CrimethInc.
War is Already Here
It's Just Not Very Evenly Distributed
February 16, 2017

Retrieved on 22nd April 2021 from crimethinc.com

theanarchistlibrary.org

War is Already Here

It's Just Not Very Evenly Distributed

CrimethInc.

February 16, 2017

Contents

Here at the tech desk, we'll examine technology and its effects from an anarchist perspective. We'll publish accessible guides and overviews on topics like encryption, operational security, and how to strengthen your defenses for everyday life and street battles. We'll zoom out to explore the relation between technology, the state, and capitalism—and a whole lot more. Stay tuned.

to capitalism. Even the most left-leaning technologists aren't interested in addressing the drawbacks of the social order that has concentrated so much power in their hands.[10]

War

Nation states are *already* engaging in cyber warfare. Someone somewhere[11] has been learning how to take down the internet.

Tech companies are best positioned to create a registry of Muslims and other targeted groups. Even if George W. Bush and Barack Obama hadn't already created such lists and deported millions of people, if Donald Trump (or any president) wanted to create a registry for roundups and deportations, all he'd have to do is go to Facebook. Facebook knows everything about you.

The Obama administration built the largest surveillance infrastructure ever—Donald Trump's administration just inherited it. Liberal democracies and fascist autocracies share the same love affair with surveillance. As liberalism collapses, the rise of autocracy coincides with the greatest technical capacity for spying in history, with the least cost or effort. It's a perfect storm.

This brief overview doesn't even mention artificial intelligence (AI), machine learning, virtual reality (VR), augmented reality (AR), robots, the venture capital system, or tech billionaires who think they can live forever with transfusions of the blood of young people.

[10] We'll explore this more in a later article about "The California Ideology."

[11] Probably a state-level actor such as Russia or China.

"The future is already here," Cyberpunk pioneer William Gibson once said; *"it's just not very evenly distributed."* Over the intervening decades, many people have repurposed that quote to suit their needs. Today, in that tradition, we might refine it thus: *War is already here—it's just not very evenly distributed.*

Never again will the battlefield be just state versus state; it hasn't been for some time. Nor are we seeing simple conflicts that pit a state versus a unitary insurgent that aspires to statehood. Today's wars feature belligerents of all shapes and sizes: states (allied and non-allied), religious zealots (with or without a state), local and expatriate insurgents, loyalists to former or failing or neighboring regimes, individuals with a political mission or personal agenda, and agents of chaos who benefit from the instability of war itself. Anyone or any group of any size can go to war.

The increased accessibility of the technology of disruption and war[1] means the barrier to entry is getting lower all the time. The structure of future wars will sometimes feel familiar, as men with guns murder children and bombs level entire neighborhoods—but it will take new forms, too. Combatants will manipulate markets and devalue currencies. Websites will be subject to DDoS attacks and disabling—both by adversaries and by ruling governments. Infrastructure and services like hospitals, banks, transit systems, and HVAC systems will all be vulnerable to attacks and interruptions.

In this chaotic world, in which new and increasing threats ceaselessly menace our freedom, technology has become an essential battlefield. Here at the CrimethInc. technology desk, we will intervene in the discourse and distribution of technological know-how in hopes of enabling readers like you to defend and expand your autonomy. Let's take a glance at the terrain.

[1] A surplus of AK-47s. Tanks left behind by U.S. military. Malware infected networked computer transformed into DDoS botnets. Off the shelf ready to execute scripts to attack servers.

Privacy

The NSA listens to, reads, and records everything that happens on the internet.

Amazon, Google, and Apple are always listening[2] and sending some amount[3] of what they hear back to their corporate data centers[4]. Cops want that data. Uber, Lyft, Waze, Tesla, Apple, Google, and Facebook know your whereabouts and your movements all of the time. Employees spy on users.

Police[5] want access to the contents of your phone, computer, and social media accounts—whether you're a suspected criminal, a dissident on a watch list, or an ex-wife.

The business model of most tech companies is surveillance capitalism. Companies learn everything possible about you when you use their free app or website, then sell your data to governments, police, and advertisers. There's even a company named Palantir, after the crystal ball in *The Lord of the Rings* that the wizard Saruman used to gaze upon Mordor—through which Mordor gazed into Saruman and corrupted him.[6] Nietzsche's famous quote, "When you look long into an abyss, the abyss also looks into you," now sounds like a double transcription error: surely he didn't mean *abyss,* but *app.*

[2] Amazon Echo / Alexa. Google with Google Home. Apple with Siri. *Hey Siri, start playing music.*

[3] What, how much, stored for how long, and accessible by whom are all unknown to the people using those services.

[4] Unless you are a very large company, "data center" means someone else's computer sitting in someone else's building.

[5] Local beat cops and police chiefs, TSA, Border Patrol, FBI… all the fuckers.

[6] Expect to read more about Palantir and others in a forthcoming article about surveillance capitalism.

Security

Self-replicating malware spreads across Internet of Things (IoT) devices like "smart" light bulbs and nanny cams, conscripting them into massive botnets. The people who remotely control the malware then use these light bulbs and security cameras to launch debilitating DDoS[7] attacks against DNS providers, reporters, and entire countries.

Hackers use ransomware to hold colleges, hospitals, and transit systems hostage. Everything leaks, from nude photos on celebrities' phones to the emails of US political parties.

Capital

Eight billionaires combined own as much wealth as the poorest 50% of the world's population. Four of those eight billionaires are tech company founders.[8] Recently, the President of the United States gathered a group of executives to increase collaboration between the tech industry and the government.[9]

The tech industry in general, and the Silicon Valley in particular, has a disproportionately large cultural influence. The tech industry is fundamentally tied to liberalism and therefore

[7] Distributed Denial of Service. More on this in a later article, as well.

[8] Bill Gates, Jeff Bezos, Mark Zuckerberg, Larry Ellison. In fact, if you count Michael Bloomberg as a technology company, that makes five.

[9] In attendance: Eric Trump. Brad Smith, Microsoft president and chief legal officer. Jeff Bezos, Amazon founder and CEO. Larry Page, Google founder and Alphabet CEO. Sheryl Sandberg, Facebook COO. Mike Pence. Donald Trump. Peter Thiel, venture capitalist. Tim Cook, Apple CEO. Safra Catz, Oracle CEO. Elon Musk, Tesla CEO. Gary Cohn, Goldman Sachs president and Trump's chief economic adviser. Wilbur Ross, Trump's commerce secretary pick. Stephen Miller, senior policy adviser. Satya Nadella, Microsoft CEO. Ginni Rometty, IBM CEO. Chuck Robbins, Cisco CEO. Jared Kushner, investor and Trump's son-in-law. Reince Priebus, chairman of the Republican National Committee and White House chief of staff. Steve Bannon, chief strategist to Trump. Eric Schmidt, Alphabet president. Alex Karp, Palantir CEO. Brian Krzanich, Intel CEO.