

No. 101

CYBERSECURITY

Geopolitical Cyber Risk

How global tensions shape cyber threats, and how organizations prepare

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 101

Geopolitical Cyber Risk

How global tensions shape cyber threats, and how organizations prepare

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Geopolitical Cyber Risk

How global tensions shape cyber threats, and how organizations prepare

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product and company names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · THE LANDSCAPE

1 Why states operate in cyberspace 5
2 Geopolitics and cyber by the numbers 7
3 The actors 9
4 Landmark events 11
5 Collateral damage 13
6 Why smaller organizations should care 15

PART II · FORMS OF RISK

7 Espionage 17
8 Pre-positioning 18
9 Disruption and destruction 19
10 Hybrid threats 20
11 State-linked crime 22
12 Influence operations and hack-and-leak 23

PART III · ASSESSING YOUR EXPOSURE

13 Assessing exposure 26
14 Threat intelligence 28
15 Geopolitical triggers 30
16 Scenario planning 32
17 Supply chain and technology dependence 33
18 Concentration risk 34

PART IV · BUILDING RESILIENCE

19 Technical resilience 36
20 Business continuity 38
21 People and travel 39
22 Communications and disinformation 41

FREE SAMPLE · ojayo.com

23 Norms, law and response 42
24 Regulation 43
25 A geopolitical cyber programme 44
26 Briefing the board 45
Checklists 46
Glossary 47
Further reading 48

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Cyberspace has become a major arena of competition between states. Governments use cyber operations to spy, to prepare for possible conflict, to disrupt opponents and, in some cases, to steal money. Organizations with no political role can be caught in the crossfire, through shared software, suppliers, infrastructure or simply because of the sector or country they operate in.

Geopolitical cyber risk is the risk that international tensions, conflicts and policies create cyber threats or disruption for an organization. This book explains, for beginners, how states and their proxies operate, what landmark events teach us, and how organizations can assess their exposure and build resilience. It is written in a neutral, practical way and does not take sides in any conflict.

What this book covers

- Why states operate in cyberspace, and the actors involved.
- Landmark events, collateral damage and hybrid threats.
- How to assess your organization's exposure.
- Threat intelligence, triggers and scenario planning.
- Resilience, supply chain diversity, travel security and continuity.
- International norms, sanctions and regulation.

Who this book is for

- **Security and risk professionals** advising leadership.
- **Executives and board members** responsible for risk.

FREE SAMPLE · ojayo.com

- **IT staff** in organizations operating internationally.

How the book is organized

- **Part I — The landscape** (Chapters 1–6): why states use cyber, the numbers, the actors, landmark events, collateral damage, and why smaller organizations should care.
- **Part II — Forms of risk** (Chapters 7–12): espionage, pre-positioning, disruption, hybrid threats, state-linked crime, and influence operations.
- **Part III — Assessing your exposure** (Chapters 13–18): exposure factors, threat intelligence, geopolitical triggers, scenario planning, the supply chain, and concentration risk.
- **Part IV — Building resilience** (Chapters 19–26): technical resilience, continuity, people and travel, communications, norms and law, regulation, a programme, and briefing the board.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in a real organization.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on attribution and screens

Attributions in this book follow public statements by governments and established security firms; attribution is difficult and sometimes disputed. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

The landscape

These chapters explain why states operate in cyberspace, who the actors are, what major events have taught us, and how ordinary organizations get caught up.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why states operate in cyberspace

States use cyber operations to pursue national goals.

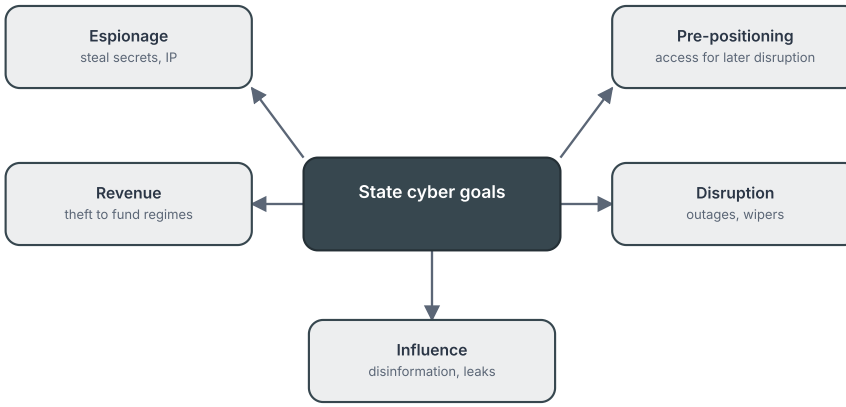


Figure 1.1 Why states operate in cyberspace

Cheap, deniable and remote

Cyber operations are relatively cheap, can be carried out from far away and are hard to attribute with certainty. That makes them attractive tools of statecraft below the threshold of open war.

Main goals

- **Espionage**: political, military and commercial secrets.
- **Pre-positioning**: hidden access to infrastructure that could be used for disruption later.

FREE SAMPLE · ojayo.com

- **Disruption and destruction**: outages and data wiping, especially during conflicts.
- **Influence**: hacking and leaking, and spreading disinformation.
- **Revenue**: some states steal money, especially cryptocurrency, to fund programmes and evade sanctions.

KEY IDEA

For states, cyber is one tool among many: diplomatic, economic, military and informational.

FREE SAMPLE · ojayo.com

CHAPTER 2

Geopolitics and cyber by the numbers

Organizations increasingly plan for geopolitically motivated attacks.

Finding	Source
64% of organizations account for geopolitically motivated attacks	WEF Global Cybersecurity Outlook 2026
91% of the largest organizations changed strategy due to geopolitics	WEF Global Cybersecurity Outlook 2026
31% have low confidence in national incident response, up from 26%	WEF Global Cybersecurity Outlook 2026
23% of public-sector bodies report insufficient resilience	WEF Global Cybersecurity Outlook 2026

Figure 2.1 Geopolitics and cyber by the numbers

The WEF view

The World Economic Forum's Global Cybersecurity Outlook 2026, based on a survey of leaders worldwide, found geopolitics remained the most influential factor in cyber risk strategies. Nearly two-thirds of organizations said they account for geopolitically motivated attacks, and 91% of the largest organizations had changed their cybersecurity strategies because of geopolitical volatility.

Confidence is falling

Almost a third of respondents reported low confidence in their country's ability to respond to major cyber incidents, up from the previous year, and nearly a quarter of public-sector organizations said their resilience was insufficient.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk (you are reading this)
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Geopolitical Cyber Risk

Enjoyed it? The full book has 53 pages and 26 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.