

UNIT X

HOW THE PENTAGON AND
SILICON VALLEY ARE TRANSFORMING
THE FUTURE OF WAR

RAJ M. SHAH AND CHRISTOPHER KIRCHHOFF

SCRIBNER

NEW YORK LONDON TORONTO SYDNEY NEW DELHI



Scribner

An Imprint of Simon & Schuster, LLC

1230 Avenue of the Americas

New York, NY 10020

Copyright © 2024 by Raj M. Shah and Christopher Kirchhoff

All rights reserved, including the right to reproduce this book or portions thereof in any form whatsoever. For information, address Scribner Subsidiary Rights Department, 1230 Avenue of the Americas, New York, NY 10020.

First Scribner hardcover edition July 2024

Scribner and design are trademarks of Simon & Schuster, LLC

Simon & Schuster: Celebrating 100 Years of Publishing in 2024

For information about special discounts for bulk purchases, please contact Simon & Schuster Special Sales at 1-866-506-1949 or business@simonandschuster.com.

The Simon & Schuster Speakers Bureau can bring authors to your live event. For more information, or to book an event, contact the Simon & Schuster Speakers Bureau at 1-866-248-3049 or visit our website at www.simonspeakers.com.

Interior design by Hope Herr-Cardillo

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data has been applied for.

ISBN 978-1-6680-3138-4

ISBN 978-1-6680-3143-8 (ebook)

If there are to be yet unimagined weapons affecting the balance of military power tomorrow, we want to have the men and the means to imagine them first.

—James Killian,
science advisor to Dwight Eisenhower

The second decade of the 21st Century was one of colossal missed opportunities for the U.S. military. The Pentagon missed the advent of modern software development, the move to cloud computing, the commercial space revolution, the centrality of data, and the rise of AI and machine learning. It's a story of the U.S. getting ambushed by the future.

—Christian Brose, staff director,
U.S. Senate Armed Services Committee

I think Henry Ford once said, "If I'd asked customers what they wanted, they would've told me a faster horse."

—Steve Jobs

INTRODUCTION: SLOW BURN

It was three in the morning, pitch black. Raj M. Shah, a twenty-seven-year-old U.S. Air Force captain, two weeks into his first tour of combat duty in 2006, was piloting an F-16 Viper along the border between Iraq and Iran when he suddenly realized he couldn't easily tell which side of the border he was on. This was a problem, because American pilots who flew into Iranian airspace ran the risk of causing an international incident—or worse, not flying back out. The F-16 was a remarkable machine—it could fly at twice the speed of sound and outmaneuver any fighter jet in the world—but, frustratingly, its outdated navigation system couldn't graphically pinpoint the plane's location on a moving map. Slip over the line at five hundred miles per hour and in less than a minute Raj could be eight miles into Iran, well within range of its anti-aircraft batteries.

There was no way to update the navigation software. So Raj figured out a hack. Back in the barracks, he had a Compaq iPAQ, a handheld device for checking email and playing Tetris. He loaded it with civilian navigation software and digital maps, snuck it into the cockpit, and kept it strapped to his knee as he flew. The software in that little \$300 gadget did a better job of telling him where he was than the system in a \$30 million jet.

That was the first time Raj realized how far Silicon Valley had leapt ahead of defense contractors like General Dynamics and Lockheed Martin when it came to developing new technology, especially software.

Ten years after Raj's hack, the outside world had self-driving cars, virtual reality goggles, and smartphones that could summon an Uber, handle banking, and pay for groceries. Yet legacy tech riddled the military's ranks. It was as if the military had resigned itself to becoming a display in the Museum of Computer History. You could visit an army, air force, or naval base to see what people used in the past, then go to Best Buy to see how far technology had evolved.

But this time, Raj could do a lot more about it than attach a pocket computer to his knee. The Secretary of Defense had appointed us (Raj and Chris) to run Defense Innovation Unit Experimental (DIUx), or Unit X for short, the Pentagon's newly created outpost in Silicon Valley. Before taking over DIUx, Raj had founded a cybersecurity startup, which he successfully sold, and he was looking for a chance to do it again. Chris, a Harvard educated Ph.D. political scientist, was the lead strategist for technology at the National Security Council.

Our mission at DIUx wasn't just to find hardware and software so military units around the world could better perform their mission. It was to disrupt and transform the culture of the largest and possibly most bureaucratic organization in the world by infusing its clogged arteries with the nimble, agile DNA of Silicon Valley—in other words, to hack the Pentagon.

Imagine a stealthy electric flying car that lands like a helicopter, flies in near silence, and can autonomously navigate behind enemy lines to drop off, pick up, or resupply U.S. forces. Or tiny AI-powered quadcopters that can map the inside of a building and recognize faces of terrorists before Navy SEALs break down the door. Or a constellation of microsatellites that can see through clouds, enabling intelligence agencies to keep a constant eye on ISIS troop movements and North Korean missiles.

All these advanced technologies—and many more like them—were being developed in 2016. They were designed not by brand-name defense companies but by plucky startups in Silicon Valley. And guess what? The U.S. military barely knew anything about them.

The U.S. had fallen dangerously behind its rivals when it came to technology. By the time we were recruited to DIUx, it was an open secret inside the Pentagon that if the U.S. went to war with China, we'd lose far more soldiers, sailors, marines, and airmen than our war plans anticipated. We might very well suffer an outright defeat, ending the era of American supremacy that began at the Second World War's end.

In a boom heard around the world, China's military leapt ahead of ours in October 2021 by launching the world's first nuclear-capable hypersonic weapon—an arrowhead-shaped sheath of titanium that flies at ten times the speed of sound, can't be seen by early warning radars, and, unlike slower intercontinental ballistic missiles, can change direction in flight, evading all known defenses. With this weapon, the People's Liberation Army can strike anywhere in the world in under fifteen minutes. The chairman of the Joint Chiefs of Staff called it "China's Sputnik Moment," comparable to the surprise Soviet launch of the world's first satellite in 1957.

How had this happened? How did the country with the largest economy and most innovative technology companies fall so far behind?

Quite simply, sometime in the 1990s, Silicon Valley and the Pentagon stopped talking to each other.

Even as Apple, Google, Microsoft, and Amazon grew into technical and business behemoths, each bigger by market capitalization than the entire defense industry combined, the Department of Defense was content to keep dealing with a handful of giant defense contractors, like Lockheed Martin, Northrop Grumman, and Raytheon—known in Washington as the "primes." This arrangement suited members of Congress who controlled the budget. The Pentagon even relied on the primes to develop the military's IT and software, a folly akin to hiring Microsoft to build an aircraft carrier. For two decades, no Secretary of Defense even bothered to set foot in Silicon Valley—not when Google invented search or Apple the iPhone or Facebook social networks or Amazon cloud storage.

For its part, the Valley had soured on doing business with the Pentagon. Startups didn't need the headache of dealing with a customer that took years to close a sale and then even more years to start using the product and paying for it. Moreover, many engineers and technologists in Silicon Valley had deep moral objections to creating products that might be used to kill people, and they demanded their companies refuse to sign contracts with the military or intelligence agencies.

In ordinary times, the de facto divorce between technologists on the West Coast and policymakers on the East Coast wouldn't imperil the future of American power. But the 2010s weren't ordinary times. Russia's Vladimir Putin, Chinese president Xi Jinping, the supreme leader of Iran, and North Korea's Kim Jong-un each saw new ways to defeat the U.S. technologically.

While most people on both coasts missed the significance of what was happening, a few of us saw the slow-motion car crash that had already begun, and we started doing all we could to stop it.

A turning point came in 2015 when President Barack Obama appointed Ash Carter to be Secretary of Defense. As soon as Carter was sworn in as secretary, he traveled to Silicon Valley to give an address to the tech industry.

"We need to drill holes in the wall that exists between the Department of Defense and the commercial and scientific sector," Carter implored.

He vowed to shake up the Department of Defense and adopt the nimble business practices of Silicon Valley. Most importantly, he wanted to start buying tech products. *Lots* of tech products. Carter's message was loud and clear: the Pentagon was open for business and wanted to push a giant shopping cart down the aisles of Silicon Valley.

Since shopping on the West Coast is hard to do from the East Coast, Carter announced that the Pentagon would open an embassy- slash-venture-fund in Silicon Valley called the Defense Innovation Unit Experimental, or DIUx. A thirty-person team would be housed in an

office building at Moffett Field, a decommissioned naval air station in Mountain View, across the fence from Google's campus.

With the military as an early user, startups could get up and running. And with the promise of future revenue the military could provide, venture capital firms would be more likely to invest. This was Carter's vision: to use military money not just to buy existing products but to help entrepreneurs develop new ones, and to harness the financial power of venture capital firms to back more businesses selling to the Defense Department. DIUx would be the fulcrum on which Carter would pivot the entire U.S. military.

But DIUx faced a daunting challenge—how to fix the parts of the Pentagon that would open the floodgates to commercial technology. Carter had vowed to speed things up and transform its risk-averse culture so that innovative products could zip from office parks in Palo Alto and Mountain View into the hands of service members. That sounded great, but the Department of Defense is the largest organization in the world, with 3 million employees, a sprawling set of offices that oversee the army, air force, navy, and marines, more rules and regulations than the Byzantine Empire, and an ingrained resistance to change. This was the organization that fielded fighter jets with outdated navigation systems and operated command centers with decades-old mainframes running software so buggy that the bugs had bugs. Now they were going to start using artificial intelligence and iPhones?

Carter's plan envisioned Silicon Valley's founders and engineers eagerly answering his call. But, as Edward Snowden had revealed, this was the same group the government had secretly manipulated to conduct espionage. The Iraq War, warrantless wiretapping, and drone strikes were things many in Silicon Valley opposed. How could a group of people so understandably alienated from the hard power of the military be enticed to help enhance its lethality? They'd come of age building technology that would make the world a better, not deadlier, place.

It was easy to give a speech about innovation and transformation and

drilling holes in walls. But who in their right mind would sign up to do the drilling?

Well, that was us.