Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

DEFENSE AND SECURITY

National Cyber Security Strategy Development Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

- **DURATION**
  5 Days Practical Hands-on
- **DELIVERY MODES**
  In-Person Class & Live Virtual
- **CERTIFICATION**
  Accredited Certificate of Completion
- **INTAKES / DATES**
  Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 21, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE

P.O. Box 102802-00101, Nairobi, Kenya

Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy

Tel: +254 724 527 104 | +254 734 969 612

Email: training@datastatresearch.org

www.datastatresearch.org

National Cyber Security Strategy Development Training Course

Defense and Security • 5 Days Intensive • Accredited Certification

Course Overview

National Cyber Security Strategy Development Training Course equips participants with practical tools, methodologies, and strategic frameworks required to develop, implement, and maintain national cyber security strategies aligned with global best practices.

Key Skills & Software Tools Covered

MS Word • Cyberbit Range • IBM QRadar • and MITRE ATT&CK Navigator

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
29 Dec 2025 – 2 Jan 2026	Bangkok	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Accra	Classroom / 5d	**$4,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
29 Dec 2025 – 2 Jan 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Cape Town	Classroom / 5d	**$4,500 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Addis Ababa	Classroom / 5d	**$3,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Singapore	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Istanbul	Classroom / 5d	**$5,000 USD / KES 90,000**
5 Jan 2026 – 9 Jan 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
5 Jan 2026 – 9 Jan 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 90,000**
5 Jan 2026 – 9 Jan 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 90,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

National Cyber Security Strategy Development Training Course

Introduction

National cyber security strategies have become essential in an era defined by escalating cyber threats, digital transformation, and increasing geopolitical tension across cyberspace. Governments, regulators, and critical national institutions must develop coordinated and robust cyber security strategies that integrate risk assessment, governance frameworks, threat intelligence, incident response, capacity building, and public-private collaboration. National Cyber Security Strategy Development Training Course equips participants with practical tools, methodologies, and strategic frameworks required to develop, implement, and maintain national cyber security strategies aligned with global best practices.

The course emphasizes real-world cyber risk analysis, digital resilience planning, regulatory harmonization, and strategic policy formulation. Participants will gain advanced skills in designing national cyber security architectures, coordinating national CERT functions, addressing emerging technologies, and fostering international cooperation. Through structured modules, simulations, and case studies, this course empowers leaders to build resilient and adaptive national cyber security ecosystems capable of safeguarding critical digital infrastructure and ensuring national cybersecurity readiness.

Course Objectives

- Understand the core components of national cyber security strategy development.
- Analyse global cyber security frameworks and apply them to national contexts.
- Conduct comprehensive cyber risk assessments for national infrastructure.
- Design governance structures and policy frameworks for national cyber security.
- Strengthen national cyber resilience through threat intelligence integration.
- Develop and coordinate national-level incident response capabilities.
- Integrate cyber capacity-building programs into national planning.
- Evaluate legal, regulatory, and compliance requirements for cyber readiness.
- Address security risks related to emerging and disruptive technologies.
- Foster multi-stakeholder collaboration among public, private, and civil sectors.
- Develop national awareness, training, and cyber hygiene programs.
- Formulate monitoring, review, and continuous improvement mechanisms.
- Align national cyber strategy with regional and international security frameworks.

Organizational Benefits

- Enhanced national cyber resilience and preparedness
- Strengthened capacity to prevent and respond to cyber threats
- Improved coordination between national cybersecurity stakeholders
- Increased compliance with global and regional security frameworks
- Better protection of critical national infrastructure
- Reduced risks of cyber espionage, attacks, and data breaches
- Improved public trust in digital government services
- Strengthened interagency and cross-sector collaboration
- Enhanced strategic decision-making at national leadership levels
- Long-term development of national cybersecurity capabilities

Target Audiences

- National security policymakers
- Cybersecurity regulators and government ICT officials
- National CERT and CSIRT leadership teams
- Defence and intelligence agencies
- Critical infrastructure security managers
- Digital government transformation teams
- Cybersecurity consultants and advisors
- International security and development partners

Course Duration: 5 days

Course Modules

Module 1: Foundations of National Cyber Security Strategy

- Understand the purpose, scope and structure of national cyber strategies
- Review global cyber security trends and national threat landscapes
- Define strategic objectives, vision and priority areas
- Identify national cybersecurity stakeholders and governance structures
- Analyse key challenges in developing coordinated national strategies
- Case Study: National cyber strategy transformation in a developing nation

Module 2: Cyber Risk Assessment & National Threat Profiling

- Conduct cyber risk assessments for critical sectors
- Map threat actors, motivations and attack vectors
- Evaluate national vulnerabilities and systemic risks
- Use cyber risk scoring frameworks to inform strategy design
- Integrate risk insights into national planning processes
- Case Study: National cyber risk assessment for critical energy infrastructure

Module 3: National Cyber Governance & Policy Frameworks

- Establish national governance mechanisms for cyber security
- Define institutional roles, mandates and coordination pathways
- Align cyber policies with legal and regulatory frameworks
- Develop national security policies for data, networks and systems
- Implement interagency mechanisms for strategic coordination
- Case Study: Governance restructuring following a national cyber incident

Module 4: National Incident Response & Crisis Management

- Build national-level incident response structures
- Coordinate CERT/CSIRT functions and reporting frameworks
- Create escalation pathways for cyber crisis management
- Strengthen communication between government and private sector
- Develop national cyber contingency and continuity plans
- Case Study: National response to a coordinated cyber attack

Module 5: Cyber Capacity Building & Workforce Development

- Assess national cyber skills gaps and workforce needs
- Develop training, certification and talent development programs
- Strengthen collaboration with universities and global partners
- Promote cyber hygiene and national awareness campaigns
- Build long-term national cybersecurity capacity plans
- Case Study: National cybersecurity workforce development strategy

Module 6: Legal, Regulatory & Compliance Requirements

- Analyse national cybersecurity legislation frameworks
- Review data protection, digital identity, and ICT laws
- Strengthen regulatory alignment across sectors
- Develop compliance and enforcement mechanisms
- Integrate regulatory requirements into national cybersecurity plans
- Case Study: Regulatory overhaul after critical data breach

Module 7: Securing Emerging Technologies

- Identify risks posed by AI, IoT, cloud, 5G and automation
- Integrate emerging technology security into national planning
- Build frameworks for innovation-friendly cybersecurity
- Strengthen oversight and certification for emerging technologies
- Monitor global emerging tech security standards
- Case Study: Integrating 5G risk mitigation into national strategy

Module 8: International Cooperation & Cyber Diplomacy

- Strengthen participation in regional and global cyber agreements
- Coordinate with international partners on threat intelligence
- Engage in cyber diplomacy and global policy dialogues
- Enhance cross-border cybercrime collaboration
- Align national strategy with global defence and security networks
- Case Study: International cooperation during cross-border cyber investigation

Training Methodology

- Interactive instructor-led presentations
- Group activities and national-level scenario exercises
- Case study analysis covering global cyber incidents
- Practical tools and templates for strategy drafting

- Peer learning discussions and collaborative workshops
- Guided development of a draft national cyber security strategy

Register as a group from 3 participants for a Discount

Send us an email: info@datastatresearch.org or call +254724527104

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 DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/national-cyber-security-strategy-development-training-course to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.