

8th annual... CYBER INTELLIGENCE EUROPE Oslo, Norway 1st – 3rd March 2022

Supporting Partners



Confirmed Speakers

- Rear Admiral **Davide Berna**, Commander, Joint Intelligence Centre, **Ministry of Defence, Italy**
- Major General **Inge Kampenes**, Commander, Cyber Defence, **Norwegian Armed Forces**
- Brigadier General **Anton Rog**, Head, National Cyberint Center, **Romanian Intelligence Service (SRI)**
- **Bente Hoff**, Head, **National Cyber Security Centre, Norway**
- **Robin Bakke**, Director, Cyber Security, Department of Public Security, **Ministry of Justice and Public Security**
- **David van Weel**, Assistant Secretary General, Emerging Security Challenges, **NATO**
- **Edvardas Sileris**, Head of European Cybercrime Centre (EC3), **Europol**
- **Tonu Tammer**, Executive Director of CERT-EE, **Information System Authority, Estonia**
- **Heiko Lohr**, Head of Cybercrime Sub-Directorate, **Federal Criminal Police Office (BKA), Germany**
- **Colonel Michele Turi**, Director, **NATO Modelling and Simulation Centre of Excellence**
- **Gudmundur Arnar Sigmundsson**, Director, CERT-IS, **Electronic Communications Office, Iceland**
- **Marc Henauer**, Head of Unit, OIC MELANI, **Federal Intelligence Service, Switzerland**
- **Neil Walsh**, Chief of Cybercrime, Anti-Money Laundering and Counter Financing of Terrorism Department, **United Nations Office on Drugs and Crime (UNODC)**
- **Dana Toren**, Head of Cyber Defense Center, **National Cyber Directorate, Israel**
- **Blerim Krasniqi**, Head of IT Forensics, **Kosovo Agency of Forensics**
- **Juhani Eronen**, Chief Specialist, **National Cyber Security Centre, Finland**
- **Eirik Tronnes Hansen**, Prosecutor, Cybercrime section, **National Criminal Investigation Service, Norway**
- **Kadri Kaska**, Law and Policy Researcher, **NATO Cooperative Cyber Defence Centre of Excellence**
- **Professor Mugavero**, President, **OSDIFE**

Sponsors and Exhibitors



Pre-Event Workshop – 1st March 2022

08.30 – 17.00

INTRODUCTION TO DATA INTELLIGENCE THROUGH OPEN AND CLOSED SOURCES

Hosted By: Raoul Chiesa, Founding Partner and President, Security Brokers

For more information visit – www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com | Tel: +44(0)1582 346706

INTELLIGENCE-SEC

EVENT SCHEDULE

Tuesday 1st March 2022

08.30 – 17.00

INTERACTIVE WORKSHOP

Introduction to Data Intelligence through Open and Closed Sources

Hosted By:

Raoul Chiesa, Founding Partner and President, Security Brokers

Wednesday 2nd March 2022

08.30 – 17.10

CONFERENCE AND EXHIBITION DAY 1

Conference Topics

Cyber Security Focus – Nordics

European focus on cybercrimes – Threats, Trends, Regulations and Laws

European Union Cyber Strategies and Policies

Thursday 3rd March 2022

08.30 – 16.30

CONFERENCE AND EXHIBITION DAY 2

Conference Topics

Military - Cyber Defence and Future Threat Preparedness

Cyber Threat Intelligence and Developments

National Cyber Security Programs and cybercrimes faced

Protecting Critical Infrastructure from cyber-attacks

For more information visit – www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com | Tel: +44(0)1582 346706

INTELLIGENCE-SEC

WORKSHOP AGENDA

Introduction to Data Intelligence through Open and Closed Sources

Time

08.30 – 17.00

Overview

This course exposes the key concepts for those who look out for the first time in the world of Intelligence and specifically the OSINT (Open Source Intelligence) and CSINT (Closed Source Intelligence), addressing the audience about which methodology, and correct approaches should be used when dealing with such topics.

Course goal is to provide you with a basic, thus **practical knowledge** about the world of *data intelligence*, related disciplines, and then focus on the analysis of information sources, and its practical applications.

Target Audience

CISOs, CSOs, CTOs, HR Heads and staff, Marketing and Communication Managers, Intelligence Analysts, Law Enforcement Officers, System and Network Administrators, Counter Fraud Officers, DPOs, Cyber Investigators, Auditors, GRC Unit Directors and/or Compliance Officers, Legal Department staff and Attorneys, Due Diligence Units, Penetration Testers, as well as Recruiters and Head Hunters, Journalists, Influencers, Private investigators.

Agenda

- 8.30 *Workshop registration opening, NDA signing & Welcome coffee*
- 8.45 General introductions, Day schedule and Rules of Engagement of the workshop
- 9.00 Tools download, installation and setup on participants' own laptops (Trainer and Proctor will provide technical support if needed)
- 9.30 Start of morning session part I
- 11.00 *Coffee break*
- 11.30 Morning session part II
- 13.00 *Lunch break*
- 14.00 Afternoon session part I
- 15.30 *Coffee break*
- 16.00 OSINT teams setup & Start of missions's challenge
- 16.30 End of missions, OSINT Report team's briefings
- 17.00 Winner's Teams prizegiving, Delivery of individual Certificates and Group photo

Workshop Host

Mr. Raoul Chiesa
Founding Partner and President
Security Brokers

For more information visit – www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com | Tel: +44(0)1582 346706

EVENT PROGRAMME DAY 1

08.30 Registration and Networking

09.00 **CHAIRMAN'S OPENING REMARKS**
Professor Mugavero, President, OSDIFE

CYBER SECURITY FOCUS – NORDICS

09.10 **NORWEGIAN CYBER SECURITY STRATEGY AND ROADMAP**

- Current cyber security program in place
- Coordinating cyber security across the civilian sector
- Current cyber security roadmap

Robin Bakke, Director, Cyber Security, Department for Public Security, Ministry of Justice and Public Security, Norway

THREATLOCKER

09.40 **THREATLOCKER PRESENTATION**
Senior Representative, ThreatLocker

10.10 Networking Coffee Break

10.40 **CURRENT CYBER SECURITY CAPABILITIES – NORWAY PERSPECTIVE**

- Role of the National Cyber Security Centre
 - Current cyber security threats seen to Norwegian critical infrastructure
 - Current cyber security capabilities of the Norwegian Government
 - Inter-agency approach to combating cyber-threats
- Bente Hoff, Head, National Cyber Security Centre, Norway

Eclectiq Intelligence at the core

11.10 **CASE STUDY: NATIONAL CERT'S COLLABORATIVE CTI SHARING COMMUNITY**

- Improving workflow of threat data analysis and processing
- Reducing false positives through higher quality and confidence of threat data
- Establishing fast automatic sharing of higher quality of threat data

Karen Sundermann, Vice President Government Sector, Eclectiq

11.40 **CYBER SECURITY THREATS FACED IN ESTONIA**

- Role of the CERT in response to cyber threats
- Current cyber defence capabilities
- Threats and cyber-attacks being faced in Estonia
- What is needed next?

Tonu Tammer, Executive Director of CERT-EE, Information System Authority, Estonia

12.10 **CYBER SECURITY THREATS FACED IN FINLAND AND ACROSS THE NORDICS**

- Current cyber security capabilities in Finland
- International threats faced to Finnish critical infrastructures
- Cooperation in assisting neighbouring nations to combating cybercrimes

Juhani Eronen, Chief Specialist, National Cyber Security Centre, Finland

12.40 Networking Lunch Break

13.40 **CYBER INVESTIGATIONS AND PROSECUTIONS – NORWEGIAN PERSPECTIVE**

- Overview of the current cyber laws in Norway
 - What are the limitations?
 - Where are the loop holes?
 - Cyber Intelligence techniques used in Norway
 - Regional collaboration on cyber law and intelligence
- Eirik Tronnes Hansen, Prosecutor, Cybercrime section, National Criminal Investigation Service, Norway

EUROPEAN FOCUS ON CYBERCRIMES – THREATS, TRENDS, REGULATIONS AND LAWS



14.10 **PRODAFT PRESENTATION**
Koryak Uzan, Co-Founder and COO, Prodaft

14.40 **CURRENT RANSOMWARE INVESTIGATIONS IN NORWAY**

- Overview of the investigations into Ransomware attacks seen in Norway
- The LockerGoga case study
- What lessons have been learnt?

Knut Jostein Satnan, Police Prosecutor, National Criminal Investigation Service, Norway



15.10 **TACTICAL CYBER, LOCATION & WEB INTELLIGENCE (WEBINT): GATHERING ACTIONABLE INTELLIGENCE VIA A POWERFUL AND HOLISTIC INTELLIGENCE PLATFORM**

Senior Representative, Cobwebs Technologies

15.40 Networking Coffee Break

16.10 **CYBERCRIME TRENDS SEEN DURING THE PANDEMIC**

- Current Europol cybercrime operations
- Cybercrimes seen over the past year due to the COVID pandemic
- New threats to European infrastructures
- Lessons learnt over the past year

Edvardas Sileris, Head of European Cybercrime Centre (EC3), Europol

16.40 **TRENDS IN INTERNATIONAL LAW FOR CYBERSPACE**

- 'International law applies in cyberspace': now what?
- Emerging state responses to malicious cyber activities
- Promoting norms of responsible behaviour
- Shift in approach to industry regulation
- Where will we be in 5 years?

Kadri Kaska, Law and Policy Researcher, NATO Cooperative Cyber Defence Centre of Excellence

17.10 **CHAIRMAN'S CLOSING REMARKS**
Professor Mugavero, President, OSDIFE

For more information visit – www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com | Tel: +44(0)1582 346706

INTELLIGENCE-SEC

EVENT PROGRAMME DAY 2

08.30 Registration and Networking

09.00 CHAIRMAN'S OPENING REMARKS

Professor Mugavero, President, OSDIFE

MILITARY - CYBER DEFENCE AND FUTURE THREAT PREPAREDNESS

09.10 CYBER DEFENCE CAPABILITIES AND PREPAREDNESS – NORWEGIAN ARMED FORCES

- Overview of the Cyber Defence Force
- Current cyber defence capabilities
- Cyber warfare and simulations
- Response to a cyber-attack

Major General Inge Kampenes, Commander, Cyber Defence, Norwegian Armed Forces

THREATLOCKER

09.40 THREATLOCKER PRESENTATION

Senior Representative, ThreatLocker

Eclectiq

Intelligence
at the core

10.10 ECLECTIQ LIVE DEMONSTRATION

Details coming shortly

10.30 Networking Coffee Break

11.00 EMERGING CYBER TERRORISM THREATS

- NATO stance on cyber security and defence
- Current trends in the cyber threats faced to NATO member states
- Importance of response and preparedness
- What is needed next?

David van Weel, Assistant Secretary General, Emerging Security Challenges, NATO

11.30 CYBER WARFARE SIMULATION DEVELOPMENTS

- Overview of the NATO Modelling and Simulation Centre of Excellence
 - Current cyber warfare techniques
 - What is being developed?
 - Training to military officials on cyber terrorism and threats
- Colonel Michele Turi, Director, NATO Modelling and Simulation Centre of Excellence

CYBER THREAT INTELLIGENCE AND DEVELOPMENTS

12.00 PANEL DISCUSSION CYBER THREAT INTELLIGENCE – FUTURE CYBER THREATS AND DEVELOPMENTS

This panel discussion will discuss the latest intelligence sharing across Europe to combat cyber-threats against critical infrastructures as well as reviewing future cyber threats since the global pandemic

Moderated by:

- Professor Mugavero, President, OSDIFE

Panellists:

- Rear Admiral Davide Berna, Commander, Joint Intelligence Centre, Ministry of Defence, Italy
- Brigadier General Anton Rog, Head, National Cyberint Center, Romanian Intelligence Service (SRI)
- Thomas Lund-Sorensen, Director, Centre for Cyber Centre, Defence Intelligence Service, Denmark
- Marc Henauer, Head of Unit, OIC MELANI, Federal Intelligence Service, Switzerland

13.00 Networking Lunch Break

NATIONAL CYBER SECURITY PROGRAMS AND CYBERCRIMES FACED

14.00 NATIONAL CYBER SECURITY PROGRAMS AND STRATEGIES – ISRAEL PERSPECTIVE

- Overview of the National Cyber Directorate of Israel
- Current cyber security strategy and roadmap
- Cyber security programs
- What is needed?

Dana Toren, Head of Cyber Defense Center, National Cyber Directorate, Israel

14.30 CYBERCRIMES – GERMAN PERSPECTIVE

- Current cybercrimes faced across Germany
- Cooperation with the Austrian and Swiss Governments
- Case studies of recent cybercrimes
- Developments for the future

Heiko Lohr, Head of Cybercrime Sub-Directorate, Federal Criminal Police Office (BKA), Germany

15.00 Networking Coffee Break

15.30 CYBER RELATED CRIMES IN KOSOVO

- Monitoring internet activities to combat any extremism
- Current technologies used in monitoring computer systems
- Case studies of cyber threats
- Lessons learnt

Blerim Krasniqi, Head of IT Forensics, Kosovo Agency of Forensics

16.00 MONITORING CRITICAL ELECTRONIC COMMUNICATIONS

- Current cyber security in place to protect electronic communications across Iceland
- Monitoring the threats and response to any breaches
- Threats being seen to critical infrastructures in Iceland
- What is needed?

Gudmundur Arnar Sigmundsson, Director, CERT-IS, Electronic Communications Office, Iceland

16.30 CHAIRMAN'S CLOSING REMARKS

Professor Mugavero, President, OSDIFE

For more information visit – www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com | Tel: +44(0)1582 346706

INTELLIGENCE-SEC

SPONSORS AND EXHIBITORS

THREATLOCKER

ThreatLocker® is a global cybersecurity leader, providing enterprise-level cybersecurity tools for the MSP industry to improve the security of servers and endpoints. ThreatLocker's combined Application Whitelisting, Ringfencing™, Storage Control and Elevation Control solutions are leading the cybersecurity market towards a more secure approach of blocking unknown application vulnerabilities.



Cobwebs is an award-winning global leader in Web Intelligence, Cyber and Open-Source Intelligence Solutions for government agencies.

Powered by advanced intelligence collection capabilities and Artificial Intelligence (AI) algorithms, Cobwebs' solutions provide simple yet sophisticated methods to passively search, collect, analyze and monitor data from the Open Web, SNS, Deep Web and Darknet and actively develop investigations via unique Social Engineering tools.

Cobwebs' solutions are tailored to the operational needs of national security agencies and successfully deployed in multiple countries and agencies across Europe, Asia and the US.

Cobwebs exclusive technology extracts targeted intelligence from big data using the latest machine learning algorithms, automatically generating intelligent insights and exposing new leads.

The logo for EclecticIQ consists of the word "EclecticIQ" in a white, bold, sans-serif font, set against a black rectangular background.

The logo for "Intelligence at the core" features the text "Intelligence at the core" in a black, sans-serif font, centered within a yellow rectangular background.

EclecticIQ is a global provider of threat intelligence, hunting and response technology and services.

Stay ahead of rapidly evolving threats and outmaneuver your adversaries by embedding Intelligence at the core™ of your cyberdefenses with our open and extensible cybersecurity platform and ecosystem.

The most targeted organizations in the world – including governments and large enterprises – use our platform to operationalize threat intelligence, enable threat hunting, detection and response, and accelerate collaboration.

Founded in 2014, EclecticIQ is a leading European cybersecurity vendor operating worldwide with offices and teams across Europe and UK, North America, India and via value-add partners. www.eclecticiq.com



PRODAFT is a pioneering company in the threat intelligence industry having its headquarters in Switzerland.

Today's security professionals face a constant flood of "partially reliable" threat alerts and notifications from multiple vendors. The non-stop flow of unverified alerts creates an extremely demanding workload for security teams.

PRODAFT's threat intelligence platform reduces the time and energy spent on analysis, interpretation, and verification of potential threats. It gives security operatives on-demand insight into threat profiles on an individual basis. Every day hundreds of companies from critical sectors use PRODAFT's solutions to receive actionable insights right from the source.

PRODAFT had published numerous threat intelligence reports publicly regarding high-end cybercrime groups such as Fin7/Carbanak, Silverfish, Conti, LockBit, FluBot, and prevented thousands of breaches globally.

www.prodaft.com

For more information visit – www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com | Tel: +44(0)1582 346706

INTELLIGENCE-SEC

SUPPORTING PARTNERS



The Observatory on Security and CBRNe Defence - Osdife is a national and international reference for researchers and specialists in these fields and, for that, it contributes to experience enhancement, development and sharing by means of study, analysis, research, education, training, workshops, symposium and publications, also involving public and private institutions, agencies, organizations, associations, companies and individuals, in order to promote and encourage the development and adoption of appropriate strategies and initiatives for risks reduction and mitigation, to ensure citizens security and safety and to guarantee the integrity, defence and protection of public and private assets, territory, infrastructure and cultural heritage also in the field of CBRNe Risk and WMD Proliferation



The Department of Electronic Engineering (DIE) of University of Rome "Tor Vergata" was founded in 1983 and now counts about 150 people, including faculty, staff, and cooperating personnel. In terms of traditional scientific areas, the department's expertise lies in the disciplines of control theory, electronics, electrical engineering, measurements, optoelectronics, telecommunications but also safety, security, defence and intelligence. However, today research is typically carried out with multi-disciplinary approaches, dealing with specific application scenarios and systems. In this since the beginning, many of the DIE teachings and research activities have had the aim to develop, deepen and promote national and international scientific and technical education, studies and researches in the field of Territorial Protection, Safety, Security and Intelligence. In particular the Research Area "Security and Defence" offers expertise in the following sectors: Homeland Security, Military Defence, Civil Defence, Civil Protection, CBRNe Risk and WMD Counterproliferation.



The "Center for Security Training and Education" (CUFS) of state University of Republic of San Marino is born in 2010 moving from an approach centered on scientific research and training to an approach oriented to the application of the discipline and to the solving of problems connected to the security area.

Starting from this first phase, the CUFS, thanks to the several professionals and skills which have been improved through years, today is an international Center of Excellence for analysis, dissemination, innovation and growing of sciences in the field of security, defence, intelligence and territorial risk. This achievement has been also possible thanks to the activities of design, development and promotion of studies, research, dissemination, networking, education and training. These activities have the objective to address and support the know-how's growth and innovation in methodologies and technologies of public and private Institutes and Organizations operating in the area of Security Defence & Intelligence. Moreover, the very same activities are applied also to specialists, technicians, experts, professionals and researchers such as to everyone who is interested in these issues.

For more information visit – www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com | Tel: +44(0)1582 346706

INTELLIGENCE-SEC

CYBER INTELLIGENCE EUROPE 2022

1st – 3rd March 2022 – Oslo, Norway

DELEGATE BOOKING FORM

DELEGATE DETAILS: Please complete your details below.				
Title/Rank:	Please Tick	Military/Govt. Public Sector Rate	Early Bird Price (book before 31st Dec 2021)	Standard Price
First Name:		Two Day Conference & Exhibition	€400	€500
Surname:		Workshop	€100	€150
Job Title:		All of the Above	€500	€650
Company:	Please Tick	Private Sector Rate	Early Bird Price (book before 31st Dec 2021)	Standard Price
Tel:		Two Day Conference & Exhibition	€800	€1,000
Fax:		Workshop	€200	€300
Email:		All of the Above	€1,000	€1,300
Address:				
PAYMENT DETAILS: Please complete your details below.				
Signature:	<input type="checkbox"/> Wire Transfer: Barclays, 16 High Street North, Dunstable, Bedfordshire, LU6 1JZ, United Kingdom Sort Code: 20 55 33 Account Number: 53554104			
Date:	<input type="checkbox"/> PayPal We will send you a PayPal Request for you to make payment with your credit card. You do not need a PayPal Account to make payment this way.			
VENUE & ACCOMMODATION				
Hotel Name: Radisson Blu Hotel Scandinavia Oslo Holbergsgate 30, NO-0166 Oslo, Norway				
Please tick here if you would us to contact you to book your accommodation <input type="checkbox"/>				
DATA PROTECTION				
Please tick the box below if you are happy for us to share your email address with the event sponsors and exhibitors post event. I am happy for you to share my email address with the sponsors/exhibitors <input type="checkbox"/>				
ADDITIONAL NOTES				
<p>Payments - All bookings made prior to the conference must be paid in full to guarantee registration. Once payment has been received, an email confirmation and a receipted invoice will be sent. If payment is not made at the time of booking, registration will be provisional. Bookings received less than two weeks before the conference date can only be paid by credit card.</p> <p>Early Bird Rate - In order to qualify for any 'early bird' rates, booking must be received before the deadline date listed in the conference marketing material.</p> <p>Substitutions & Cancellations - Delegates may nominate an alternative person from their organisation to attend up to 24 hours prior to the start of the event, at no extra charge. Should substitution not be possible, cancellation charges apply as follows: 8 weeks or more prior to start of event: 10% of the delegate fee, 4 to 8 weeks prior to start of event: 50% of the delegate fee, 4 weeks or less prior to start of event: 100% of the delegate fee. All substitutions and cancellations must be received in writing</p> <p>Access Requirements - Delegates should advise of any special access requirements at the time of registration.</p> <p>Registration Information - Registration information will be sent to registered delegates by email at least seven days prior to the event. Any delegate not receiving the registration information should contact us by email to events@intelligence-sec.com</p> <p>Alterations to Programme - Cancellation/Postponement of Event - Intelligence-Sec reserves the right to make alterations to the conference programme, venue and timings.</p> <p>In the unlikely event of the programme being cancelled by Intelligence-Sec, a full refund will be made. Liability will be limited to the amount of the fee paid by the delegate. In the event of it being found necessary, for whatever reason, that the conference is being postponed or the dates being changed, the organisers shall not be liable for any expenditure, damage or loss incurred by the delegate. If by re-arrangement or postponement the event can take place, the booking between the delegate and the organisers shall remain in force and will be subject to the cancellation schedule in paragraph 3</p> <p>Speakers - Views expressed by speakers are their own. Intelligence-Sec cannot accept liability for advice given, or views expressed, by any speaker at the conference or in any material provided to delegates.</p> <p>Photography & Filming - For promotional purposes, there may be a professional photographer and video production taking place during the conference. Delegates who do not wish to be filmed or recorded should advise the organisers by email to events@intelligence-sec.com prior to the event.</p> <p>Data Protection - By submitting registration details, delegates agree to allow Intelligence-Sec and companies associated with the conference to contact them regarding their services. Delegates who do not wish to receive such communications please email events@intelligence-sec.com. The contact details of registered delegates will be placed on the attendee list which will be passed to sponsoring companies and to all attendees for them to see who is at the conference for the purpose of networking and meetings. Delegates who do not wish to be included on this list should advise at the time of booking.</p> <p>Websites & Links - The conference and associated Intelligence-Sec websites may link to other websites and networking tools provided for the convenience of the users. The contents of these websites are maintained by their owners, for which Intelligence-Sec takes no responsibility. Neither can responsibility be taken for contents of any website linking to this website.</p> <p>Insurance - It is the responsibility of the delegate to arrange appropriate insurance cover in connection with their attendance at the conference. Intelligence-Sec cannot be held liable for any loss, liability or damage to personal property. If you have any questions about these Terms & Conditions, please contact – events@intelligence-sec.com</p>				

For more information visit – www.intelligence-sec.com