# Convocation Research + Design
# Security Services

Convocation Research and Design Labs (CoRD Labs) is an interdisciplinary think tank investigating the intersections of cybersecurity, design, and human rights. We focus on how technology is built, the harms it amplifies, and its impact on marginalized communities.  Our collaborations include the United Nations, Mozilla Foundation, Coalition Against Online Violence, Interledger Foundation, Plan C Pills, Palestine Legal, National Democratic Institute, trust and safety teams at BandCamp, Facebook, and Wikimedia Foundation.

For inquiries or additional information, please contact:

Caroline: caroline@convocation.design
Sam: sam@convocation.design

CONVOCATION
RESEARCH + DESIGN

We work directly with organizations, communities, groups, and individuals to increase online privacy, security, and digital literacy, ensuring safer and positive online experiences. As well as providing rapid response and security training, along with in-depth digital forensics for compromised devices.

Over the past five years, we've worked with over 5000 activists, human rights defenders, civil rights defenders, environmental defenders, political candidates, political dissidents, journalists, social justice organizations, nonprofits, NGOs, and others. As a direct service provider, we offer help ranging from one-on-one  rapid responses for individuals facing online threats such as doxing to large-scale lectures on digital footprint management.

Our privacy and security services cover a broad spectrum of complexity—from accessible solutions that anyone (your grandparents) can implement to advanced security measures requiring expertise in Bash, Python, and Kubernetes. We provide training, workshops, demos, support, direct services, and ongoing care for our clients across multiple disciplines.

## WHAT SETS US APART?

Unlike traditional design firms, CoRD Labs is founded by long-time activists and responsible technology stewards with deep expertise in policy reform, user experience design, user research, and product development. We approach security through a trauma-informed lens, prioritizing the needs of those at the margins first—working inward from there.

## OUR SERVICES & IMPACT

We collaborate with **organizations, communities, and individuals** to enhance online privacy, security, and digital literacy. Our work includes:

- **Direct security support** – From **one-on-one rapid response** for individuals facing online threats (e.g., doxxing) to large-scale training sessions on **digital footprint management**. We have helped over 1000 individuals secure themselves online and offline.
- **Workshops and training** – We provide security workshops tailored for **all skill levels**, from beginner-friendly privacy tools to **advanced security strategies** for sysadmins using Bash, Python, and Kubernetes.
- **Digital security services** – We work with **nonprofits, tech companies, NGOs, and advocacy groups** to build safer digital spaces.
- **Rapid response & crisis intervention** – We have **supported over 5,000 activists, journalists, human rights defenders, and political dissidents** with digital security solutions.

### Previous and Current Clients

Over the past year CoRD Labs has helped dozens of organizations being targeted by bad actors for providing gender affirming care, reproductive services, transgender healthcare, and gender equity in ban states. Additionally we have provided digital security support and privacy consulting to over 1000 individuals engaged in human rights and civil rights activism. Our track record includes providing crucial support to organizations and communities facing digital security challenges across diverse contexts. We've worked closely with organizations working in disaster response, climate change, digital inclusion, and also healthcare providers protecting sensitive patient data, particularly in regions where access to care faces political challenges. Our partnerships have included collaborations with research organizations, civil society, academia, established organizations like Mozilla, and a large nationwide civil rights legal firm, where we've helped strengthen digital security practices and infrastructure. Through these engagements, we've developed and implemented customized security protocols that address each organization's unique needs while building their capacity for long-term resilience.

## CoRD's Security Services

| Service | Description |
|---|---|
| Initial Meeting | Convening crucial meetings to introduce and align all pertinent stakeholders and external parties involved in the workflow and project. |
| Rapid Response | 24/48 hour turn around for those under current or imminent threat. |
| Red Teaming | Our ethical hackers are authorized by your organization to emulate real attackers' tactics, techniques and procedures (TTPs) against your own systems. As well as software security audits, expert help with tackling known security issues, and security architecture and design reviews. |
| Human Rights Documentation and Tracking | We offer Human Rights documentation for: collecting evidence of war crimes internationally, documenting violence against women, and other global human rights violations tracking. |
| Online Harassment Defense | Core to our organizations belief, we provide up to date monitoring of current online targeted harassment tactics implemented by bad actors in order to better explain methods used and how to counter them. |
| Software and Hardware Audit | We recommend the right software/programs/apps for your individual needs as well as the right hardware for the best security that fits your organization or group. |
| Security for Specific Groups | Security specific to human rights activists, civil rights activists, migrants, lawyers, reproductive justice seekers, medical providers, gender affirming care seekers, environmental activists, protesters/activists, politicians, celebrities, public figures, and more. |

| | |
|---|---|
| Website Security Assessment | Broad spectrum analysis of organizations or individuals website security |
| Strategic Security Analysis | In-depth scrutiny of the organizational environment, prevailing conditions, and legal/policy variations relevant to our esteemed clients and their associated cohorts. |
| Organization Security Audit | Conduct security audit of existing client and cohort infrastructures: interview and documentation across the Clear/Dark/Deep Webs. Protect your team from online harassment, fraud, doxing, and social engineering. |
| Organization Security Research and Audit Report | Evaluate procedures/toolchains, identify critical vulnerabilities, make recommendations for implementation, and generate written audit reports. |
| Initial Threat Assessment for Monitoring Scope | A meticulous evaluation of the client and cohort space to identify potential threats and key actors, which will inform the formulation of the proposed monitoring requirements. |
| Dis/Mis/Malinformation | What these topics mean, what they aren't, and how to counter them. |
| Artificial Intelligence and Machine Learning | A general introduction, implementation for organizations and groups, safety, security, and future-proofing. |
| AI Implementation | How to better automate processes, prompt creation, and safer use. |
| AI Safety Consulting | Jailbreaking, red teaming, and future concerns. |
| Secure Communications | We secure your physical communication devices. Everything from office lines, employee cell phones, application based communications, E2EE, mesh networks, radios, and VOIPs. This also includes us physically buying, side loading if needed, securing your new devices, and sending it to you in tamper-proof packaging. |
| Pegasus Diagnosis | Do you or do you not have NSO Group's Pegasus spyware on your device? We will give you a yes or no answer. |
| Spyware and Stalkerware Mitigation and Analysis | Digital forensics is the investigation of malicious software used in an attack. We reverse engineer the attack vector as well as software used. |
| Malicious Program Identification | Do you have spyware, stalkerware, bossware, or malware on your device? Let us take a look at your devices. [Only recommended for those with high threat models] |
| Identity Research | Deep dive into individual client identity exposure and risk online. |
| Vetting Research | Conduct vetting on groups for a variety of concerns, e.g. event attendees, new hires, volunteers, and donors. |
| Organization Monitoring | Conduct research on Client organization and monitor mentions, publications, and chatter across the clear net, dark web, and deep web. |

| | |
|---|---|
| Opposition Intelligence | Conduct opposition research around known and unknown bad actors across the dark, deep, and clear web. Primarily we are using OSINT techniques, but also private and closed sources. Our speciality is a focus on far-right movements, white nationalist movements, christian nationalists movements, identitarian movements, and the broader extremist ecosystems. We search across hundreds of platforms, dozens of dark web sources, hundreds of forums, dozens of message boards, and thousands of websites. |
| Threat Intelligence Research | Conduct research on emergent or past threats in a compressed or extended timeline as well as ongoing monitoring for clients. Our team has access to thousands of websites, image boards, forums, groups, and chats of bad actors to make sure we have who is talking about our clients. |
| Guide Creation | We have written dozens of How To Guides, and often write new ones for clients, organizations, and movements based on a variety of subject expertise. |
| Data Removal Service | We provide a bespoke white glove service for those looking to have their Personal Identifiable Information (PII) removed from the internet. This typically covers 300+ data brokers, a security audit, as well as a 3/6/9/12 month check up. |
| Ransomware Incident Response | We guide clients in the best practices to prevent and protect against ransomware attacks. Monitor and detection. Response and recovery. |
| Trainings and Learning Labs | |
| Digital Security Trainings | We have 101, 201, and 301 trainings on Digital Security. |
| Anti-Doxing Training | We literally wrote the book about anti-doxing, and in the training we cover how to prevent being doxed as well as how to remove PII about you if you have already been doxed. |
| Know Your Rights Trainings | Specific to the client's organization or field of work. |
| Harassment Literacy | What it is, and how to defend against it. |
| Organizational Trainings | Security training for client's internal employees, grantees, or individuals. |
| Secure Border Crossing Training | How to enter and exit countries with hostile privacy laws. This can be catered towards immigrants or citizens. |
| Anti-Phishing Training | Plenty of Pish in the Sea (Everything from Vishing to Social Engineering) |
| Counter-Infiltration Training | This training covers both state and non-state actors infiltration. |
| Physical Security Training | Physical security for offices, homes, apartments, and in person. |

| | |
|---|---|
| Security Culture and OpSec | Broader lifestyle changes to create a more robust security. |
| Privacy Trainings | Becomings more private both online and offline. |
| OSINT Training | Open Source Intelligence gathering, documentation, chain of custody, and analysis training. |