Beyond the Burner

Practical Digital Security & Privacy for Organizers

INDIVISIBLE
BALTIMORE COUNTY

contact@indivisible-baltimorecounty.org

Session Overview

Introduction

- Purpose & Objectives

SITREP: Where are we in July 2025?

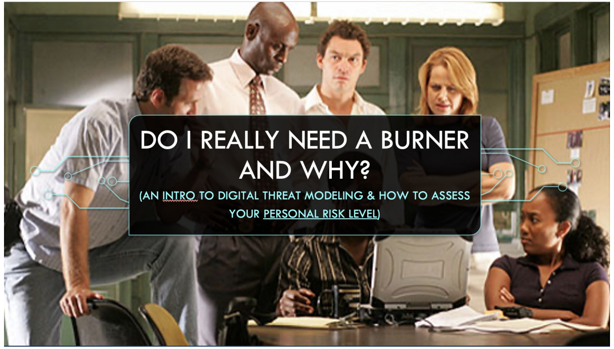
- Surveillance Capitalism Meet Autocracy
- Life below the “Cyber Poverty Line”

Pause for Discussion, Questions and Feedback

OPLAN: How do we prep for 2026 and beyond?

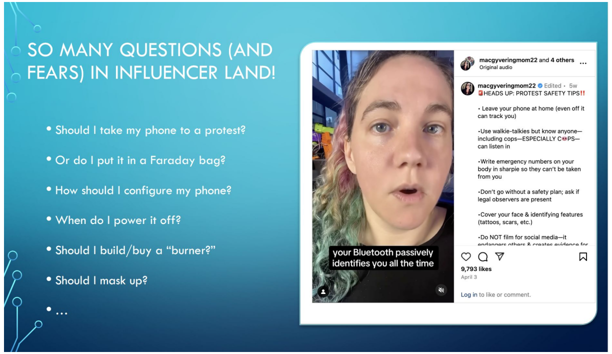
- Security & Privacy Terminology
- Partitioning the Solution Space: Leaders vs. Members
- Immediate Actions and Follow-on actions

Wrap-Up Discussion, Questions and Feedback



DO I REALLY NEED A BURNER AND WHY?

(AN INTRO TO DIGITAL THREAT MODELING & HOW TO ASSESS YOUR PERSONAL RISK LEVEL)



SO MANY QUESTIONS (AND FEARS) IN INFLUENCER LAND!

- Should I take my phone to a protest?
- Or do I put it in a Faraday bag?
- How should I configure my phone?
- When do I power it off?
- Should I build/buy a “burner?”
- Should I mask up?
- …

your Bluetooth passively identifies you all the time

macgyveringmom22 and 4 others ...
Original audio

macgyveringmom22 Edited • 5w
🚨HEADS UP: PROTEST SAFETY TIPS‼️

• Leave your phone at home (even off it can track you)

•Use walkie-talkies but know anyone—including cops—ESPECIALLY C🐽PS—can listen in

•Write emergency numbers on your body in sharpie so they can’t be taken from you

•Don’t go without a safety plan; ask if legal observers are present

•Cover your face & identifying features (tattoos, scars, etc.)

•Do NOT film for social media—it endangers others & creates evidence for

9,793 likes
April 3

Log in to like or comment.

💡Purpose & Objectives

Why are we here?

- Create a **shared understanding** of the **privacy and cybersecurity challenges** faced by Indivisible Groups during this **moment of authoritarian breakthrough** (that has been enabled by U.S. tech ~~leaders~~ oligarchs)
- Define concrete actions that **Indivisible members, organizers and groups** can take to **lift our groups above the "Cyber Poverty Line"**

**** This as an experiment to build a community of teachers and learners that can prepare themselves and their groups for operating for uncertainty digital threat environment.*

SITREP

Where are we in July 2025?

2025: Over 3 Decades of Tech “Innovation” & Market Consolidation

1990s Bush Clinton	“End of History” & Gulf War 1.0 Windows 95 & the Commercial Internet. “Solar Sunrise” & “Eligible Receiver” DotCom/E-Commerce. Telcom Bubble, Cisco. Yahoo
2000s Bush Obama	9/11 & The Patriot Act. GWOT & “Axis of Evil.” Rise of SaaS, SalesForce, Google and Web 2.0. Golden Age of Internet Worms Microsoft “TrustWorthy Computing” Mobile: Nokia to BlackBerry to iPhone/Android Great Financial Crisis
2010s Obama Trump	Age of **“Big Data”** Machine Learning, Analytics Twitter, Facebook Operation Aurora. Edward Snowden. Stuxnet. APTs. DNC Hack. **Cloud** Concentration of Compute, Data, and Algorithms GDPR. Brexit. Wikileaks. Solar Winds.
2020s Biden Trump	CCPA. COVID Tech Bubble Rise & Fall of Anti-Disinformation / Content Moderation Russia-Ukraine War. October 7. SingnalGate. AI Bubble

Long Term Cyber/Tech Trends

- Market forces (disruption due to **high profile incidents**, nation state **breaches** & new technologies) ***have* driven major improvements.**
  - Products <u>are</u> safer that they were 30 years ago, but complexity, interdependence has also increased–and reliance (and too must trust) in a few U.S. companies.
- Cyber and disinformation **ops by sophisticated state/non-state actors** have had significant global (military and political) impact
- Across all administrations, the **"public private partnership" meant <u>industry has driven policy</u>.**
  - Corporations have escaped significant product security/privacy regulation, with some exceptions (EU, USGOV vendors and agencies)
- Stock **market valuations mirror the concentration of data, compute, power** of Big Tech.
  - COVID and AI Bubble have accelerated this!
- In terms of funding, tools, organizational maturity, workforce there is a **massive gap between the have and the have nots**

the "Cyber Poverty Line"

What is the Cyber Poverty Line? (Wendy Nather, Cisco)

"…organizations that struggle with security usually because of **insufficient IT budget, expertise, capability, or influence.** These entities might include startups struggling to get a product to market, schools, and small-to-medium enterprises (SMEs) **without the resources for dedicated security staff, or the information technology (IT) departments** of state, local, tribal, and territorial governments (SLTTs) doggedly competing for **scarce taxpayer funding**. There are other, less intuitive examples too: **large enterprises with low margins; organizations where considerations for safety far outweigh those for security, as in aviation and healthcare;** and any entities that **cannot influence their own supply chains** to improve security. Cyber poverty exhibits dynamics very similar to real-world poverty: **simply providing money or free expertise does not necessarily address poor technological designs, poor market incentives, misaligned sociocultural attitudes towards security**, or other barriers."

https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line/

Atlantic Council

Common Volunteer/Nonprofit Tech/Cyber Challenges

- **Scarce cybersecurity expertise** and **single points of knowledge/ownership**
  - BYOE (Bring Your Own Everything) with **lack of governance**, policy, standards – *typically foundations of security & privacy programs*.
- Most **communication and collaboration occurs using free services** from U.S. Cloud Providers – *especially Google and Microsoft*
- Many **cloud** (including those used by activists) **tools lack enterprise features**
  - Monitoring, MFA, privileged account management, etc.
- **Ease of use**/access/communication often **outpriorizes security and privacy**
- **Spotty general tech literacy** among pro-democracy communities
  - Activist demographics skew older and tend to be less tech savvy, challenges using (let alone) securing too many tools.
- Use of **older hardware** and **software**
  - PCs, laptops, mobile devices that might not be patcheable or easy to secure.

OPLAN

Preparing for 2026 and beyond

Some terms… Same but different?

Safety

protection from hazards (usually accidental or natural)

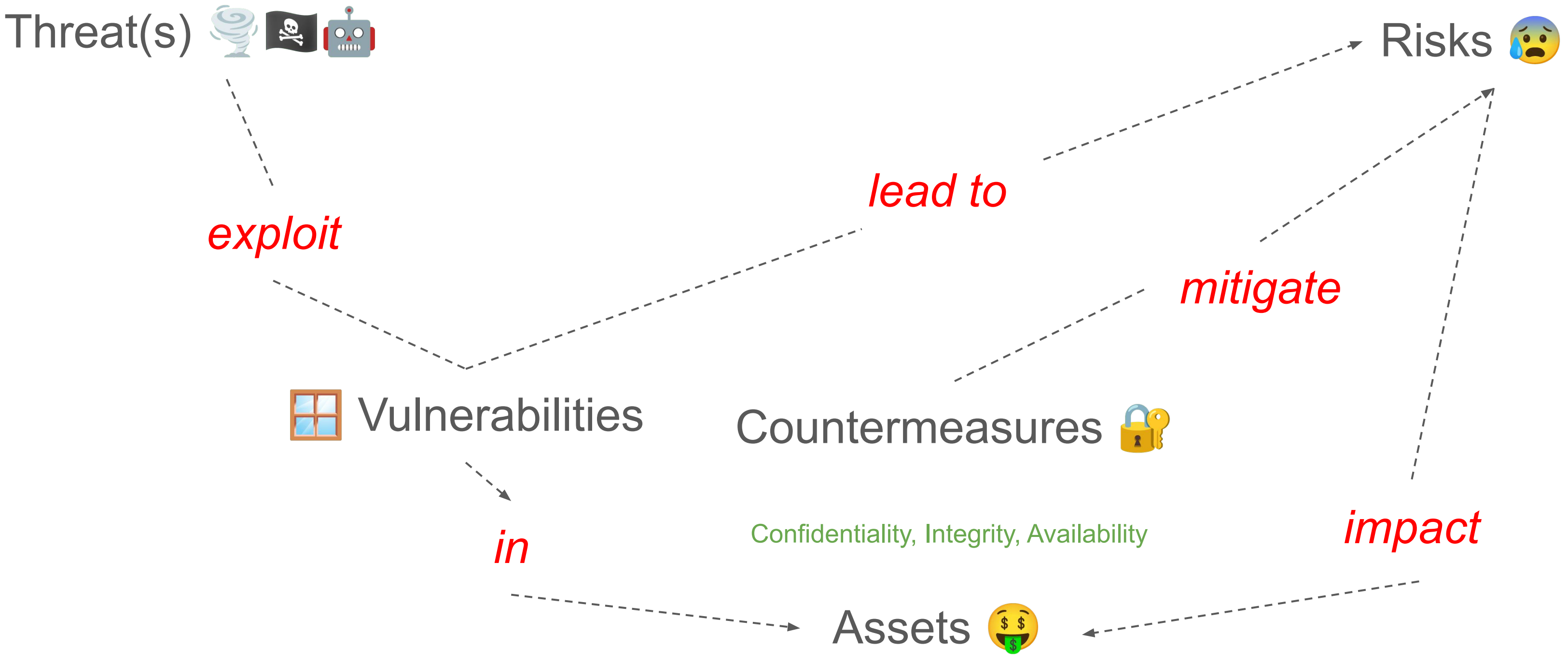
Security

safeguarding an asset from (usually intentional) threats

Privacy

the right to be “left alone” or not be tracked, and your data handled appropriately

Core Security Concepts (Both Physical and Cyber)



Threat(s) 🌪️🏴‍☠️🤖

exploit

🪟 Vulnerabilities

lead to

Risks 😰

in

Assets 🤑

Countermeasures 🔐

mitigate

impact

Confidentiality, Integrity, Availability

Who does what: Partition Next Actions by Risk, Effort, Impact

Who	What & Why
Leaders & Organizers	- Have the most access to the tools and data–*are likely privileged users* - Most visible (and vocal?) and might be first targeted by threat actors? - Highest level of engagement and motivation, so (hopefully) can achieve wins quickly, once they level up their skills. - Can (and should) model good practices and train others
Indivisible Groups	- Requires alignment, consensus, coordination and resources and lots of meetings, commitment across the group to implement controls. - Can provide resilience and structure to sustain growth and OpSec - Accountable (risk owners) for tools and data of members?
Members & Participants	- Varying levels of engagement could make compliance challenging - Variety of skill levels and risk levels–*generational differences.*

Some Threat Scenarios to Ponder (Risk = Likelihood x Severity)

What could/should be done to deter/prevent/respond?

- County/city police gains access to member lists including email, phone number and then …
- Far Right Hacktivist groups target organizer phones with malware to …
- Infiltration by counter-protestors into Signal Chats through compromised member account or PC/Phone
- U.S. Cloud company suspends personal email address upon request from local/federal law enforcement
- Physical device seizure (laptop/mobile device) during protest or F2F meeting
- "Script Kiddie" compromise of Mobilize admin account due to weak password and gets all the signups information about actions.

What else? Save your thoughts for discussion.

Immediate Actions: Leaders MUST set the example

- Compartmentalize personal and organizational/activism online accounts
    - Should you get locked out accounts or those were compromised by an attacker/nation state
    - Migrate activism off the personal emails you uses for the 3F’s (Family, Friends, Finances)
- When available, ensure strong MFA (Authenticator NOT) on ALL email/cloud accounts where it available
    - Withstand compromise of email (brute force and resist Phishing attacks
- Consider segregated data and device usage for personal vs. democracy work
    - Create a different user on your laptop if a dedicated system
    - Microcenter has inexpensive refurbished PCs and laptops
- Consider diversification across multiple cloud providers for personal accounts
    - Apple, Google, Microsoft, and Proton
- Enable you have full disk/device encryption (with strong password/passphrase)
- Secure your passwords
    - Local password safe or trusted password provider
    - Decide which passwords you save in your browser

Authy

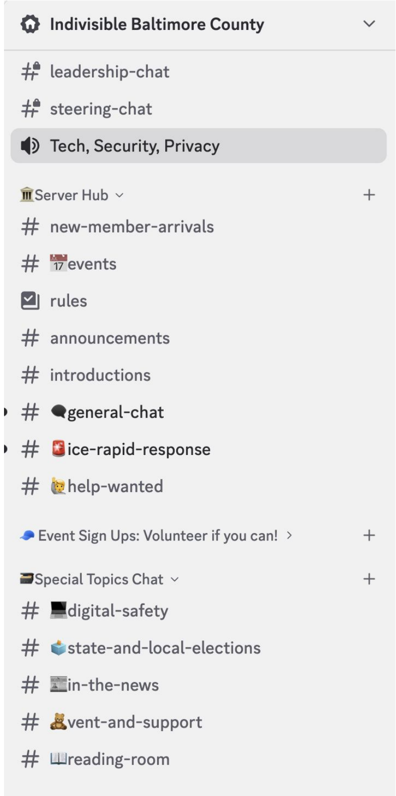
Proton Mail

KeePassXC

Microsoft
Authenticator

Immediate Actions: Groups

- **Perform a Digital Asset Inventory, focusing on “ownership” and data content, storage, and export capabilities**
  - Cloud Accounts (Google/Microsoft)
  - Outbound Communication (MailChimp, etc.)
  - Banking and Act Blue accounts
  - Mobilize, ExtraAction and other engagement platforms
  - Slack, Discord, Signal Groups, etc.
  - Website/Content Management System
  - Social Media Groups
- **Iterate on privacy and risk norms with goal of establishing a policy**
  - What data can/should be collected about members?
  - Who has access? Who can it be shared with? Where is it stored?
  - Game out exposure scenarios and consequences, appreciate differences across demographics
- **Find a “security champion”** who can promote awareness and education with the group
  - Establish a channel (Discord, Slack, etc.) for sharing information and putting together a curriculum and discussion groups for rational risk discussions
- **Standardize on Signal** for “sensitive” comms (sharing passwords or other data)
  - Establish procedures for channel governance and lifecycle
- **Review best practices for small business**
  - UK Guidance for Small Businesses



Follow-On Actions: Organizations

- Develop a **Risk Register** based on the Digital Asset Inventory
  - Classify Risk, Threat, Vulnerability, Asset
- Develop a **basic privacy plan** for member data and Ops (protests, etc.)
- Implement controls to address high risks
  - Harden shared documents (stop using Google Share Link!)
  - Depending on funds, implement group email inbox and for external communication to front-end member identity
- Determine **document management** approach
- Develop a **vendor/tool assessment checklist** as you make choices
  - What data do you feel safe hosting where?
- **Brainstorm risk and threat contingencies** to drive awareness among members

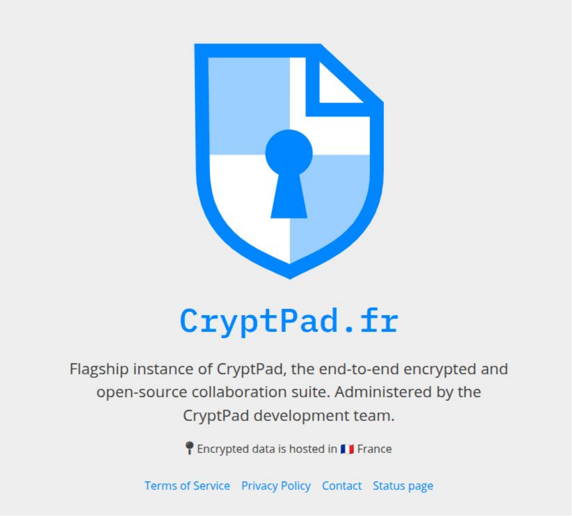
Immediate Actions for Members

- **Reflect on personal risk tolerance** and their digital exposures (devices, online accounts, etc.)
  - Evaluate whether they in a higher risk group and need to adopt practices recommended for leaders
- Begin the **journey of basic system hygiene** and privacy awareness
  - Application, Operating System, and Mobile Device updates
- Consume online security training (Canada, UK, EU)
  - https://www.getcybersafe.gc.ca/en
  - https://www.ncsc.gov.uk/

What else?

Thinking about the worst, worst case

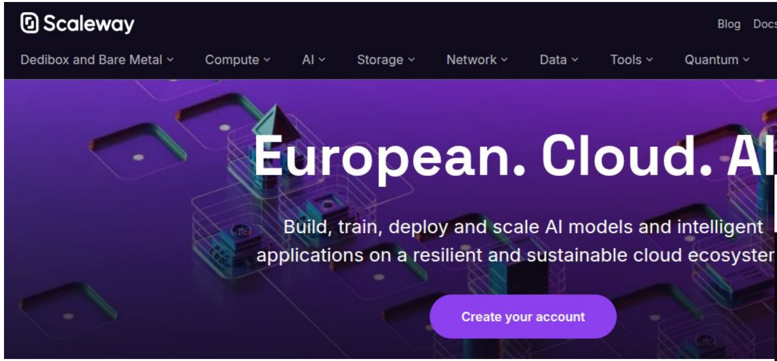
- Migration off U.S. Technology Providers?
- Self-Hosting Secure Communication Platform?


CryptPad.fr

Flagship instance of CryptPad, the end-to-end encrypted and open-source collaboration suite. Administered by the CryptPad development team.

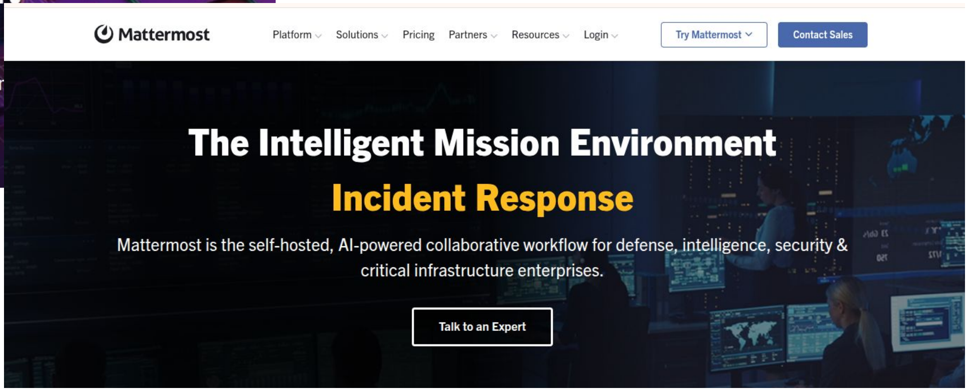
Encrypted data is hosted in 🇫🇷 France

Terms of Service Privacy Policy Contact Status page



European. Cloud. AI.

Build, train, deploy and scale AI models and intelligent applications on a resilient and sustainable cloud ecosyster



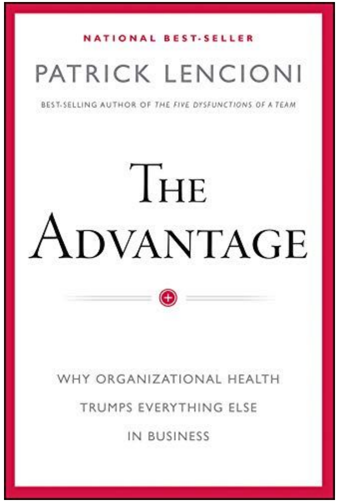
The Intelligent Mission Environment

Incident Response

Mattermost is the self-hosted, AI-powered collaborative workflow for defense, intelligence, security & critical infrastructure enterprises.

Reading on Building Resilient Organizations

(Security & Privacy are Socio-Technical Problems)



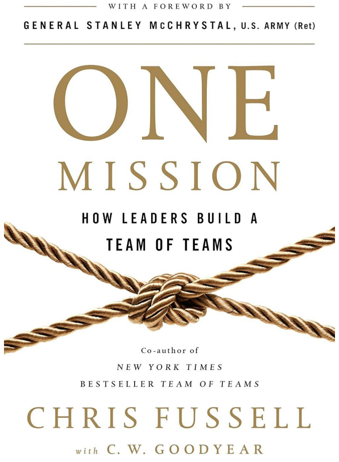
NATIONAL BEST-SELLER

PATRICK LENCIONI

BEST-SELLING AUTHOR OF *THE FIVE DYSFUNCTIONS OF A TEAM*

THE ADVANTAGE

WHY ORGANIZATIONAL HEALTH TRUMPS EVERYTHING ELSE IN BUSINESS



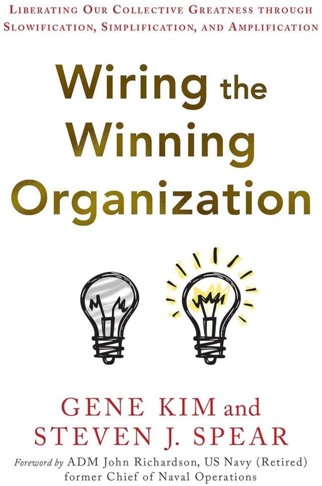
WITH A FOREWORD BY
GENERAL STANLEY McCHRYSTAL, U.S. ARMY (Ret)

ONE MISSION

HOW LEADERS BUILD A TEAM OF TEAMS

Co-author of
NEW YORK TIMES
BESTSELLER *TEAM OF TEAMS*

CHRIS FUSSELL
with C. W. GOODYEAR

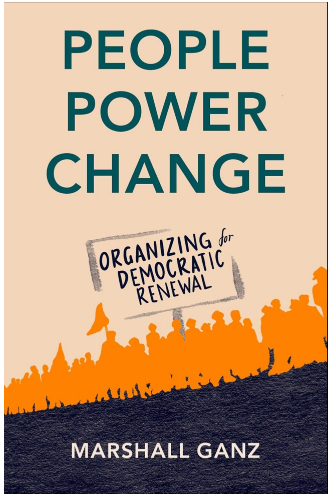


LIBERATING OUR COLLECTIVE GREATNESS THROUGH SLOWIFICATION, SIMPLIFICATION, AND AMPLIFICATION

Wiring the Winning Organization

GENE KIM and
STEVEN J. SPEAR

Foreword by ADM John Richardson, US Navy (Retired)
former Chief of Naval Operations

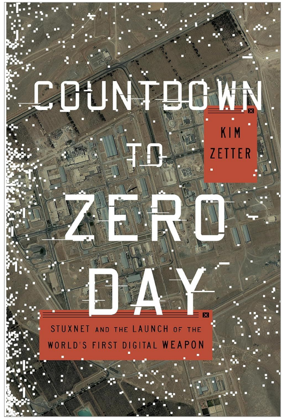


PEOPLE POWER CHANGE

ORGANIZING *for* DEMOCRATIC RENEWAL

MARSHALL GANZ

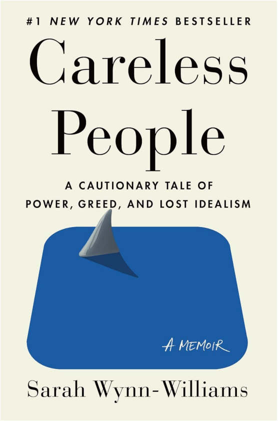
Further Reading on Big Tech, Cyber, and Disinformation



COUNTDOWN TO ZERO DAY

KIM ZETTER

STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON



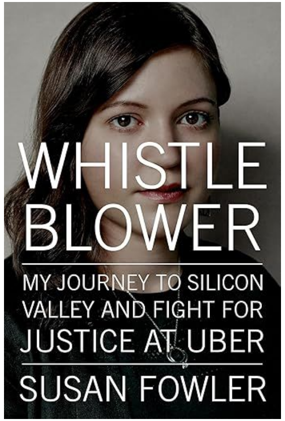
#1 *NEW YORK TIMES* BESTSELLER

Careless People

A CAUTIONARY TALE OF POWER, GREED, AND LOST IDEALISM

A MEMOIR

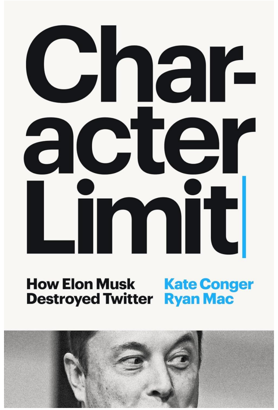
Sarah Wynn-Williams



WHISTLE BLOWER

MY JOURNEY TO SILICON VALLEY AND FIGHT FOR JUSTICE AT UBER

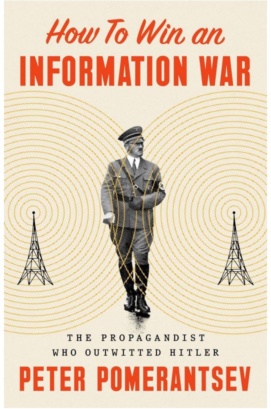
SUSAN FOWLER



Character Limit

How Elon Musk Destroyed Twitter

Kate Conger
Ryan Mac



How To Win an INFORMATION WAR

THE PROPAGANDIST WHO OUTWITTED HITLER

PETER POMERANTSEV