Data and Surveillance in Authoritarian Regimes Training Course

Professional Development Training Course Outline

Category	Political Science and International Relations	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The proliferation of **digital technologies** has fundamentally altered the landscape of **state control**, creating new and unprecedented opportunities for **surveillance** in **authoritarian regimes**. This course delves into the complex and critical intersection of **data science**, **artificial intelligence (AI)**, and **authoritarian governance**. We will explore how modern autocracies leverage everything from facial recognition and social credit systems to sophisticated data analytics and censorship to maintain power, suppress dissent, and shape public behavior. Data and Surveillance in Authoritarian Regimes Training Course is essential for anyone seeking to understand the mechanisms of **digital authoritarianism** and its profound impact on human rights and global security.

This program moves beyond a theoretical understanding to provide a practical, hands-on exploration of the tools, techniques, and **policy frameworks** that enable **data-driven repression**. Participants will analyze real-world case studies to uncover how states exploit big data for **social control**, **predictive policing**, and **online censorship**. Our goal is to equip professionals with the knowledge and skills to identify, analyze, and counter these evolving threats, fostering a more secure and equitable digital future.

Programme Curriculum

Data and Surveillance in Authoritarian Regimes Training Course

Introduction

The proliferation of **digital technologies** has fundamentally altered the landscape of **state control**, creating new and unprecedented opportunities for **surveillance** in **authoritarian regimes**. This course delves into the complex and critical intersection of **data science**, **artificial intelligence (AI)**, and **authoritarian governance**. We will explore how modern autocracies leverage everything from facial recognition and social credit systems

to sophisticated data analytics and censorship to maintain power, suppress dissent, and shape public behavior. Data and Surveillance in Authoritarian Regimes Training Course is essential for anyone seeking to understand the mechanisms of **digital authoritarianism** and its profound impact on human rights and global security.

This program moves beyond a theoretical understanding to provide a practical, hands-on exploration of the tools, techniques, and **policy frameworks** that enable **data-driven repression**. Participants will analyze real-world case studies to uncover how states exploit big data for **social control**, **predictive policing**, and **online censorship**. Our goal is to equip professionals with the knowledge and skills to identify, analyze, and counter these evolving threats, fostering a more secure and equitable digital future.

Course Duration

5 days

Course Objectives

By the end of this course, participants will be able to:

1. Analyze the historical evolution of surveillance from physical methods to digital repression.
2. Evaluate the role of big data and AI in reinforcing authoritarian governance.
3. Identify key data surveillance technologies and their applications in repressive contexts.
4. Assess the ethical and human rights implications of state surveillance.
5. Uncover the use of social credit systems and predictive policing as tools of control.
6. Deconstruct the mechanics of online censorship and information control platforms.
7. Explore the geopolitical implications of exporting digital authoritarianism.
8. Formulate counter-surveillance strategies and digital security protocols.
9. Interpret the legal and policy challenges of data protection in repressive states.
10. Analyze the role of tech companies and international actors in digital repression.
11. Develop an understanding of cybersecurity threats targeting activists and journalists.
12. Examine open-source intelligence (OSINT) techniques for monitoring state surveillance.
13. Anticipate future trends in emerging technologies and their potential for state control.

Target Audience

- Human rights advocates and NGO staff
- Journalists and investigative reporters
- Cybersecurity professionals and data analysts
- Policy makers and government officials
- Researchers and academics
- Tech company employees involved in content moderation or data privacy
- Civil society leaders and activists
- Legal professionals specializing in international law and human rights

Course Outline

Module 1: Foundations of Data-Driven Authoritarianism

- The historical shift from physical to digital surveillance.
- Understanding the surveillance state and its core pillars.
- The role of big data, AI, and cloud computing.
- State capacity and the digital panopticon.
- **Case Study:** The rise of China's "social credit system" and its impact on citizen behavior.

Module 2: Technology & Repression Tools

- Facial recognition, biometric data, and mass surveillance cameras.
- Predictive policing algorithms and their ethical pitfalls.
- Deep packet inspection (DPI) and internet filtering.
- Drone and satellite surveillance.
- **Case Study:** The use of surveillance technology in Xinjiang, China, to monitor and control the Uyghur population.

Module 3: Online Censorship & Information Control

- The Great Firewall of China and other national internet censorship models.
- Social media surveillance and content moderation.
- Disinformation, propaganda, and state-sponsored cyber campaigns.
- Weaponizing information and controlling narratives.
- **Case Study:** Russia's "sovereign internet" and the suppression of online dissent following the 2022 invasion of Ukraine.

Module 4: Global Tech & Corporate Complicity

- The role of international tech companies in enabling or resisting state surveillance.
- Data localization laws and demands for local data storage.
- Ethical sourcing of technology and supply chain transparency.
- Sanctions and export controls on surveillance technology.
- **Case Study:** The complicity of Western tech companies in providing tools and infrastructure to authoritarian governments.

Module 5: Citizen Resistance & Counter-Surveillance

- Digital security best practices for activists and journalists.
- Using virtual private networks (VPNs) and secure messaging apps.
- Strategies for bypassing censorship and accessing blocked content.
- The role of global advocacy and international cooperation.
- **Case Study:** Activists in Hong Kong and Belarus using decentralized networks and secure communications to organize protests.

Module 6: Legal, Ethical & Policy Frameworks

- International human rights law and digital privacy.
- Debates around government access to encrypted data.
- Developing and implementing robust data protection laws.
- The role of UN bodies and international organizations.
- **Case Study:** The legal and ethical battles fought by organizations like the EFF and Amnesty International against state surveillance programs.

Module 7: Emerging Technologies & Future Threats

- Quantum computing and the threat to encryption.
- The use of AI for deepfakes and advanced disinformation.
- The future of data collection from smart cities and IoT devices.
- The intersection of biotech and surveillance.

- **Case Study:** How new AI capabilities could enable even more sophisticated forms of social engineering and psychological manipulation.

Module 8: Practical Application & Simulation

- Hands-on exercises in digital security and threat modeling.
- Group simulations of a state-sponsored cyber-espionage campaign.
- Building a secure communication plan for a sensitive mission.
- A final capstone project where participants analyze a real-world case and propose a counter-strategy.
- **Case Study:** A comprehensive simulation of a journalist in an authoritarian state, from secure communication to data exfiltration.

Training Methodology

This course employs an immersive, multi-modal training approach to ensure a deep and practical understanding of the subject matter. The methodology includes:

- Expert-Led Lectures
- Interactive Workshops.
- Case Study Analysis.
- Policy Simulation.
- Multimedia Resources.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com