SORINTEQ

PHOENIX PROGRAMME

COVERT NETWORK INVESTIGATOR

Postgraduate Certificate
(PgCert)
in Cyber Security & Intelligence

- 12 Month Programme
- Specialist Training for Law Enforcement
- All Training Equipment Provided
- In Association With the University of Buckingham

Contact Us

0333 0063248

Sorinteq Academy

SORINTEQ

Overview of the Programme

Modern investigations demand professionals who can operate confidently across the full digital investigative landscape. From cybercrime and cryptocurrency to darknet environments, radio frequency exploitation, covert research, and advanced cyber reconnaissance, investigators must be able to work across multiple technical disciplines while maintaining evidential integrity and operational security.

The Phoenix Programme – Covert Network Investigator (CNI) is one of Sorinteq's premier learning pathways, designed to transform experienced investigators into highly capable digital operatives who can work across all aspects of digital investigation and under a range of authorisations and warrants.

This flagship 12-month professional development pathway equips delegates with the knowledge, technical capability, and operational confidence required to become advanced digital investigators capable of supporting intelligence-led operations, cyber investigations, covert activity, and technical exploitation.

Successful learners achieve a Postgraduate Certificate (PgCert) in Cyber Security & Intelligence, combining academic recognition with real-world operational capability.

The Phoenix Programme develops investigators who can work independently, support specialist teams, and operate effectively in complex and hostile digital environments.

SORINTEQ

Programme Structure

The Phoenix Programme is delivered across 12 months and consists of:

9 Specialist Modules

Each module delivered over 2 days, combining theory, operational practice, and practical assessment.

Academic Written Assignment

A 5,000-word essay focused on Cyber Crime, testing both academic understanding and operational application.

Final Operational Exercise

A month-long live investigative exercise designed to test the full range of learned capabilities in a realistic operational environment.

Final Dissertation Submission

A substantial written submission demonstrating professional competence, strategic understanding, and applied investigative methodology.

Successful completion results in the award of a PgCert in Cyber Security & Intelligence.

Who is this Programme For?

This programme is designed for experienced investigators and intelligence professionals seeking to develop into high-level digital operatives, including:

- Law enforcement investigators
- Government intelligence officers
- Cybercrime and cyber security investigators
- Digital forensic practitioners
- Intelligence analysts and technical collection staff
- Corporate investigation and serious fraud specialists
- Protective intelligence and operational security professionals

The programme is ideal for delegates who already possess investigative experience and require advanced development into full-spectrum digital investigators.

SORINTEQ

Programme Modules

1. Introduction to Cyber Crime
Understanding the modern cybercrime landscape, offender methodologies, and investigative opportunities.
Including:

- Cyber-enabled vs cyber-dependent crime
- Threat actor behaviours
- Criminal methodologies and typologies
- Organised cybercrime groups
- Investigative opportunities and case studies

2. Fundamentals of Cryptocurrency Investigation
Providing the operational understanding required to investigate digital currencies and criminal financial flows.
Including:

- Cryptocurrency types and ecosystems
- Wallets, blockchain, and tracing
- Criminal use of digital assets
- Investigative opportunities
- Evidential recovery considerations

3. Fundamental Darknet Investigations
Developing capability to investigate hidden online ecosystems and criminal marketplaces.
Including:

- TOR and alternative darknet platforms
- Forums, marketplaces, and criminal services
- Encrypted messaging platform crossover
- Investigative opportunities
- Operational case studies

4. Security in Cyber Operations
Building secure operational environments and reducing digital exposure in sensitive investigations.
Including:

- Digital footprint management
- Public key encryption
- Secure smartphone builds
- Virtual machines and isolated environments

Adversary targeting and operational security

SORINTEQ

Programme Modules

5. Fundamental Cyber Recon
Introducing technical skills to enhance online investigations through Linux and code-based methodologies.
Including:

- Linux fundamentals
- Virtual operational environments
- Automation opportunities
- Command-line capability
- Technical investigative support tools

6. Fundamentals of Radio Frequency Exploitation
Understanding how RF signatures create investigative opportunities across the physical and digital environments.
Including:

- RF spectrum awareness
- Smartphone and Wi-Fi exploitation opportunities
- Digital breadcrumbs and subject tracking
- Behavioural pattern development
- Operational case studies

7. **Fundamentals of HUMINT in Cyber Operations**
Combining traditional human intelligence principles with modern digital investigative tradecraft.
Including:

- Online engagement principles
- Source development
- Behavioural indicators
- Rapport building in digital environments
- Intelligence capture and validation

8. Intermediate Cyber Recon
Building on foundation skills with enhanced technical capability and code-based investigative methods.
Including:

- Advanced Linux operations
- Social media and platform exploitation
- Code-based research tools
- Intelligence enhancement and analysis
- AI-assisted investigative opportunities

SORINTEQ

Programme Modules

9. Integrated Investigative Development Module
Bringing together multiple investigative disciplines to support high-level operational delivery.
Including:

- Cross-discipline intelligence fusion
- Advanced investigative strategy building
- Operational planning and prioritisation
- Multi-source intelligence validation
- Preparation for final operational exercise

Final Exercise Phase
Month-Long Live Operational Exercise
Delegates will participate in a complex live investigative environment requiring the use of all programme disciplines within a realistic operational setting.
This exercise includes:

- Live cyber investigation
- Cryptocurrency tracing
- Darknet intelligence development
- HUMINT and covert engagement opportunities
- RF and behavioural intelligence development
- Operational reporting and evidential product creation
- Supervisory review and structured debrief

This phase replicates the pressures and complexity of real-world operational investigations and confirms readiness for independent deployment.

Academic Assessment
5,000-Word Essay
A formal academic submission focused on Cyber Crime, testing analytical thinking, investigative understanding, and academic application.
Final Dissertation Submission
A substantial professional dissertation demonstrating mastery of the programme and the practical application of digital investigative methodologies.

The Outcome
Qualified students will be a major asset to any digital investigation, cyber intelligence, or technical operational team, bringing:

- Advanced digital investigative capability
- Strong technical and operational judgement
- Professional evidential standards
- Multi-discipline intelligence capability
- Academic credibility through a recognised PgCert award

Become a Phoenix
The best investigators don't just follow the digital trail—
they understand how to control it.
Train to become one of them

SORINTEQ

Aims and Objectives of the Course

By the end of the Phoenix Programme, learners will be able to:

- Operate independently as a professional Covert Network Investigator
- Conduct advanced digital investigations across multiple technical environments
- Investigate cybercrime and identify opportunities for evidential and intelligence development
- Understand cryptocurrency ecosystems and exploit investigative opportunities
- Operate effectively within darknet environments and criminal online communities
- Apply cyber operational security and secure investigative tradecraft
- Conduct cyber reconnaissance using Linux, code-based tools, and virtual environments
- Identify and exploit radio frequency (RF) opportunities to support investigations
- Apply HUMINT principles within cyber and digital operational environments
- Deliver intelligence and evidential outputs to professional and judicial standards
- Operate lawfully, proportionately, and effectively under appropriate authorisations and warrants

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations worldwide. The Phoenix Programme is designed by operational specialists who understand the reality of modern digital investigations and the need for investigators who can operate across multiple disciplines.

This is more than a course—it is a complete professional development pathway. Graduates leave as highly capable, operationally credible Covert Network Investigators, equipped with both academic accreditation and advanced technical capability.

Students undertaking courses provided by Sorinteq may earn credits towards formal academic qualifications such as Post Graduate Certificate, Diploma or MSc at the university of Buckingham.

For further enquiries please email info@sorinteq.com or call Sorinteq on +44 (0)333 0063248.

Sorinteq provide all necessary training equipment including laptop computers, internet connectivity, mobile devices and training material.