DODS | TRAINING

Cybercrime and Cyber Security
Training Courses

About Dods Group

For over 180 years, Dods has provided essential access, insights and analysis to the political and public sectors. Since the first publication of the Dods Parliamentary Companion in 1832, Dods has evolved into an international business intelligence, media and events company. With impartiality and transparency underpinning everything we do, we are a trusted source of political intelligence and debate.

Dods utilises its access and intelligence to help brands better understand the regulatory and legislative environment that they work in and provides platforms to engage with policy makers and those that implement policy across the UK and EU. We provide unrivalled integrated services, delivering 360 campaigns that maximise impact across a broad spectrum of channels to help inform, educate and engage corporates, policy makers and governments.

Dods Training

Dods Training partners with governments, businesses, central and development banks, NGOs, and UN agencies to devise learning and development solutions that help improve people, organisational, and systems performance.

For the past 20 years, we have evolved into an internationally recognised and respected name in training with an unparalleled reputation across the public sector for providing outstanding courses. Dods Training is a longstanding partner to the governments around the world, including the European Union and is also a supplier to Civil Service Learning.

Having worked in more than 40 countries, we have extensive networks of associates across different regions including:
- Europe
- the Western Balkans
- Central America
- Caribbean
- South Asia
- the Middle East
- Sub-Saharan Africa

Our broad networks ensure we can deliver programmes that are of a consistent quality across a range of geographical locations, combining local with global expertise.

Our Trainers

Our teams of experts and specialist trainers deliver engaging and comprehensive learning programmes that meet clients' skills and development needs. We will work closely with you to make sure we bring the right blend of topic and training experience for your departments and organisational development.

Our Courses

The digital world is here to stay, and as we rely on the convenience of our many devices to carry out daily tasks from communicating with others, banking, to meeting potential mates, there are others who are using the technology for harm. We have developed some new courses to address this challenge.

Cybercrime Investigation and Cyber Security

An introduction to the concepts, systems vulnerabilities, types of attacks, ways to respond, and procedures to enhance the detection and investigation of cybercrimes. It also looks at ways to extract and preserve digital evidence so that it leads to prosecution, in compliance with international standards, with the support of mutual legal assistance.

The training is targeted towards law enforcement personnel, judicial officers and prosecutors.

Learning objectives: To enhance capabilities to investigate cybercrime and to prevent and respond to cyber attacks. Issues covered include:
- digital transformation and need for cyber security
- attack types and identifying vulnerabilities
- managing cyber/digital incidents
- collecting digital evidence and its preservation and integrity
- chain of custody
- ethical considerations, regulations and standards
- mutual legal assistance

Cyber Enabled Gender-Based Violence and Criminal Exploitation

Cyber enabled gender-based violence and criminal exploitation is a silent crime and has increased over the Covid 19 Pandemic. Criminals are adapting rapidly to the changing environment. This crime type involves organised criminal groups and serial dangerous offenders perpetrating against multiple victims.

The training is designed for justice professionals including law enforcement, judicial officers, prosecutors, health and social care professionals, and those who wish to enhance their knowledge of the subject.

Learning objectives: To understand the presentation of recent crimes, the victim impact, and measures to address these crimes. Issues covered include:
- what cyber enabled gender-based violence is and the different forms it takes
- the role that justice and security sector partners and public authorities play in taking a gender responsive approach
- the victim's perspective
- the requirements for collaboration at country, regional and global levels
- knowledge of the practical application of the underpinning principles to prevent and tackle gender-based violence and criminal exploitation

Cyber Security Awareness in the Workplace

Many businesses and organisations have a degree of cyber security in place but it can be innocently negated by lack of knowledge and understanding within the workforce. The workshop explores the vulnerabilities faced by every business at every level and the ways in which these vulnerabilities can be minimised.

Learning objectives: To understand the importance of cyber awareness within organisations, and how to institute measures to reduce the risks and respond to and recover from cyber-attacks. Issues covered include:

- components of cyber awareness training
- ways that cyber-attacks are launched
- the continuous level of security required for office, hybrid and remote/home working
- password protocol and management
- admin controls — the rule of least privilege
- the inherent risks of employing internet connected devices (IoT)
- asset management
- identifying and securing key data
- risk assessment and recovery

Combatting Fraud and Corruption

Ways in which organisations can reduce the threats from internal and external fraud and corruption.

It is targeted towards departments in organisations where the risks from fraud are likely to be greater and the potential impact of fraudulent activity will pose most threat to the reputation of the institution whether in government, an NGO or an institution.

Learning objectives: To understand the boundaries between diplomacy, politics, commerce and corruption and ways in which risks can be minimised.

Key topics:
- risk assessments, policies, fraud response plans
- fraud and corruption classification
- internal and independent scrutiny and oversight mechanisms
- codes of conduct and declaration of assets registers
- beneficial ownership registration
- conflicts of interest
- mutual legal assistance and unexplained wealth orders
- deferred prosecutions
- first steps on suspecting fraud or corruption
- reporting mechanisms
- using forensic experts
- sanctions

# Confronting Money Laundering and Terrorist Funding

Examine ways in which organisations and individuals can protect themselves from the dangers of illicit movement of funds.

This training is for organisations and individuals who need an understanding of the main challenges in this area and want to gain a familiarity with how the illicit movement of money threatens organisations and individuals as well as what can be done to minimise risks.

Learning objectives: To understand how to reduce the risks of money laundering and identify potential weaknesses and find assistance in dealing with suspect transactions.

Key topics:
· the nature of money laundering
· risk areas and protection methodologies
· the impact of cybercrime and cyber enabled crime
· finding out who owns what
· cryptocurrencies
· approaches adopted by major economies
· legislative and regulatory frameworks
· where to get advice and help
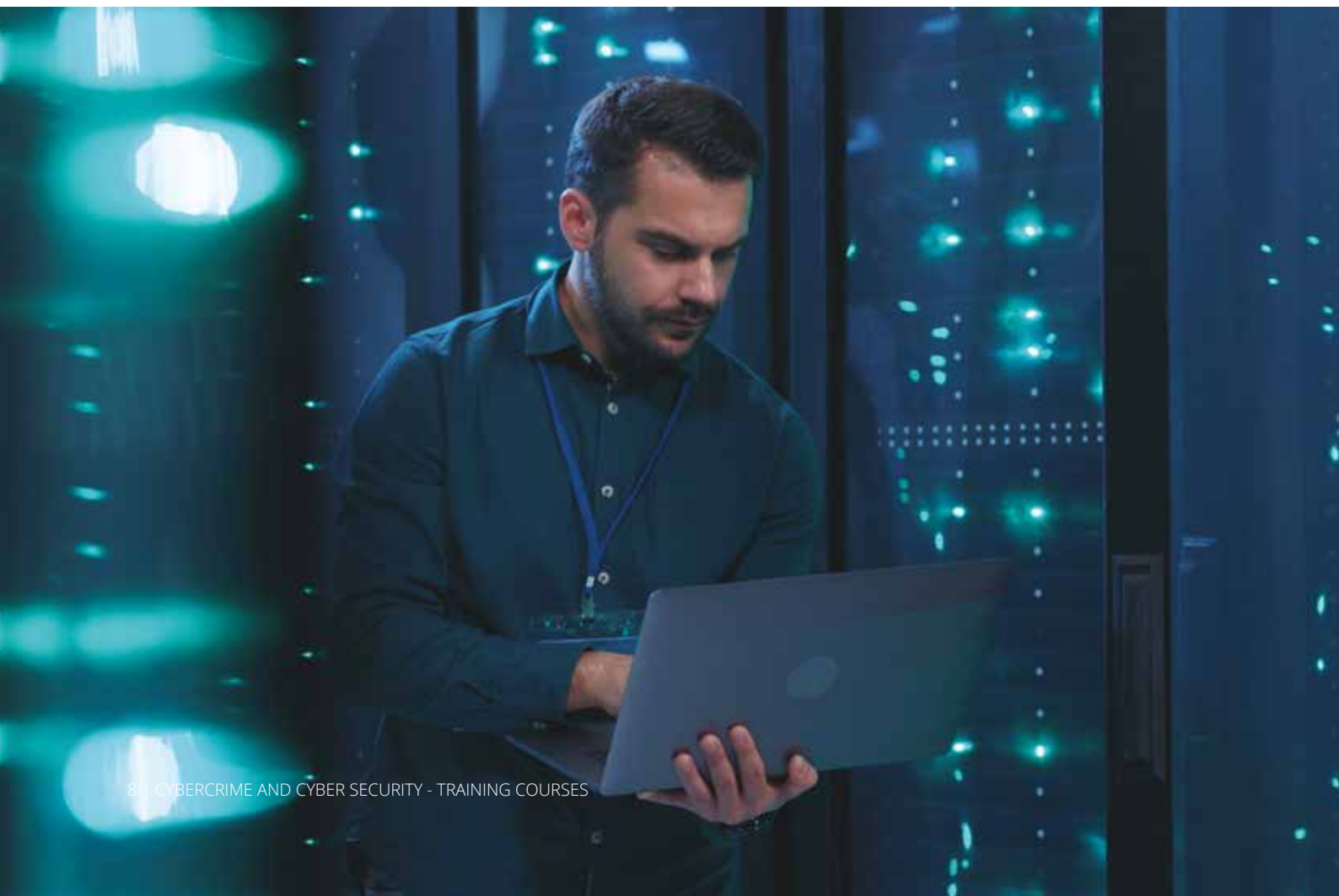
Our specialist trainers in this area include:

Gerry Campbell

Gerry Campbell is an expert consultant on issues of rule of law, policing, security and gender-based violence (GBV) in the UK and internationally. He is a former Detective Chief Superintendent at Scotland Yard, serving for the last 30 years, leading strategy on Community Safety and Public Protection whilst managing high risk operations including the responses to domestic abuse, honour-based abuse, forced marriage, and the management of dangerous and violent offenders. He is an Associate Lecturer in Criminology & Psychology and an independent Chair of Statutory Domestic Homicide Reviews. He has authored books and articles on GBV and developed and delivered training on these issues to UK bodies like NHS England, the Bar Council, and in international jurisdictions to the judiciary and law enforcement agencies, and to UN bodies of IOM and UN Women. In 2019 he received a UK National Honour for Services to Crime Prevention and to the elimination of Violence Against Women and Girls.

Neil McCallum

Neil's area of expertise is the prevention and deterrence of fraud, in particular through document, records and information management systems. He has led a number of international development projects and study programmes, working with public servants, politicians and civil society on a range of good governance issues around the better utilisation of public sector information to reduce fraud and corruption opportunities. Recent assignments include enhancing court records systems in The Gambia, exploring opportunities for ethical change with the Kenya Judicial Services Commission, reviewing plans for a new Anti-Corruption court in Sierra Leone and promoting integrity in Monserrat. Neil is a member of the Royal African Society and the Royal Commonwealth Society. In September 2017, Neil was elected a Fellow of the Institute of Information Management of Africa in recognition of his contribution to improvements in public sector information handling in Africa.

Simon Newman

Simon has over 15 years' experience in senior Project / Programme Management roles working for the Home Office and National Police Improvement Agency. He was Programme Director for the National Police Air Service – the first operational policing function ever to have been delivered nationally and has led a number of major business change programmes. He has also led in-depth reviews of projects both in the UK and overseas. Since leaving the Civil Service in 2013, Simon has worked as a Strategic Advisor to Abu Dhabi Police and the Ministry of Interior in the UAE and is now Head of Cyber and Business Services for Police Crime Prevention Initiatives, working across Government and the private sector to enhance the security posture of the UKs small business community.

Neil Sinclair

Neil Sinclair is the National Cyber Lead for the UK Police Digital Security Centre. Neil has been recognised in "The Progress 1000: London's most influential people" for his work in Technology & Cyber Security. Neil worked in UK counter-terrorism policing for over thirty years during which time he was involved in most of the Metropolitan Police's biggest Terrorist Operations. He was a key member of the National Terrorist Financial Investigation Unit for 10 years and is an accredited Financial Investigator. Neil has delivered training courses for the UK Government and UN.

Neelam Sarkaria

Neelam is an expert consultant on the rule of law, criminal justice sector reform, gender-based violence, equality and diversity, and gender mainstreaming in the UK and internationally. She has a strong prosecution and Whitehall policy background of more than 24 years. As a former Non-Executive Director of the Civil Nuclear Police Authority she led work on People, Gender and Inclusion and Audit and Risk on behalf of the Board. She has expertise in gender equality as former Chair and of the Association of Women Barristers and the Bar Council of England and Wales Equality, Diversity and Social Inclusion Committee. She now sits as a part-time Tribunal Judge and regulatory Chair, is a Gender Adviser for a UK national police force and chairs Domestic Homicide Reviews. She works as an advisor for UN Agencies and with the judiciary and law enforcement on matters of the Rule of Law, GBV and Gender Mainstreaming in Africa, Middle East, Europe and Asia.

For More Information

UK based training contact
Alice McDavid
Head of UK Training
alice.mcdavid@dodsgroup.com
+44 (0) 7880 195 011

Outside of the UK training contact
Christine Tokar
Senior International Project Manager
christine.tokar@dodsgroup.com
+44 (0) 7867 457 650

DODS | **TRAINING**