The Geopolitics of Data and Information Training Course

Professional Development Training Course Outline

Category	Political Science and International Relations	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid **digital transformation** of our world has ushered in a new era where data and information have become the central currencies of power. The Geopolitics of Data and Information Training Course delves into the intricate and evolving field of the **geopolitics of data**, exploring how the control, flow, and governance of information are fundamentally reshaping international relations, national security, and global economic competition. We'll examine the strategic importance of **data sovereignty**, the impact of **digital authoritarianism**, and the emergence of a multi-polar **techno-geopolitical** landscape. This course is designed to equip professionals with the critical foresight needed to navigate these complex challenges and leverage data as a strategic asset.

In this dynamic global environment, understanding the intersection of technology, data, and power is no longer optional it's essential. From **cyber warfare** and disinformation campaigns to the control of critical **digital infrastructure** and the race for **AI supremacy**, the battle for influence is being fought in the digital realm. This course provides a comprehensive framework to analyze these trends, offering practical insights and methodologies to help you assess **geopolitical risk** and formulate effective strategies. Join us to unlock the secrets of **digital statecraft** and stay ahead in the new global power game.

Programme Curriculum

The Geopolitics of Data and Information Training Course

Introduction

The rapid **digital transformation** of our world has ushered in a new era where data and information have become the central currencies of power. The Geopolitics of Data and Information Training Course delves into the intricate and evolving field of the **geopolitics of data**, exploring how the control, flow, and governance of

information are fundamentally reshaping international relations, national security, and global economic competition. We'll examine the strategic importance of **data sovereignty**, the impact of **digital authoritarianism**, and the emergence of a multi-polar **techno-geopolitical** landscape. This course is designed to equip professionals with the critical foresight needed to navigate these complex challenges and leverage data as a strategic asset.

In this dynamic global environment, understanding the intersection of technology, data, and power is no longer optional it's essential. From **cyber warfare** and disinformation campaigns to the control of critical **digital infrastructure** and the race for **AI supremacy**, the battle for influence is being fought in the digital realm. This course provides a comprehensive framework to analyze these trends, offering practical insights and methodologies to help you assess **geopolitical risk** and formulate effective strategies. Join us to unlock the secrets of **digital statecraft** and stay ahead in the new global power game.

Course Duration

10 days

Course Objectives

- Analyze the strategic **geopolitical implications** of data flows and digital technologies.
- Evaluate the concept of **data sovereignty** and its impact on national policies and international law.
- Assess the role of **critical digital infrastructure** in global power dynamics.
- Examine the use of **data as a weapon** in cyber warfare and information operations.
- Understand the **techno-nationalism** and **digital protectionism** trends shaping global trade.
- Identify emerging threats and opportunities in the **AI arms race**.
- Develop strategies for mitigating **geopolitical risk** related to data governance and privacy.
- Analyze the impact of **surveillance capitalism** on international relations.
- Comprehend the role of international organizations in shaping **global data governance**.
- Examine the influence of **Big Tech** and non-state actors in the digital geopolitical landscape.
- Formulate a cohesive strategy for **data security** and resilience in a fractured world.
- Recognize the ethical and human rights implications of the **geopolitics of data**.
- Predict future trends and scenarios in the evolving **data-driven global order**.

Target Audience

1. **Policy Makers & Government Officials:** Individuals involved in national security, foreign policy, and economic regulation.
2. **Corporate Strategy & Risk Analysts:** Professionals managing business risks and international market strategies.
3. **Legal & Compliance Officers:** Lawyers and compliance experts navigating evolving data regulations.
4. **Journalists & Researchers:** Those reporting on or studying technology, international relations, and security.
5. **Technology Sector Executives:** Leaders in the tech industry, including Big Tech, startups, and telecommunication companies.
6. **Diplomats & International Relations Specialists:** Foreign service officers and diplomats dealing with digital issues.
7. **Cybersecurity Professionals:** Experts focused on national and corporate cybersecurity strategies.
8. **Academics & Think Tank Professionals:** Scholars and analysts researching geopolitics, technology, and governance.

Course Modules

Foundations of Digital Geopolitics

- Defining the core concepts: data as a strategic resource, information as power.
- Historical context: from land-based geopolitics to data-driven statecraft.
- The rise of **digital sovereignty** and **techno-nationalism**.
- Key actors: states, multinational corporations, non-state groups, and individuals.
- The digital divide and its geopolitical consequences.
- **Case Study:** The US-China technological rivalry and its impact on global supply chains for semiconductors and 5G technology.

Data as a Strategic Asset and a Weapon

- Data as a tool for economic power and surveillance capitalism.
- The use of data in intelligence gathering and strategic advantage.
- **Cyber warfare** and its role in modern conflict and competition.
- The weaponization of information: disinformation and propaganda.
- Protecting critical **data infrastructure**.
- **Case Study:** Russia's use of information operations and cyberattacks to influence foreign elections and political discourse.

The New Borders of Information

- Data localization and its policy implications.
- Cross-border data flows and the challenges of a fragmented internet.
- Regulatory fragmentation: the "splinternet" and competing legal frameworks.
- The role of international organizations in setting digital norms.
- The privacy-security trade-off in a connected world.
- **Case Study:** The EU's General Data Protection Regulation (GDPR) and its "Brussels Effect" on global data privacy standards.

Digital Infrastructure as a Geopolitical Battleground

- The strategic importance of undersea cables and satellite networks.
- The race for **5G dominance** and the role of major telecom companies.
- Cloud computing and the concentration of data in a few geographic locations.
- The politics of internet backbones and internet governance.
- Securing critical national digital infrastructure.
- **Case Study:** The Huawei controversy and Western concerns over China's access to and control of critical 5G networks.

The Geopolitics of Artificial Intelligence

- The **AI arms race** and its implications for military and economic power.
- Dual-use technologies and the challenge of export controls.
- Ethical and governance challenges posed by AI.
- The role of AI in surveillance, social control, and predictive analysis.
- The future of AI and the global power balance.
- **Case Study:** China's Social Credit System and the use of big data and AI for large-scale social control and governance.

Data Governance and Human Rights

- The impact of data collection on human rights and civil liberties.
- The rise of **digital authoritarianism** and its tools.
- **Data privacy** as a human right and its global protection.
- The role of non-governmental organizations and civil society in advocating for digital rights.
- Balancing security imperatives with individual freedom.
- **Case Study:** The use of surveillance technology in Xinjiang, China, and the international response to human rights violations.

Corporate Power in the Digital Age

- The geopolitical influence of **Big Tech** companies.
- Navigating different regulatory and market environments.
- Corporate responsibility in a world of conflicting jurisdictions.
- The "platform economy" and its effects on national sovereignty.
- Corporate strategies for managing geopolitical risk.
- **Case Study:** The conflict between Apple and the FBI over iPhone data and the legal and geopolitical fallout.

Economic Geopolitics of Data

- The data economy as a driver of national competitiveness.
- Trade wars and data protectionism.
- Intellectual property rights and technology transfer.
- The role of data in economic sanctions and financial warfare.
- Building national data resilience and competitiveness.
- **Case Study:** The US-China trade war and its expansion to include technological restrictions on data and hardware.

Geopolitical Risk Analysis and Strategic Foresight

- Analytical frameworks for assessing data-related geopolitical risks.
- Scenario planning for a data-driven future.
- Integrating data geopolitics into corporate and national strategy.
- Building resilient organizations in a volatile digital world.
- The role of intelligence and open-source information in risk analysis.
- **Case Study:** Analyzing the potential impact of a major cyberattack on critical infrastructure, using a scenario-planning framework.

Global Data Governance and Norms

- The role of multilateral institutions like the UN and ITU.
- Competing models of global governance: US vs. China vs. EU.
- The debate over a global treaty on data and cyberspace.
- The challenge of regulating emerging technologies like quantum computing.
- The future of international cooperation on data.
- **Case Study:** The United Nations Group of Governmental Experts (UNGGE) on cybersecurity and the challenges of reaching a global consensus on digital norms.

Disinformation and The Digital Public Sphere

- The use of social media and algorithms for political manipulation.

- Identifying and countering disinformation campaigns.
- The role of platforms in content moderation and accountability.
- The impact of deepfakes and generative AI on truth and trust.
- Building a resilient digital public sphere.
- **Case Study:** The impact of social media and disinformation on the 2016 US presidential election and the subsequent public and political response.

The Geopolitics of Surveillance

- The evolution of state and corporate surveillance.
- Technological tools of surveillance: facial recognition, data mining, and location tracking.
- Exporting surveillance technology and its impact on global human rights.
- The battle for encryption and digital privacy.
- Civil society's response to ubiquitous surveillance.
- **Case Study:** The use of Pegasus spyware by governments to surveil journalists and political opponents, and the international outcry.

Data and the Future of Warfare

- The concept of **data-centric warfare**.
- The role of AI and big data in military decision-making and autonomous weapons.
- Cyber deterrence and the challenges of attribution.
- The militarization of space and its connection to data.
- Protecting against attacks on satellite and communication systems.
- **Case Study:** The use of data and AI in the conflict in Ukraine, from intelligence gathering to drone operations.

Geopolitics of Data in Developing Countries

- The challenge of digital colonialism.
- Dependency on foreign digital infrastructure and tech companies.
- The potential for data to drive economic development.
- Balancing foreign investment with digital sovereignty.
- The role of regional blocs in data governance.
- **Case Study:** Africa's position in the global data economy, balancing investment from Western and Chinese companies while trying to develop local digital ecosystems.

Future Outlook and Strategic Implementation

- Anticipating future trends: quantum computing, brain-computer interfaces, and the metaverse.
- Developing a strategic roadmap for data governance.
- Building a resilient and ethical data ecosystem.
- The need for cross-functional and multi-stakeholder collaboration.
- Actionable steps for professionals and organizations.
- **Case Study:** A comprehensive discussion on how a hypothetical government or corporation could implement the lessons from the course to enhance its digital resilience and strategic position.

Training Methodology

- **Instructor-Led Sessions:** Expert-led lectures and presentations on core concepts.

- **Case Study Analysis:** In-depth, guided discussions of real-world examples to apply theoretical knowledge.
- **Scenario-Based Workshops:** Collaborative group exercises to develop strategic foresight and problem-solving skills.
- **Interactive Discussions:** Fostering a dynamic learning environment through Q&A sessions and peer-to-peer knowledge sharing.
- **Multimedia Integration:** Use of videos, infographics, and policy briefs to enhance understanding.

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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