Cybersecurity Policy and International Law 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 **hyper-connected** digital landscape, **cybersecurity threats** have become a critical concern for governments, organizations, and individuals worldwide. The proliferation of digital technologies and the increasing reliance on online systems have exposed critical **infrastructures** to a wide range of cyber threats, from sophisticated **nation-state attacks** and **cyber warfare** to **ransomware attacks** and **data breaches**. A proactive and robust approach to cybersecurity requires a comprehensive understanding of not only the technical aspects of security but also the complex legal and policy frameworks that govern digital space.

Cybersecurity Policy and International Law Training Course addresses this critical need. It is designed to equip professionals with the knowledge and skills to navigate the intricate intersection of technology, law, and policy. Participants will delve into the core principles of **cybersecurity governance**, explore the legal dimensions of **cybercrime**, and analyze the evolving landscape of **international cyber law**. Through a blend of theoretical knowledge and practical application, this course will empower you to develop and implement effective **cybersecurity strategies** that comply with both domestic and global legal standards, ensuring **digital resilience** and protecting national and organizational interests in the face of escalating **cyber threats**.

Programme Curriculum

Cybersecurity Policy and International Law Training Course

Introduction

In today's **hyper-connected** digital landscape, **cybersecurity threats** have become a critical concern for governments, organizations, and individuals worldwide. The proliferation of digital technologies and the

increasing reliance on online systems have exposed critical **infrastructures** to a wide range of cyber threats, from sophisticated **nation-state attacks** and **cyber warfare** to **ransomware attacks** and **data breaches**. A proactive and robust approach to cybersecurity requires a comprehensive understanding of not only the technical aspects of security but also the complex legal and policy frameworks that govern digital space.

Cybersecurity Policy and International Law Training Course addresses this critical need. It is designed to equip professionals with the knowledge and skills to navigate the intricate intersection of technology, law, and policy. Participants will delve into the core principles of **cybersecurity governance**, explore the legal dimensions of **cybercrime**, and analyze the evolving landscape of **international cyber law**. Through a blend of theoretical knowledge and practical application, this course will empower you to develop and implement effective **cybersecurity strategies** that comply with both domestic and global legal standards, ensuring **digital resilience** and protecting national and organizational interests in the face of escalating **cyber threats**.

Course Duration

5 days

Course Objectives

This course aims to empower participants to:

1. Analyze global **cybersecurity frameworks** and **international law** applications.
2. Assess the legal implications of **emerging technologies** like AI and blockchain.
3. Develop robust **cybercrime legislation** and policy recommendations.
4. Master the principles of **digital forensics** and **evidence handling** in cross-border investigations.
5. Formulate effective **incident response plans** aligned with legal requirements.
6. Understand and ensure compliance with global **data privacy** regulations like GDPR and CCPA.
7. Analyze the role of **nation-states** and **non-state actors** in cyber conflict.
8. Design and implement **critical infrastructure protection** strategies.
9. Evaluate **cybersecurity governance** structures for public and private sectors.
10. Navigate the complex legal challenges of **cyber espionage** and attribution.
11. Strengthen **international cooperation** mechanisms for combating cyber threats.
12. Cultivate a culture of **cyber resilience** through policy and awareness.
13. Address the ethical and legal challenges of **cyber surveillance** and intelligence.

Target Audience

- Policymakers and Government Officials
- Legal Professionals and Corporate Lawyers
- Cybersecurity Analysts and IT Managers
- Law Enforcement and Intelligence Professionals
- Compliance Officers and Risk Managers
- Military and Defense Personnel
- Academics and Researchers
- Executives and Senior Management

Course Outline

Module 1: Foundations of Cybersecurity Policy & Law

- Understanding the **cybersecurity ecosystem**.
- Core legal principles: sovereignty, jurisdiction, and due diligence.

- Policy vs. legal frameworks.
- The role of national governments and international bodies.
- **Case Study:** The **Estonia Cyberattacks** and their impact on national cyber defense policy.

Module 2: International Law and Cyber Conflict

- Application of the **UN Charter** and the laws of armed conflict to cyberspace.
- Principles of **necessity** and **proportionality** in cyber operations.
- Distinction between cybercrime and cyber warfare.
- Legal challenges of **cyber espionage** and attribution.
- **Case Study:** The **NotPetya** attack and its classification as an act of war.

Module 3: Cybercrime and Digital Evidence

- Classification of cybercrimes: from DDoS to ransomware.
- The **Budapest Convention on Cybercrime** and its global impact.
- Legal procedures for **digital evidence collection** and preservation.
- Challenges of jurisdictional issues in cross-border investigations.
- **Case Study: Operation Pacifier**, a global takedown of child abuse material and its lessons on international legal cooperation.

Module 4: Data Privacy and Regulatory Compliance

- Deep dive into **GDPR**, **CCPA**, and other data protection regulations.
- Defining and protecting **Personally Identifiable Information (PII)**.
- The legal requirements for **data breach notifications**.
- Privacy by Design and the principle of data minimization.
- **Case Study:** The **Capital One Data Breach** and the legal fallout of a massive data exposure.

Module 5: Critical Infrastructure and National Security

- Legal frameworks for protecting **Critical Information Infrastructure (CII)**.
- Public-private partnerships in national cybersecurity strategies.
- Regulation and policy for industrial control systems (ICS) and SCADA networks.
- Addressing **supply chain vulnerabilities**.
- **Case Study:** The **Colonial Pipeline Ransomware Attack** and the policy response to critical infrastructure threats.

Module 6: Emerging Technologies and Legal Challenges

- The legal and ethical implications of **AI in cybersecurity**.
- Policy frameworks for **IoT security**.
- Blockchain's role in security and its legal challenges.
- Regulation of **crypto-jacking** and cyber currency.
- **Case Study:** The use of **facial recognition technology** in public spaces and the subsequent privacy and civil liberty debates.

Module 7: Incident Response and Threat Intelligence

- Developing legally compliant **incident response protocols**.
- Legal roles and responsibilities during a cyber incident.
- Integrating **threat intelligence** into policy and decision-making.

- Communication and reporting requirements for cyberattacks.
- **Case Study:** The **SolarWinds attack** and the policy challenges of responding to a large-scale supply chain compromise.

Module 8: Policy Development and Implementation

- **Stakeholder engagement** and policy formulation.
- Drafting and implementing effective **cybersecurity policies**.
- Creating internal governance and **risk management frameworks**.
- Auditing and continuously improving cybersecurity policy.
- **Case Study:** The **Yahoo Data Breach** and the lessons in corporate governance, policy, and legal liability.

Training Methodology

This course employs a **blended learning methodology** to ensure comprehensive knowledge transfer and skill development. It combines:

- **Interactive Lectures** and facilitated discussions led by industry experts and legal practitioners.
- **Scenario-Based Simulations** where participants work in groups to respond to simulated cyber incidents.
- **Case Study Analysis** of real-world cyberattacks to understand the interplay of technology, law, and policy.
- **Hands-on Policy Drafting Labs** where participants develop and refine policy documents.
- **Role-Playing Exercises** to practice negotiation and communication in legal and diplomatic contexts.
- **Peer-to-Peer Learning** and networking opportunities to build professional relationships.

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