Cybersecurity and Geopolitics 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

In today's interconnected world, the lines between **cybersecurity** and **geopolitical stability** are increasingly blurred. Nation-states, non-state actors, and cybercriminal syndicates are leveraging digital tools to conduct espionage, disrupt critical infrastructure, and influence political processes. This convergence creates a complex and dynamic threat landscape that demands a new kind of expertise one that bridges the gap between technical cybersecurity knowledge and an understanding of international relations. Cybersecurity and Geopolitics Training Course will provide a comprehensive, actionable framework to analyze and navigate these **complex threats**, equipping professionals with the strategic foresight necessary to protect their organizations and national interests in the digital age.

The digital domain has become the new frontier of global power competition. From **cyber warfare** and **digital sovereignty** to the protection of **critical infrastructure**, the interplay between technology and diplomacy has profound implications for national security, economic stability, and international law. This training is designed to move beyond traditional IT security, focusing on the strategic and policy dimensions of cyber threats. By examining real-world **case studies** of state-sponsored attacks, supply chain vulnerabilities, and the weaponization of information, participants will develop the skills to assess **geopolitical risk**, formulate robust **cyber defense strategies**, and contribute to global efforts for a more secure and stable cyberspace.

Programme Curriculum

Cybersecurity and Geopolitics Training Course

Introduction

In today's interconnected world, the lines between **cybersecurity** and **geopolitical stability** are increasingly blurred. Nation-states, non-state actors, and cybercriminal syndicates are leveraging digital tools to conduct

espionage, disrupt critical infrastructure, and influence political processes. This convergence creates a complex and dynamic threat landscape that demands a new kind of expertise one that bridges the gap between technical cybersecurity knowledge and an understanding of international relations. Cybersecurity and Geopolitics Training Course will provide a comprehensive, actionable framework to analyze and navigate these **complex threats**, equipping professionals with the strategic foresight necessary to protect their organizations and national interests in the digital age.

The digital domain has become the new frontier of global power competition. From **cyber warfare** and **digital sovereignty** to the protection of **critical infrastructure**, the interplay between technology and diplomacy has profound implications for national security, economic stability, and international law. This training is designed to move beyond traditional IT security, focusing on the strategic and policy dimensions of cyber threats. By examining real-world **case studies** of state-sponsored attacks, supply chain vulnerabilities, and the weaponization of information, participants will develop the skills to assess **geopolitical risk**, formulate robust **cyber defense strategies**, and contribute to global efforts for a more secure and stable cyberspace.

Course Duration

5 days

Course Objectives

1. Analyze the **geopolitical landscape** and its impact on the **cyber threat environment**.
2. Identify and profile various **state-sponsored threat actors** and their motivations.
3. Understand the principles of **digital sovereignty** and **cyber deterrence**.
4. Assess and mitigate risks to **critical infrastructure protection** (CIP).
5. Explore the role of **AI and machine learning** in both cyberattacks and cyber defense.
6. Formulate effective **incident response** plans for geopolitically motivated attacks.
7. Deconstruct **cyber warfare** doctrines and international law in cyberspace.
8. Recognize and counter **disinformation campaigns** and foreign influence operations.
9. Develop a **zero trust security model** tailored for global organizations.
10. Evaluate the security implications of **supply chain vulnerabilities**.
11. Implement strategies for **cyber resilience** and business continuity.
12. Navigate international **cybersecurity policy** and **regulatory compliance**.
13. Apply **threat intelligence** to proactively identify and prepare for emerging geopolitical cyber risks.

Target Audience

1. Cybersecurity Professionals.
2. Risk Management Specialists.
3. Government & Policy Analysts.
4. Corporate Executives & C-Suite.
5. IT & Network Administrators.
6. Diplomats & International Relations Experts.
7. Legal & Compliance Officers
8. Military Personnel.

Course Outline

Module 1: The Geopolitical Cyber Battlefield

- Defining the cyber-geopolitical nexus.

- Identifying key state and non-state actors.
- Understanding national security interests in cyberspace.
- Case Study: The Stuxnet attack on Iran's nuclear program, analyzing state-sponsored sabotage.
- **Case Study:** The **SolarWinds** hack, exploring the sophistication and geopolitical motives behind supply chain attacks.

Module 2: Critical Infrastructure & National Security

- Mapping and protecting critical national infrastructure (CIP).
- Examining the vulnerabilities of energy grids, financial systems, and telecommunications.
- Developing cyber-physical security strategies.
- Case Study: The 2015 and 2016 attacks on Ukraine?ÇÖs power grid, demonstrating the real-world impact of cyberattacks on essential services.
- **Case Study:** The Colonial Pipeline ransomware attack, illustrating the disruptive power of attacks on private infrastructure.

Module 3: Information Warfare & Digital Influence

- Techniques of **disinformation**, misinformation, and propaganda.
- The role of social media platforms in foreign influence operations.
- Countering malign influence and building information resilience.
- Case Study: The Russian Internet Research Agency's (IRA) influence campaign during the 2016 US election.
- **Case Study:** The **"Ghostwriter"** campaign, revealing a coordinated effort to spread false narratives and manipulate public perception.

Module 4: Cyber Deterrence & International Law

- Exploring doctrines of cyber deterrence and attribution.
- Analyzing the applicability of international law to cyberspace (e.g., the Law of Armed Conflict).
- The role of international norms and treaties.
- Case Study: The NotPetya attack and the challenges of international attribution and response.
- **Case Study:** Ongoing debates at the UN on establishing norms of responsible state behavior in cyberspace.

Module 5: Digital Sovereignty & Policy

- Defining **digital sovereignty** and its implications for data governance.
- Analyzing key cybersecurity policies and regulations (e.g., GDPR, NIS 2 Directive).
- Navigating the fragmentation of the global internet.
- **Case Study:** The US-China tech rivalry, focusing on Huawei and the debate over 5G security.
- **Case Study:** India's data localization policies and their impact on global tech companies.

Module 6: Supply Chain & Third-Party Risk

- Identifying and managing risks in complex global supply chains.
- Vetting vendors, partners, and open-source software.
- Implementing best practices for supply chain security.
- Case Study: The WannaCry ransomware attack, tracing the spread of malware through unpatched systems.
- **Case Study:** The compromised dependencies in open-source software like **Log4j**.

Module 7: Emerging Threats & Strategic Foresight

- The future of cyberattacks with **AI-powered threats**.
- Securing the **Internet of Things (IoT)** and smart city infrastructure.
- The cybersecurity challenges of **quantum computing** and post-quantum cryptography.
- Case Study: The use of AI in deepfake creation for sophisticated social engineering attacks.
- **Case Study:** Securing the **connected car** ecosystem from nation-state threats.

Module 8: Cyber Resilience & Incident Response

- Building a **cyber resilience** framework.
- Developing an effective **incident response plan** for high-stakes incidents.
- Post-incident analysis and lessons learned.
- Case Study: The response to the Maersk cyberattack, showcasing operational recovery and business continuity in a global crisis.
- **Case Study:** The **Target** data breach, examining the breakdown of security protocols and third-party risk management.

Training Methodology

This course employs a **blended learning** approach to ensure comprehensive knowledge transfer and practical skill development.

- **Instructor-Led Sessions:** Expert-led live lectures with interactive Q&A.
- **Interactive Workshops:** Collaborative problem-solving exercises in a virtual or in-person setting.
- **Real-World Case Studies:** In-depth analysis of major cyber incidents to illustrate theoretical concepts.
- **Simulations & Scenarios:** Hands-on exercises to apply learned skills in a realistic, risk-free environment.
- **Peer-to-Peer Learning:** Group discussions and knowledge sharing among participants.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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