

Jack toggled his screen to a rear-facing view and observed the rest of the patrol. Three crew vehicles, with the rearmost one pulling the q-ped trailer. He noted quadcopters landing on the center vehicle, taking on a battery reload, and then lifting off again to resume station some distance away from the convoy. At any given time, four quadcopters were in the air running a diamond pattern. At least two were armed with direct-fire systems or short-range missiles.

He was seeing their video feeds on his screens and in his AR visor, but he knew AN41 could use her chip to sort of see the feeds in her brain. He also knew she wasn't dedicating much time or focus to it, because the MIND would monitor the feed and spot trouble in the quads' integrated sensor data.

The robotic centerpiece to Legionnaire operations was the q-ped. They were about as big as a Clydesdale horse or a medium-size camel. Each carried a coffin-like box on its back with large, hinged bay doors. These folded down to reveal a variety of payloads: anything from additional quadcopters to short-range-missile racks to medical and treatment capabilities. Jack had no idea how many variants existed, but he knew they were rumored to have hauled small tactical nukes during the decisive-action phase against Donovia.

The three q-peds were behind Jack now, all riding on the trailer with their legs tucked under them like sleeping canines, no observable markings on the mission package boxes on their backs.

He dozed, lulled by the almost imperceptible swaying of the crew compartment, but woke up when he heard the chimes.

"Jack, toggle to QC-1 feed," AN41 said. She was staring blankly ahead, lost in whatever info the MIND was pushing her. He toggled to the quadcopter feed so he could see what she was seeing.

The scene before them looked pretty rough. Ahead, Jack counted the remnants of several houses and at least three vehicles that had been hit with some type of explosive weapon. An Eastern European–looking station wagon was on fire. Multiple Otsoian bodies were strewn about, and most were heavily burned.

"We've got movement on the north side of the burned-out wagon. You have contact with my pointer?" Jack saw the infrared dot she was beaming out of QC-1. It was on his screen, hovering on a moving human just north of the truck.

"Contact pointer," Jack responded.

"Let's dismount your squad and move ... here." She moved the red dot farther to the north along a wooded area that would be the natural avenue of escape if this individual wanted to split.

"Got it. Moving." Jack spoke the words into his helmet mic while bailing out the side of the vehicle and jogging back toward the rest of the squad. He did a quick press check on his rifle and signaled his squad to rally and follow him. He headed toward the northern wood line.

The whine of the quadcopters died away as

Her mouth never moved; the voice was computer-generated to sound just like her.

they picked up a larger orbit around the patrol. AN41 had pushed them out to distance. She was experienced, and this smelled like trouble. She dismounted, and one of the q-peds immediately stood up from the trailer and trotted over to her left shoulder. AN41 was about five foot five on a good day. The eight-foot-tall q-ped towered over her.

The other two Legionnaires were nowhere to be seen, but the other two q-peds had disappeared from the trailer.

AN41 didn't appear to be taking any great tactical precautions as she moved up on the last known location of the person they had seen from the air. A door burst open from the one of the houses, and a child flopped out to the ground at her feet.

The boy looked to be about nine years old and in tremendous distress. AN41 crouched down next to him, her exoskeleton's knee actuators making a soft whine as she did so. The boy was covered in grime and sweat. He held his left arm up in a half-hearted defensive gesture as AN41 spoke quietly to him.

Jack noticed that the boy's clothes and hair were matted with the fine dust that you see settle after buildings are pulverized with high explosives, or after a massive earthquake.

The boy shivered and spoke in a language unrecognizable to Jack but clearly processed by AN41's chip; she nodded and pointed around the scene in conjunction with the boy's murmurs.

Her connection to the MIND gave her access to a translation and behavioral gesture application that put previous versions to shame. The MIND would ingest the boy's statements and provide AN41 with the most appropriate response, based on what it judged the best course of action for the mission. AN41 was still a human, though, and she could choose to adjust the strategy on the fly by instinct, and the MIND would adapt.

And right now, her body language said something didn't fit.

The boy continued to talk and pointed up the slope, to another set of villas and compounds about half a klick away, built directly into the mountainside. He held up two fingers, pointed at himself and at them. Parents? Sisters? He pointed again to the middle compound on the slope and stood up. He tugged on the right forearm of AN41's exoskeleton armor, which contained her close-combat and backup weapon, a 40-caliber single-barrel direct-fire system. The boy started walking up the slope.

"Team, this is AN41. Deploy for contact. We are going to move up and check this out."

Even as she moved, Jack knew, her connection to the MIND was adjusting the strategy and feeding new recommendations into her chip.

~

"Jack, can we get some overwatch on the two smaller compounds to the east?" AN41's voice came over helmet comms, but he was watching her face. She was "speaking," but her mouth never moved; the voice was computer-generated to sound just like her. Jack called up his B Team leader and sent the team to a small, low wall about a quarter of the way up the slope that offered some frontal cover and good sight lines across the entire eastern side of the compound.

The other two Legionnaires had reappeared, and now they started going up the slope on opposite sides. Each had a q-ped in close proximity. Neither was looking at AN41 as she made her way up the middle, behind the boy.

Jack was trying to figure out why the Legionnaires had chosen to take this detour when he heard a computer-generated alert in his comms. "Take cover. Take cover."

In an age of networked sensors and weapons systems, everything happened at a speed humans were not built to manage. There was no bright, hot light from the high explosive. There was no whine from quadcopters, and no bark from machine guns. There was just a feeling of overpressure and the sound of air being split by a projectile.

Behind them, one of their vehicles exploded. Jack was diving toward a large rock to his right as multiple things began to swirl around him. Each of the housings on the back of the q-peds had opened up. AN41's q-ped began flinging countermeasures into the air with a sound like a child's scream. Less than three seconds had passed.

The easternmost q-ped put three short-range missiles in the air while the westernmost one revealed a monster 25mm direct-fire system under its housing and began blasting through a window more than 300 meters up the slope with incredible accuracy.

Jack hit the dirt. Now seven seconds in.

More overpressure. AN41's q-ped exploded.

Jack suspected he knew the system they were up against. It was exceptionally rare to bump into a mobile railgun that accurate, that small, and

You never really hear the rounds. You just feel the pressure as they impact around you.

with that rate of fire. They had stumbled into some trouble here.

Five more seconds had passed. Now came the barking report of a machine gun and the shrieking of a short-range-missile swarm. These could loiter, swarm, even chase if needed. There must have been three dozen in the air—Jack didn't know if they were his side's or the enemy's.

The westernmost q-ped broke station and headed down to cover AN41 as she moved toward the low wall where Jack's B Team was cowering. He crawled over to join them and pulled himself up behind the wall as she came and took a knee next to him. Machine-gun rounds pinged off the q-ped with no visible effect, but making a tremendous racket.

AN41 popped her visor up. Dust clung to her armor. The impact points from the rounds were visible on her exo's shoulder and chest. She grinned. "Here's the plan."

She was interrupted, amid the din of missiles and machine-gun rounds, by a very human scream. The boy, almost forgotten about, had been a little farther up the slope from them when the shooting had started. Now it sounded like he'd been hit. As his screams continued, AN41 jumped the wall and moved toward him. She hesitated as she closed on the boy. The moment's delay was enough.

AN41 dropped as if someone had flipped off her light switch. The other two Legionnaires reacted instinctively when she was hit and broke cover for just an instant. Both were immediately dropped. Suddenly, all fire from the top of the hill shifted to the low wall.

"Jack. This is Annie."

"Moving your way, 41." He motioned for Team B to cover him as he prepared to leave the shelter of the low wall.

"Jack." Her voice on his internal audio was calm and steady, but insistent. "I want you to hold what you've got."

Jack was breathing heavily; the stress of being under fire, combined with the exertion, had his ears ringing and heart pounding.

"Jack, you know what it wants. It needs to take all three of us alive. It will kill the rest of your squad and then come down here and collect us."

Three more enemy quadcopters began to move lower on the horizon. Another q-ped exploded from a railgun shot. The last q-ped's active suppression was going crazy, flinging small projectiles into the air at an unsustainable pace.

"Jack." This one was firm; she sounded different. "I'm offline with my team. They may be unconscious."

"I'm also paralyzed," she continued.

"Jack, we've got about 90 seconds here. The Q is down to projectile countermeasures, and those quadcopters are going to chew you all up once it runs out. This was a damn good trap. And I walked us right into it."

"41, we'll have fast movers up here ... Just keep hanging on."

"Jack, CAS is 20 minutes out. We don't have much time to discuss. I need you to do what you have to do—what someone did for your brother."

Jack momentarily flashed back to the man in uniform handing a US flag to his mother. He had heard the stories, but he hadn't wanted to believe Ben had gone down like this. He had been too good.

The quadcopters were screaming in now.

Annie had her helmet off and her eyes closed. Her mouth wasn't moving, but Jack still heard her in his ears.

"Jack. Thirty seconds. Make it count."

"Can't do this, 41. Not in me."

"No time for that, Jack, this is bigger than you. This is why your squads come out with us. The MIND can't do this for us, but you can."

The last two quadcopters were spitting fire now, but Jack couldn't hear it. Time was slowing down.

You never really hear the rounds. You just feel the pressure as they impact around you. Jack rolled to a nearby opening in the low wall, his optic integrated with the visor. He fired twice and rolled back, but not before catching a glimpse of the boy, clearly unhurt, running up the slope toward the compound. He must have been chipped too, Jack realized—the only way he could have played his part so perfectly in an otherwise entirely automated ambush.

Immediately after Jack shot Annie, the firing stopped. The swarm of missiles dropped to the earth, dead lumps of metal. The quadcopters turned and flew off, their buzzing echoing down the valley as it faded.

Colonel Jasper Jeffers is an infantry officer who has been deployed to Iraq, Afghanistan, and elsewhere. This story won the 2019 Science Fiction Writing Contest run by the Army Mad Scientist Laboratory. A longer version was first published by the Modern War Institute on its website.

Looking back at the future of warfare

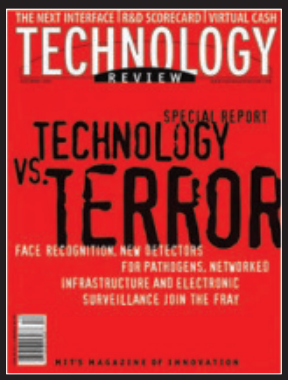
Our war coverage through the years has emphasized how technology might change the way wars are fought—or how it could help us avoid conflict in the first place.

June 1967

From "The first battle of World War III": World War I was fought with chemistry, and World War II with physics …. World War III, if it ever occurs, may be fought bloodlessly with mathematics. It is not wholly inconceivable that two opposing general staffs will gather some day in full battle dress for a morning's war at an international computer center. At preliminary low-level conferences they will have already agreed on a computer program and, like attorneys at a pre-trial hearing, stipulated essential input data. All that will remain to be done on the fateful morning will be to push the "start" button and wait for the computer to wage the war 10,000 times. We can envision one commander-in-chief pushing aside a sheaf of print-outs that he has been poring over. "Okay," he says. "You wiped us out 9,327 times. I'll tell my Prime Minister to pull out of the Balkans."

April 1984

From "The Fallacy of Laser Defense": During a televised address to the nation on March 23, 1983, President Reagan surprised many viewers by proposing a long-term plan to shield the United States against nuclear attack … Despite the Reagan administration's rhetoric about making nuclear weapons obsolete through defense, the Pentagon is already studying how to penetrate a future Soviet BMD (ballistic-missile defense) system. Under a program operated by the Defense Nuclear Agency at a yearly cost of $3.5 million, pieces of U.S. ICBMs have been exposed to lasers modeled after those used in Soviet research, so engineers can develop countermeasures. DARPA is also working on laser-resistant materials … In sum, as military analyst Thomas Karas has written, "As long as both sides are determined to maintain it, assured destruction is bound to be mutual."



December 2001

From "Recognizing the Enemy": Of all the dramatic images to emerge in the hours and days following the September 11 attacks, one of the most haunting was a frame from a surveillance-camera video capturing the face of suspected hijacker Mohamed Atta as he passed through an airport metal detector in Portland, ME. Even more chilling to many security experts is the fact that, had the right technology been in place, an image like that might have helped avert the attacks. According to experts, face recognition technology that's already commercially available could have instantly checked the image against photos of suspected terrorists on file with the FBI and other authorities. If a match had been made, the system could have sounded the alarm before the suspect boarded his flight.

MIT Technology Review (ISSN 1099-274X), November/December 2019 issue, Reg. US Patent Office, is published bimonthly by MIT Technology Review, 1 Main St. Suite 13, Cambridge, MA 02142-1517. Entire contents ©2019. The editors seek diverse views, and authors' opinions do not represent the official policies of their institutions or those of MIT. Periodicals postage paid at Boston, MA, and additional mailing offices. Postmaster: Send address changes to MIT Technology Review, Subscriber Services, PO Box 5001, Big Sandy, TX 75755, or via the internet at www.technologyreview.com/customerservice. Basic subscription rates: $59.94 per year within the United States; in all other countries, US$69. Publication Mail Agreement Number 40621028. Send undeliverable Canadian copies to PO Box 1051, Fort Erie, ON L2A 6C7. Printed in USA. Audited by the Alliance for Audited Media.