

Navigating Beyond Quantum

Building trusted, privacy-first and quantum-resilient systems for the next generation of digital infrastructure.



Cybersecurity for today.

Resilience for tomorrow.

www.nbq-engineering.com

Engineering Security Beyond the Quantum Transition

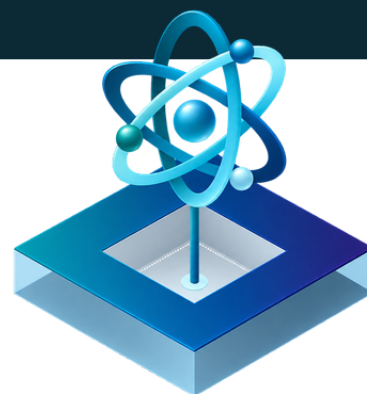
NBQ Engineering is a cybersecurity and engineering company focused on post-quantum cryptography, cryptographic resilience, secure communications and next-generation security architectures.

We work at the intersection of cybersecurity research and practical engineering, helping organizations understand existing cryptographic exposure, strengthen digital infrastructure and prepare for the transition toward quantum-resistant security.

From cryptographic discovery and post-quantum readiness assessments to secure communication architectures and experimental security platforms, NBQ Engineering connects research, cybersecurity and engineering implementation.



Advanced security research becomes valuable when it can be translated into systems that organizations can actually deploy.



OUR MISSION

To build trusted, privacy-first and quantum-resilient security technologies that help organizations move safely into the next era of digital infrastructure.

OUR VISION

To accelerate the transition toward digital systems where privacy, trust, security and cryptographic resilience are built into the architecture from the beginning.

NBQ = Navigating Beyond Quantum

Preparing systems not only for the threats organizations face today, but for the cryptographic challenges that will define tomorrow.

The Cryptographic Landscape Is Changing

Modern digital infrastructure depends on cryptography. Certificates, PKI, VPNs, authentication systems, embedded devices, cloud services, industrial systems and critical infrastructure all rely on cryptographic mechanisms to establish identity, confidentiality, integrity and trust.

The emergence of quantum computing introduces a long-term challenge to many public-key mechanisms used today. For organizations, post-quantum security is not simply an algorithm replacement problem. It is an infrastructure transition problem.



01

What cryptography do we currently use?

02

Where is it deployed?

03

Which systems depend on it?

04

Which assets face long-term cryptographic risk?

05

What can be upgraded - and what cannot?

06

How can migration occur without disrupting operations?

You cannot migrate what you cannot see.

The first step toward quantum resilience is understanding the organization's existing cryptographic attack surface and dependencies.

Our Core Capabilities

01 Post-Quantum Cryptography

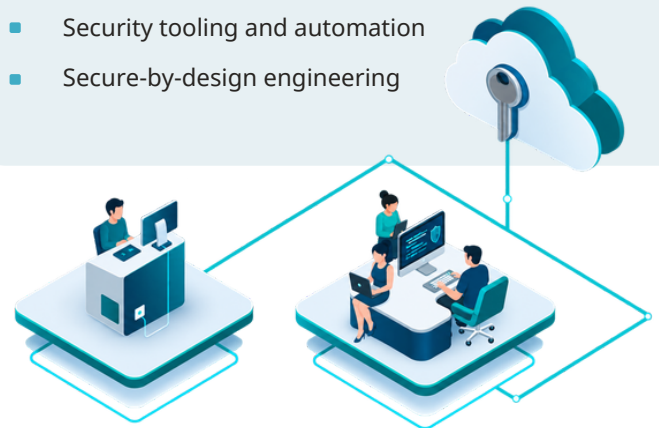
*Prepare cryptographic infrastructure for the **quantum** era.*

- Post-quantum readiness assessments
- Cryptographic asset discovery
- Cryptographic inventory / Crypto-BOM development
- Quantum-risk analysis
- Algorithm and protocol assessment
- Migration strategy and roadmapping
- Crypto-agility planning
- Hybrid classical/post-quantum architectures
- PQC experimentation and proof-of-concept development
- Performance and compatibility evaluation

02 Cybersecurity Engineering

*Turn security requirements into **practical engineering**.*

- Security architecture assessment
- System and network hardening
- Secure network design
- Security monitoring concepts
- Infrastructure security assessment
- Cryptographic configuration analysis
- Security tooling and automation
- Secure-by-design engineering



03 Secure Communications

***Protect** data across networks, devices and infrastructure.*

- Secure network communications
- VPN and encrypted communication architectures
- PKI and certificate architectures
- Hybrid cryptographic communication
- Post-quantum secure channels
- Edge and constrained-device communications
- Satellite and remote communication environments

04 Applied Security R&D

*Bridge **research** and real-world **deployment**.*

- Post-quantum cryptography
- Cryptographic migration
- Quantum-safe communications
- IoT and embedded cybersecurity
- OT and critical infrastructure security
- Cybersecurity automation
- Security testing environments
- Emerging communication technologies

From Cryptographic Discovery to Migration

Post-quantum migration should **not** begin by blindly replacing algorithms. NBQ Engineering approaches the problem as an engineering lifecycle.



THE OBJECTIVE IS NOT SIMPLY "PQC DEPLOYMENT."

It is to create infrastructure capable of discovering, replacing and evolving cryptography throughout its lifecycle.

PQAudit

CRYPTOGRAPHIC DISCOVERY & POST-QUANTUM READINESS

PQAudit is an NBQ Engineering R&D; platform designed to help organizations understand the cryptography present within their infrastructure and assess readiness for the post-quantum transition.

The platform focuses on transforming fragmented technical information into a structured view of an organization's cryptographic security posture.

PQAudit / readiness assessment workflow

01 DISCOVER

Identify cryptographic mechanisms

02 INVENTORY

Build structured crypto asset data

03 ASSESS

Detect weak / quantum-vulnerable exposure

04 PRIORITIZE

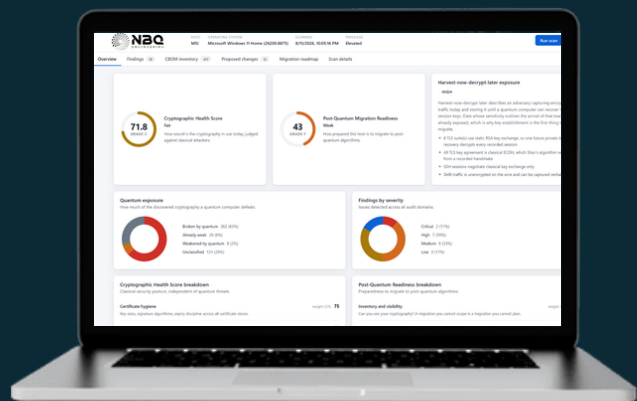
Rank systems by attention needed

05 PLAN

Support migration and crypto-agility

CURRENT R&D AREAS

- Linux cryptographic discovery
- Windows cryptographic discovery
- TLS and SSH configuration analysis
- Certificates and public-key mechanisms
- Crypto-BOM generation
- Cryptographic security scoring
- PQC readiness indicators
- Security recommendations
- Reporting and visualization
- Post-quantum migration support



[REQUEST DEMO](#)

Discover > Understand > Prioritize > Migrate

PQAudit is under active research and development. Capabilities may vary between platforms and deployment environments.

Research That Moves Toward Deployment

Practical prototypes, testbeds and proof-of-concept implementations evaluated under real engineering constraints.

NBQ Engineering explores emerging cybersecurity technologies not only theoretically, but under realistic constraints including performance, interoperability, resource consumption, network conditions and deployment complexity.

01

Post-Quantum Secure Communications

Experimental implementation and evaluation of classical, hybrid and post-quantum communication mechanisms, including key establishment, secure-channel experimentation, performance, overhead and interoperability.

02

IoT & Embedded Security

Exploring how modern cryptographic mechanisms can be integrated into resource-constrained devices and connected systems.

03

Critical Infrastructure & OT Security

Security research around industrial environments, operational technology, cyber-physical systems and cryptographic resilience for long-lived infrastructure.

04

Cybersecurity Testbeds & Quantum-Secure Networking

Controlled environments for attack simulation, monitoring, cryptographic evaluation and defensive validation, alongside exploration of quantum-safe networking architectures.





Where We Can Contribute

Our technologies are particularly relevant to environments where security, operational continuity and long-term confidentiality matter.

01 Critical Infrastructure

Cryptographic discovery, network security, crypto-agility and post-quantum migration for long-lived and operationally sensitive infrastructure.

02 Maritime & Transportation

Security assessment and cryptographic resilience across navigation, communication, operational and shipboard systems.

03 Telecommunications & Networks

Secure communications, authentication, cryptographic infrastructure and next-generation network security.

04 IoT & Embedded Systems

Secure device communication, cryptographic integration, identity and lifecycle security for constrained and connected systems.

05 Cloud & Enterprise Infrastructure

Cryptographic visibility, secure communications, certificates, keys and migration planning across heterogeneous infrastructure.

06 Space & Satellite Systems

Secure communication architectures and quantum-resilient security concepts for satellite, ground-segment and remote communications.

ALSO RELEVANT TO

Public Sector | Defence & Dual-Use R&D; | Healthcare | Finance | Research Infrastructure | Industrial Systems

07 | COMPLEX DIGITAL ENVIRONMENTS

Security, operational continuity and long-term confidentiality.

From Research Question to Engineering Solution

NBQ Engineering can contribute at different stages of a cybersecurity or research project - independently on specialized technical problems, or alongside an organization's engineering, cybersecurity and research teams.

01 ASSESS

Understand the system, architecture, cryptographic dependencies, threat landscape and security requirements.

RESEARCH | ENGINEERING | VALIDATION

02 DESIGN

Develop security architectures, migration strategies and technical specifications.

RESEARCH | ENGINEERING | VALIDATION

03 PROTOTYPE

Build demonstrators and proofs of concept to validate approaches before larger-scale deployment.

RESEARCH | ENGINEERING | VALIDATION

04 TEST

Measure security, interoperability, performance and operational constraints.

RESEARCH | ENGINEERING | VALIDATION

05 INTEGRATE

Support the introduction of security mechanisms into existing systems and architectures.

RESEARCH | ENGINEERING | VALIDATION

06 EVOLVE

Design toward crypto-agility so security can adapt as standards, threats and technologies change.

RESEARCH | ENGINEERING | VALIDATION

Research & Consortium Collaboration

NBQ Engineering is interested in collaborating with companies, SMEs, universities, research centres, technology providers and public-sector organizations developing the next generation of secure digital infrastructure.

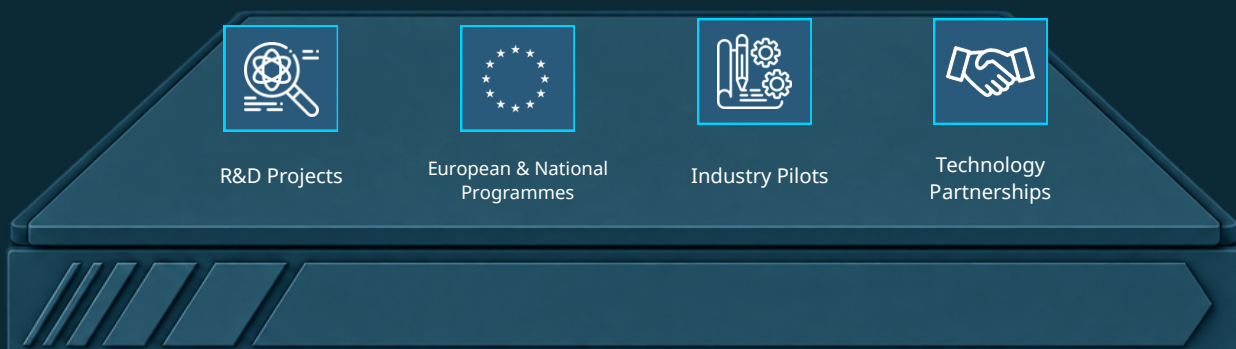
RESEARCH & TECHNICAL CONTRIBUTIONS

- Post-quantum cryptography
- Cryptographic migration and crypto-agility
- Cybersecurity architecture
- Secure communications
- Cryptographic asset discovery
- Critical infrastructure security
- IoT and embedded security
- Maritime cybersecurity
- Secure satellite communications
- Quantum-safe networking
- Security testing and validation

PROJECT CONTRIBUTIONS

- Requirements definition
- Architecture and technical specifications
- Technology assessment
- Prototype development
- Integration
- Cybersecurity testing
- Demonstration environments
- Performance evaluation
- Technical documentation
- Pilot support
- Research dissemination

COLLABORATION MODELS



From research concepts to deployable security.

A specialized cybersecurity and post-quantum engineering partner for collaborative R&D, pilots and technical integration.



Let's Build What Comes Next.

Exploring post-quantum migration or building a research consortium, NBQ Engineering is ready to contribute.

Cybersecurity

Post-Quantum Cryptography

Secure Systems Engineering

Applied Security R&D

NBQ ENGINEERING

Navigating Beyond Quantum

WEB www.nbq-engineering.com

EMAIL contact@nbq-engineering.com

LOCATION Greece | European Union

Cybersecurity for today.
Quantum resilience for tomorrow.

