TACTIC
AUTONOMOUS SERVERS

Organized collectives use networked computers and software to provide communications tools directly to their communities and resist spying, exploitation and control of their data by corporations and the state.

CONTRIBUTED BY

May First Movement Technology

May First Movement Technology is a non-profit membership organization that engages in building movements by advancing the strategic use and collective control of technology for local struggles, global transformation, and emancipation without borders.

""DEFENDING THE PRIVACY AND CONTROL OF ONE'S OWN COMMUNICATIONS AND DATA IS A NECESSARY ACT OF DEFIANCE.""

"One of the major components of oppression is to convince you that you don't matter... Telling people about the threat of surveillance is effectively telling them that their information and lives are important to everyone else. That's the power of the struggle against oppression and surveillance."
—Alfredo Lopez

Since the early 90s, activists have increasingly recognized the potential of using the internet as a tool for networked resistance, a space for building community and collective liberation. The internet has helped us share information, organize protests, and build power together in decentralized and horizontal ways.

However, nearly all internet communication has also been captured and controlled by technology corporations bankrolled by surveillance capitalism. These companies mine our personal data for their own profit. Their cooperation with state governments and law enforcement has enabled sophisticated new forms of surveillance to track and target people on an unprecedented scale. New evidence has revealed widespread abuse of the power these platforms hold to directly manipulate the flow of information to people in ways that distort emotional states and public discourse. In this context, defending the privacy and control of one's own communications and data is a necessary act of defiance.

Autonomous servers run by collectives and cooperatives who host their own internet communications tools and services demonstrate a way to actively resist corporate and state efforts to capture, commodify, and control our information. Using virtual servers or

POTENTIAL RISKS

Autonomous servers have been subjected to equipment seizures, legal requests for data, and gag orders by law enforcement. They have been the target of cyber attacks against organizations supporting the reproductive justice movement, Black Lives Matter, and boycott and divestment campaigns protesting the occupation of Palestine. Sufficient planning and preparation is needed to defend against these potential scenarios, protect data, and safeguard the resilience of movement communications.

RELATED TOOLS

Stories

- Battle in Seattle
- CryptoRally in Mexico City
- Occupy Wall Street

Tactics

installing their own hardware in data centres to host free software based web and e-mail services, file sharing, videoconferencing, and other useful tools for online organizing, these projects maintain their own technical infrastructure. This infrastructure forms the basis of a shared territory of resistance.

Each collective brings their own politics and practice to this work. Projects are organized both internationally or within local communities in different countries and languages. For instance, feminist and transfeminist autonomous server projects have emerged to work towards a more gender and culturally diverse presence online.

Originally home to early open publishing sites like those of the Indymedia (IMC) anti-globalization media network, autonomous server projects have provided email services, listserves, and websites for organizing countless movements over the years. They have proven adept at resisting legal requests for user data and provide sanctuary against attempts to censor content that denounces repressive governments and corporations.

These projects are often long-term commitments requiring active participation in collective decision-making processes, user support, documentation, and regular system maintenance. Through fundraising campaigns, membership dues, or other arrangements, these projects find creative ways to sustain their shared infrastructure. Unfortunately the hard work invested in these projects is often invisibilized and participant burnout is a common risk. Successful long-term projects find ways to ensure the collective care of those involved.

Despite the overwhelming popularity of corporate social media platforms, more people are using independently hosted tools and services on autonomous servers than ever before. These projects are essential to the day-to-day organizing activities of social movements worldwide. The good news for the tech layperson: you don't need to build a server from scratch. You can use any number of the tools listed below!

LEARN MORE

May First defends member data
May First Movement Technology
https://support.mayfirst.org/wiki/legal

FBI seizes server
Electronic Frontier Foundation, 2012
https://www.eff.org/deeplinks/2012/04/may-firstriseup-server-seizure-fbi-overreaches-yet-again

Another Network is Possible
April Glaser, Logic Magazine, 2019

- Consumer boycott
- General assembly

Principles

- Create many points of entry
- Practice digital self-defence
- Seize the means of communication
- The price of a successful attack is a constructive alternative

Theories

- Direct action
- Hacking
- The commons

Methodologies

- Power mapping

TAGS

Digital organizing, Digital security, Communications, Direct action, Movement building