ICC
Commercial
Crime Services
A specialised division of the
International Chamnber of Commerce

23rd ICC CCS
Internet **Intelligence** Course
The New Era of Open-Source Intelligence

A Three Day Hands-On Workshop
at University of Cambridge

Venue
Queens' College
University of Cambridge

Date
22 - 25 September 2025

The Truth is Out There - If You Know Where to Look

In a world awash with disinformation, censorship, source credibility issues, AI feedback loops and "infoxication", finding reliable information online is now more challenging than ever.

This comprehensive three day hands-on workshop will provide you with updated skills, new ways of thinking, and the cutting-edge online tools required to navigate the online domain with precision, efficiency, and ethical integrity.

By attending delegates will learn how to:

Advance Search Techniques:
The latest tools and techniques used by intelligence analysts, law enforcement, cybersecurity experts, and corporate investigators.

A New Investigative Mindset:
To tackle challenges posed by AI-driven search engines and use them more effectively.

To Identify Deception and Suspicious Activity:
The cognitive mechanisms behind deception and the techniques for effectively overcoming them.

To Leverage Online Monitoring and Automation Tools:
Setting up systems to convert raw data into actionable insight, while avoiding common traps that result in failures.

How to Use Dark and Deep Web Tools for Threat Intelligence:
Reduce risk exposure by uncovering attack plans and leaked information to improve incident response time.

Registration Details:

Course fees: GBP 2,950 (inc. VAT)

To register, please visit: www.icc-ccs.org/IIcourse

or contact:
Annette Galloway,
Tel: +44 (0)20 7423 6960
Email: agalloway@icc-ccs.org

Facilitators:

David Toddington
Founder & CEO
Toddington International Inc

Vincent Cook
Founder & CEO
Cyb3r Operations

Attendees will get Exclusive Access to the CyberOperations Third Party Intelligence Platform

The New Era of Open-Source Intelligence

A Three Day Hands-On Workshop at University of Cambridge

Curriculum Highlights

Search Foundations for Effective OSINT:
- Strategies for Managing AI Driven Technological Change
- Search Query Analysis
- Online Security: Maintaining Operational Integrity
- Managing and Leveraging Location-Based "Filter Bubbles"
- Advanced Search Operators and Results "Signal to Noise Ratios"
- Key Identifier Resolution (including Usernames, Email Addresses, Phone Numbers)
- Fact Checking Best Practices
- OSINT Ethical and Legal Considerations

Misinformation, Disinformation, and Malinformation (MDM):
- MDM Actors and Motivations
- Disinformation Propagation Mechanisms
- Impact of MDM on OSINT Operations
- MDM Identification and Assessment
- MDM Mitigation Strategies

Tools for Automation and Monitoring:
- Discovering, Assessing and Responding to Third-Party Risks
- Proactive Threat Assessment Techniques
- Predictive Risk Scoring and Exposure Analysis
- Insider Threat Monitoring

Mechanisms of Deception: Deepfake Imagery:
- How Deepfakes are Created Using AI and Machine Learning
- Best Practices for Verifying Deepfake Imagery
- Legal Frameworks and Regulations Aimed at Combating the Misuse of Deepfakes

Image Intelligence and Analysis:
- Image Verification and Authentication
- Meta Data and Image Forensics
- Photogrammetry and Location Analysis
- Ethical Facial Recognition Tools

Strategic and Tactical Threat Analysis Using the Deep and Dark Web:
- Using the Dark Web for Threat Intelligence and Organizational Risk Assessment
- Tor Hidden Services Overview
- Dark Web Research Tools and Techniques
- Automation for Effective Threat Assessment

Social Media Intelligence:
- Social Media for Specific Intelligence Needs and Goals
- Data Collection and Analysis Techniques and Tools
- Best Practices for Ensuring Compliance and Protecting Privacy

Critical Thinking for OSINT Practitioners:
- Information Resilience and Fact Checking
- Evaluating Sources for Credibility and Reliability
- Cross-Referencing and Corroborating Information
- Identifying and Mitigating Cognitive Biases

contact:
Annette Galloway,
Tel: +44 (0)20 7423 6960
Email: agalloway@icc-ccs.org

Attendees will get Exclusive Access to the CyberOperations Third Party Intelligence Platform

The New Era of Open-Source Intelligence

A Three Day Hands-On Workshop at University of Cambridge

An Outstanding Learning Experience:

Presented by ICC – Commercial Crime Services and led by Toddington International Inc., this highly acclaimed workshop attracts international participants from both the private and public sectors. In addition to cutting edge training, it's an excellent networking opportunity, with accommodation, meals, and social events included for a unique and memorable "Cambridge University Experience".

Who Should Attend:

- Law Enforcement and Security Professionals
- Manufacturers and Suppliers
- Government Regulators
- Risk Mitigation Specialists and Insurance Professionals
- Legal Professionals and Compliance Specialists
- Distributors and Logistics Providers
- Academics and Researchers
- Investigative Journalists
- Auditors and Analysts
- Human Resources Professionals
- Competitive Intelligence Specialists

Venue

The Course takes place at Queens' College, University of Cambridge. Queens' College was founded in 1448 and is situated in the centre of Cambridge close to many historic buildings and shops, and is within easy reach of the rail station.

Accommodation is provided for delegates in single, en-suite university-style rooms.

Parking is not available at the college but car parks are located close by.
Further details about the college can be found at
www.queens.cam.ac.uk.
Queens' College, Cambridge, CB3 9ET. Tel: +44 (0) 1223 335511

Registration Details: Course fees: GBP 2,950 (inc. VAT)

Note: Payment must be received in advance of the course. Three or more delegates from the same company are entitled to a 10% discount. Delegates are responsible for their travel expenses in travelling to the Course. Cancellations received 14 days before the Course date will receive a refund, minus a £500 administration fee.

After this date the full fee must be paid but substitutions may be made at any time.

Your Facilitators

David Toddington

With a career that started during the earliest days of public Internet access over twenty-five years ago, David Toddington is internationally recognized as one of the world's most experienced Open-Source Intelligence professionals.

Combining his unique front-line experience in national security, police, and military operations, with his background as a senior manager in the IT industry, David founded Toddington International in 1997 to provide advanced OSINT training and operational support services to investigative and research professionals around the world.

Specializing in weapons non-proliferation, sanctions enforcement and cooperative threat reduction issues, David works with government, NGO, and private sector clients internationally.

Driven by the desire to use OSINT to help make the world a better and safer place, David serves as an Affiliated Expert with NGO CRDF Global; he is a member of the Safe Ukraine 2030 Expert Council in Kyiv and a Special Advisor to the International Chamber of Commerce Commercial Crime Services in London. David also serves as a Strategic Advisor to Cyb3r Operations, a UK based technology company providing Cyber Threat Assessment solutions.

Vincent Cook

Vincent Cook is a driven entrepreneur with a passion for cyber security and education. Vincent began his first cyber security company at 14 years old, delivering security assessments and Open-Source Intelligence driven investigations.

He is certified in several leading OSINT training programs, which enables Vincent to support Toddington International by developing and facilitating specialized Dark Web Intelligence, Deep Web Intelligence, and Social Media Intelligence training courses and content for a wide range of agencies.

Vincent delivers intelligence driven investigations and training to international partners, including government agencies, counter-terrorism units, financial institutions, and private sector organizations.

His goal for clients is to help develop and strengthen their ability to use Open-Source Intelligence methodology within tactical collection and data analytics tools.
Vincent is the Founder and CEO of Cyb3r Operations and serves as TII's Chief Technology Officer.

About Toddington International Inc (TII)

Over the past 27 years, and guided by the principles of Knowledge, Integrity, and Excellence, TII has built a broad international network of practitioners, deliberately selected from a variety of backgrounds for their passion and innovation. The TII team has extensive experience in national security issues, complex criminal investigations, counter-terrorism operations, disinformation countermeasures, anti-money laundering compliance, sanctions enforcement, non-proliferation, public safety, and anti-human trafficking issues, among others.

TII's clients include a wide range of law enforcement, public safety, and regulatory agencies around the world, particularly in Canada, the United Kingdom, Australia, New Zealand, and the United States. Training services are regularly conducted on behalf of Interpol to its member organizations; NGOs served include CRDF Global and the International Justice Mission, and ongoing training is provided to a wide range of private sector organizations in North America, Latin America, Europe, Asia, and Africa.

A federally certified educational institution in Canada, TII is committed to improving people's lives around the world, and each year donates expertise, resources, and funding to various humanitarian initiatives.