Geopolitics of the Internet and Information 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

Welcome to the digital frontier. In an age of unprecedented connectivity, the **geopolitics of the internet** is no longer a niche topic but a critical field of study impacting international relations, national security, and global economics. This course provides a comprehensive exploration of how technology, data, and information flows are reshaping the global balance of power. We?ÇÖll delve into the complex interplay between states, corporations, and civil society, analyzing the strategic importance of digital infrastructure, cyberspace, and data sovereignty. Participants will gain a nuanced understanding of key concepts, from cyber warfare and information warfare to the rise of digital authoritarianism and the struggle for a free and open internet. Geopolitics of the Internet and Information Training Course is designed to equip you with the knowledge to navigate the complex challenges and opportunities of the digital age.

The course's pedagogical approach emphasizes a blend of theoretical knowledge and practical application. We'll use real-world **case studies** and interactive exercises to illustrate the profound implications of digital policy and technology on global affairs. You'll learn to critically analyze the motivations and strategies of various actors from nation-states to tech giants as they vie for influence in the digital realm. By the end of this training, you'll be able to identify emerging **cybersecurity threats**, understand the legal and ethical dilemmas of digital governance, and contribute to informed discussions on the future of the internet. This training is essential for professionals seeking to stay ahead of the curve in a world where digital power is the new currency.

Programme Curriculum

Geopolitics of the Internet and Information Training Course

Introduction

Welcome to the digital frontier. In an age of unprecedented connectivity, the **geopolitics of the internet** is no longer a niche topic but a critical field of study impacting international relations, national security, and global economics. This course provides a comprehensive exploration of how technology, data, and information flows are reshaping the global balance of power. We?ÇÖll delve into the complex interplay between states, corporations, and civil society, analyzing the strategic importance of digital infrastructure, cyberspace, and data sovereignty. Participants will gain a nuanced understanding of key concepts, from cyber warfare and information warfare to the rise of digital authoritarianism and the struggle for a free and open internet. Geopolitics of the Internet and Information Training Course is designed to equip you with the knowledge to navigate the complex challenges and opportunities of the digital age.

The course's pedagogical approach emphasizes a blend of theoretical knowledge and practical application. We'll use real-world **case studies** and interactive exercises to illustrate the profound implications of digital policy and technology on global affairs. You'll learn to critically analyze the motivations and strategies of various actors from nation-states to tech giants as they vie for influence in the digital realm. By the end of this training, you'll be able to identify emerging **cybersecurity threats**, understand the legal and ethical dilemmas of digital governance, and contribute to informed discussions on the future of the internet. This training is essential for professionals seeking to stay ahead of the curve in a world where digital power is the new currency.

Course Duration

5 days

Course Objectives

- Understand the foundational concepts of **cyber geopolitics** and their historical context.
- Analyze the role of **digital infrastructure** (e.g., submarine cables, data centers) as strategic assets.
- Evaluate the impact of **cyber warfare** and state-sponsored hacking on international security.
- Explore the dynamics of **information warfare** and the spread of disinformation and misinformation.
- Critically assess the concept of **digital sovereignty** and its implications for nation-states.
- Examine the role of major technology companies as powerful geopolitical actors.
- Differentiate between different **internet governance** models
- Analyze the legal and regulatory frameworks for **data governance** and privacy protection.
- Identify and mitigate key **cybersecurity threats** to critical infrastructure.
- Investigate the use of social media and online platforms for political influence and activism.
- Understand the challenges of **digital divide** and its geopolitical consequences.
- Develop strategies for effective **digital diplomacy** and international cooperation.
- Forecast future trends in the **geopolitics of AI** and emerging technologies.

Target Audience

- **Government officials** and policy advisors working on digital affairs.
- **International relations** and foreign policy specialists.
- **Cybersecurity professionals** and risk analysts.
- **Journalists** and researchers covering technology and politics.
- **Legal experts** specializing in internet law and data privacy.
- **Academics** and students in political science, media studies, and sociology.
- **Corporate strategists** from technology companies and multinational corporations.
- **NGOs** and civil society advocates focused on digital rights.

Course Outline

Module 1: Foundations of Cyber Geopolitics

- Defining the digital domain as a new sphere of geopolitical competition.
- The history of internet governance: from technocratic control to a multistakeholder model.
- Key actors in the digital realm: states, tech giants, and civil society.
- The concept of **digital divide** and its economic and political implications.
- **Case Study:** The battle over control of ICANN and global internet naming conventions.

Module 2: Strategic Digital Infrastructure

- The strategic importance of undersea **fiber optic cables** and satellites.
- **Data centers** and cloud infrastructure as national assets.
- The politics of **telecommunications networks**, particularly 5G technology.
- Supply chain security and the dependency on a few key technology manufacturers.
- **Case Study:** The U.S.-China rivalry over Huawei and the global rollout of 5G.

Module 3: Cybersecurity and Digital Conflict

- **Cyber warfare**: understanding state-sponsored hacking and its objectives.
- The challenges of **attribution** in cyberspace and the "fog of war."
- Protecting **critical national infrastructure** from cyberattacks.
- The role of non-state actors in cyber conflicts.
- **Case Study:** The Stuxnet attack on Iran's nuclear program and its implications for digital warfare.

Module 4: The New Information Warfare

- The weaponization of information: disinformation, misinformation, and propaganda.
- The mechanics of foreign interference in democratic processes.
- Social media platforms as tools for political manipulation.
- **Cognitive security**: protecting a society's shared reality from digital threats.
- **Case Study:** Russia's influence operations during the 2016 U.S. presidential election.

Module 5: Digital Sovereignty and Governance

- Defining and evaluating different approaches to **digital sovereignty**.
- **Data localization** laws and their impact on global tech companies.
- The "Great Firewall of China" and other models of state-controlled internet.
- The EU's **GDPR** as a model for regulatory power projection.
- **Case Study:** The European Union's regulatory challenges against U.S. tech giants, focusing on data privacy.

Module 6: Big Tech as Geopolitical Actors

- The immense power of tech companies in shaping global norms and policies.
- **Platform diplomacy**: the role of social media platforms in international relations.
- Antitrust and regulatory battles as a form of state-corporate conflict.
- The ethical responsibilities and dilemmas of tech companies.
- **Case Study:** The dispute between Australia and Facebook over news content payments.

Module 7: The Geopolitics of AI and Emerging Tech

- The race for **AI supremacy** between major powers.

- The strategic implications of **quantum computing** and **biometrics**.
- The use of AI for surveillance and social control.
- Ethical and regulatory challenges in governing AI on a global scale.
- **Case Study:** The development and deployment of facial recognition technology in public spaces in China and the West.

Module 8: The Future of the Digital World

- Scenarios for the future of the internet: fragmentation vs. cooperation.
- Building resilient and secure digital societies.
- The role of **digital diplomacy** and international cooperation.
- The balance between security and civil liberties in the digital age.
- **Case Study:** The UN-led Global Digital Compact and the ongoing debate over internet governance.

Training Methodology

This program utilizes a **blended learning approach** combining interactive lectures, group discussions, and hands-on exercises.

- **Interactive Lectures:** Led by experts, these sessions will provide foundational knowledge and context.
- **Case Study Analysis:** Participants will work in groups to dissect real-world examples, applying theoretical concepts to practical situations.
- **Simulations and Role-Playing:** Engaging in mock negotiations and scenario planning to practice **digital diplomacy** and crisis management.
- **Peer-to-Peer Learning:** Fostering a collaborative environment where participants share insights and experiences.
- **Online Resources:** Access to a curated library of academic articles, policy reports, and multimedia content.

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