SORINTEQ

PILGRIM PROGRAMME

COVERT INTERNET 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

The modern investigative landscape demands professionals who can operate confidently in both the digital and human intelligence environments. Traditional online investigation skills alone are no longer enough—today's investigators must be capable of combining OSINT, Digital HUMINT, covert engagement, behavioural analysis, darknet awareness, cryptocurrency understanding, and cyber investigative tradecraft to operate effectively against sophisticated adversaries.

The Pilgrim Programme – Covert Internet Investigator (CII) is Sorinteq's flagship 12-month professional development pathway, designed to take learners from foundational understanding to advanced operational competence as independent covert internet investigators.

This specialist pathway is designed for investigators and researchers whose roles rely heavily on the concentration of Digital HUMINT skills, particularly where covert engagement, online behavioural analysis, intelligence development, and discreet digital investigations are central to operational success.
Delegates who successfully complete the programme achieve a Postgraduate Certificate (PgCert) in Cyber Security & Intelligence, providing both academic accreditation and significant operational capability.

The Pilgrim Programme develops highly competent operators capable of working independently in challenging digital HUMINT environments and producing results against even the most hardened targets.

SORINTEQ

Programme Structure

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

8 Specialist Modules

Each module delivered over 2–5 days, combining theory, operational practice, and practical assessment.

Academic Written Assignment

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

Final Operational Exercise

A month-long live investigative exercise designed to test all learned capabilities in a realistic operational environment.

Dissertation Submission

A substantial final written submission demonstrating professional competence, analytical ability, and applied operational understanding.

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

Who is this Programme For?

This programme is designed for professionals working in intelligence gathering, investigations, and discreet digital operations, including:

- Government investigators and intelligence officers
- Law enforcement personnel
- Corporate intelligence and due diligence professionals
- Counter-fraud and financial investigators
- Cyber intelligence and digital research teams
- Protective intelligence and security professionals
- Researchers involved in covert online engagement and behavioural investigations

The programme is ideal for delegates who are relatively new to the Digital HUMINT environment but require rapid development into highly capable operational practitioners.

SORINTEQ

Programme Modules

1. Legal Considerations in Digital Investigations
Understanding the legal frameworks, authorisations, proportionality, and governance required when conducting covert online activity and digital investigations.
Including:

- Investigatory powers and legal thresholds
- Covert online activity considerations
- Privacy, proportionality, and human rights
- Evidence recovery and legal defensibility
- Governance and operational compliance

2. Building Your CII Toolkit and Team
Developing the operational infrastructure, secure environments, and support mechanisms required for effective covert internet investigation.
Including:

- Operational security (OpSec)
- Secure devices and communications
- Virtual environments and infrastructure
- Team structure and operational planning
- Identity management and resilience

3. Intermediate Internet Intelligence & Investigation (I3)
Developing enhanced OSINT capability using advanced internet research methodologies and investigative tradecraft.
Including:

- Linux operational environments
- Advanced platform investigations
- Code-based investigative tools
- Enhanced social media exploitation
- Intelligence development and validation

4. Fundamentals in Digital HUMINT
Introducing the principles of covert online engagement, elicitation, and behavioural intelligence gathering.
Including:

- Human source development online
- Rapport and trust building
- Online behavioural indicators
- Covert engagement principles
- Intelligence capture and validation

SORINTEQ

Programme Modules

5. Fundamental Darknet Investigations
Understanding the structure, operation, and investigative opportunities within darknet environments.
Including:

- TOR and alternative darknet platforms
- Forums and marketplaces
- Criminal use of the darknet
- Encrypted messaging platform crossover
- Investigative opportunities and case studies

6. Fundamental Cryptocurrency Investigations
Providing an operational understanding of digital currencies and how they support criminality and intelligence opportunities.
Including:

- Cryptocurrency types and ecosystems
- Wallets and blockchain understanding
- Transaction tracing
- Investigative opportunities
- Evidential recovery considerations

7. Intermediate Digital HUMINT
Building on foundational HUMINT skills with enhanced elicitation, engagement, and operational management techniques.
Including:

- Advanced elicitation strategies
- Covert engagement planning
- Persona development
- Counter-detection awareness
- Managing digital source relationships

8. Fundamental Cyber Recon
Introducing technical skills to enhance intelligence collection through code-based tools and Linux operational environments.
Including:

- Linux fundamentals
- Virtual investigative environments
- Automation opportunities
- Basic scripting and tool usage
- Operational cyber research techniques

SORINTEQ

Programme Modules

Final Exercise Phase
Month-Long Live Operational Exercise
Delegates will participate in a structured, high-pressure digital investigation where all programme disciplines must be applied in a realistic covert operational environment.
This exercise includes:

- Live intelligence gathering
- Covert identity management
- Digital HUMINT engagement
- Darknet and crypto investigative opportunities
- Reporting and evidential product generation
- Supervisory debrief and operational review

This phase is designed to replicate real-world operational demands and confirm readiness for independent deployment.

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

The Outcome
Qualified students will be an asset to any discreet digital research or intelligence team, bringing:

- Advanced covert online investigative capability
- Strong operational judgement
- Professional evidential standards
- Enhanced HUMINT and cyber investigative skills
- Academic credibility through a recognised PgCert award

Become a Pilgrim
The digital world belongs to those who can move through it unseen.
Train to become one of them.

SORINTEQ

Aims and Objectives of the Course

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

- Operate independently as a professional Covert Internet Investigator
- Conduct advanced Digital HUMINT operations against sophisticated online subjects
- Develop and maintain covert online identities and operational infrastructure
- Conduct structured intelligence gathering using advanced OSINT and I3 techniques
- Understand legal authorities, governance, and evidential requirements in digital investigations
- Operate effectively across darknet platforms and criminal online ecosystems
- Understand cryptocurrency environments and exploit associated investigative opportunities
- Use cyber reconnaissance techniques to enhance intelligence collection
- Build professional investigative strategies combining HUMINT and cyber methodologies
- Deliver intelligence and evidential outputs to a professional, defensible standard
- Operate safely, ethically, and effectively in hostile digital environments

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations globally. The Pilgrim Programme is designed by operational specialists who understand the realities of modern covert digital investigations.

This is not simply training—it is a professional transformation pathway. Graduates leave as highly capable, operationally credible Covert Internet Investigators, equipped with both academic accreditation and real-world 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.