**ISS World Europe** is the world's largest gathering of Regional Law Enforcement, Intelligence and Homeland Security Analysts as well as Telecom Operators responsible for Cyber Defense, Electronic Surveillance and Network Intelligence Gathering.

ISS World Programs present the methodologies and tools for Law Enforcement, Public Safety and Government Intelligence Communities in the fight against drug trafficking, cyber money laundering, human trafficking, terrorism and other criminal activities conducted over today's telecommunications network and the Internet.

Track 1: **Lawful Interception and Criminal Investigation Training**
Track 2: **OSINT Automation for Cyber Defense and Threat Detection**
Track 3: **Bitcoin and Dark Web Investigations**
Track 4: **Defeating Encryption with IT Intrusion**
Track 5: **LEA, Defense and Intelligence Analyst Product Demonstrations**
Track 6: **Social Network Monitoring and Big Data Analytics Product Demonstrations**
Track 7: **Mobile Signal Intercept and Electronic Surveillance Product Demonstrations**
Track 8: **Information Security and Defense with Quantum Safe Cryptography**

**Plus Special Training Seminars lead by Law Enforcement Officers and Ph.D. Computer Scientist**

---

**ISS World Agenda From 2017 ISS World Europe Program**

**ISS World Europe 2018**
**Agenda and Registration Link**
**Available March 2018**

---

# Training Seminars Led by Law Enforcment Officers and Ph.D Computer Scientists

## Tuesday, 13 June 2017

### Seminar #1
### 09:00-17:15

## Online Social Media and Internet Investigations

Presented by: *Charles Cohen,* ***Cohen Training and Consulting, LLC*** *Charles Cohen also holds the position of Captain, Office of Intelligence & Investigative Technologies,* ***Indiana State Police, USA***

09:00-10:00

**Understanding Cell Handset Geolocation: What Investigators Need to Know**

10:15-11:15

**Open Source Intelligence (OSINT) Collection Tools:  Creating an Inexpensive OSINT Toolbox**

11:30-12:30

**Metadata Exploitation in Criminal Investigations**

13:45-14:45

**Conducting Covert Online Observation and Infiltration Activities: Challenges and Opportunities for Investigators**

15:00-16:00

**Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators**

16:15-17:15

**Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators (continued)**

## Seminar #2
## 9:00-17:15

## Practitioners Guide to Internet Investigations

Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***

The aim of this 1 day seminar is to take the attendees from the basics of understanding the Internet, how to find data, through to a full understanding of best practice of an Internet investigator, having awareness and knowledge of all the tools available to achieve this. It is aimed primarily at the investigator, delivered from the perspective of detective, to empower them to have the best methodology and tradecraft to profile and catch suspects.

This is exclusively Law Enforcement only, as Practical examples, covert and investigative methodology and tradecraft will be given throughout the seminar.

09:00-10:00

**The Internet, and how suspects leave a Digital Footprint**

10:15-11:15

**Recognizing Traffic Data and digital profiling**

11:30-12:30

**WIFI, geolocation, and Mobile Data traces**

13:45-14:45

**Awareness of Emerging Technologies, Masking Tech and Tools, TOR and proxies**

15:00-16:00

**Advanced Techniques in Tracing Suspects, and lateral problem solving**

16:15- 17:15

**Open Source Tools, resources and techniques**

## Seminar #3
## 9:00-12:30

## Understanding ISS Technologies and Products Deployed in Telecommunications Networks for Lawful Interception and Mass Surveillance

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies***

This half-day seminar covers how criminals and terrorists communicate over today's public telecommunications wireline and wireless networks, over the top Internet services and social networks. This seminar is ideal for law enforcement, interior security, public safety and others who need to understand the ISS technologies and products used to lawfully intercept electronic communications and conduct mass network surveillance as discussed at ISS World Conference sessions and by exhibitors.

9:00-10:00

**Introduction to Wireline and IP Infrastructure and Related ISS Products for Lawful Interception and Mass Surveillance**

10:15-11:15

**Understanding Mobile Wireless Infrastructure, and Related ISS Products for Lawful Interception and Mass Surveillance**

11:30-12:30

**Understanding the Internet Over-the-Top (OTT) Services and Related ISS Products for Mass Intelligence Gathering and Surveillance**

## Seminar #4
## 13:45 -14:45

## SS7 Vulnerabilities and Intercept Options

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies*** *and a* ***Distinguished Telecom Technology Expert to be announced***

There are two very important aspects of telco SS7 infrastructure law enforcement and inteior security needs to understand. For law enforcement: you can locate and track a target anywhere in the world if they just turn on their cell phone. For Interior Security: large scale distributed denial of service attacks over SS7 can completely take down today's telecom networks.

## Seminar #5
## 15:00-16:00

## Intercept Implications of 4G/5G Diameter Signaling Replacing SS7

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies*** *and a* ***Distinguished Telecom Technology Expert to be announced***

As telecom service providers transition to IP based VoLTE and introduce 5G, SS7 will be replaced with diameter signaling. This session provides the technical basics of diameter, options for transitioning SS7 to diameter and the new challenges facing law enforcement.

## Seminar #6
## 16:15-17:15

## The Implications of multi-IMSI and OTA for Law Enforcement and the Government Intelligence Community

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies*** *and a* ***Distinguished Telecom Technology Expert to be announced***

The era of SIM Cards with static IMSIs issued by cellular operators is changing. Deployment of multi-IMSI as well as network programmable (OTA) SIM cards will create new challenges for law enforcement. This session looks at the implications of multi-SIM and OTA for LEAs and Intel analysts.

## Seminar #7
## 13:45-14:45

## Investigation Techniques for Unmasking TOR Hidden Services and Other Dark Web Operations

Presented by: *Matthew Lucas, (Ph.D Computer Science), VP,* ***TeleStrategies***

TOR networks are notoriously effective at hiding the online identity of criminals, terrorists and others who are up to no good. The other side that receives less attention are TOR hidden services. These are services that leverage TOR's anonymizing capabilities to mask the identity of criminally-

hosted online services - forming the basis of just about all illegal gambling sites, drug markets, child exploitation material, firearm sales, terrorism propaganda, and more.

## Seminar #8
## 15:00-16:00

## Defeating Network Encryption: What Law Enforcement and The Intelligence Community Needs to Understand

Presented by: *Dr. Matthew Lucas (Ph.D Computer Science), Vice President,* ***TeleStrategies***
The starting point to defeating encryption is to separate techniques addressing stored encrypted data such as with the Apple iPhone issue. The other challenge is defeating encrypted data in transit (e.g. Telegram, Whatsapp, etc.) or Network Encryption. This webinar is about defeating the later. When it comes to defeating network encryption the technical community separates into two camps. Those who want to impede law enforcement and the government intelligence community from defeating network encryption: IETF, Silicon Valley and hundreds of third party encryption services. And your camp, those who want to investigate criminals and terrorist group who depend on network encryption.

## Seminar #9
## 16:15-17:15

## Bitcoin Interception Experience

Presented by: *Vladimir Vesely, Researcher, FIT-BUT,* ***Brno University of Technology***
This session surveys interception options of the Bitcoin network. Namely, it investigates what kind of data may be collected from intercepted traffic of Bitcoin clients, miners and relevant services (online wallets, exchanges, payment gateways). Moreover, two real-life use-cases (involving Bitcoin fraud and ransomware) are presented together with the used methodologies.

## Wednesday, 14 June 2017

## Seminar #10
## 9:00-10:00

## Bitcoin 101: Introduction to What Technical Investigators Need to Know about Bitcoin Transactions, Dark Web Commerce and Blockchain Analysis

Presented by: *Dr. Matthew Lucas, Vice President,* ***TeleStrategies***

This 101 training seminar is an introduction to Bitcoin, how the system is used to support criminal activities (e.g. Dark Web) and why technical investigators need to understand the basic Bitcoin transaction mechanism (Blockchain) to successfully defeat 21st century criminals and terrorist actions. Specifically, this introduction to Bitcoin for technical investigators addresses:

## Seminar #11
## 9:00-10:00

## Quantum Computing and Defeating Encryption: Myths vs. Realities for Cyber Security Decision Makers

Presented by: *Jerry Lucas (PhD, Physics) President,* ***TeleStrategies***

The sole reason nation state governments are investing billiions of dollars in quantum computing development is to defeat today's crypto systems. On the otherhand the sole reason nation state governments as well as the venture capital community are investing in quantum safe cryptograph is to defeat quantum computers. If you have responsibilities for sifting through the myths and realities of quantum computing and/or quantum safe cryptography product readiness claims but don't have a degree in physics nor math, this webinar is for you.

## Seminar #12
## 12:00-12:30

## Cryptocurrency Miner Detection in your Organization's Network

Presented by: *Vladimir Vesely, FIT-BUT,* ***Brno University of Technology***

Ways to automatically detect cryptocurrency miners in computer network who are exploiting resources of their organization (usually free of charge electricity and reliable Internet connectivity comparing to households). Methodology on how to detect devices running mining software from the Netflow records. Running a web service which can tell you whether a given IP address is the mining pool/client or not.

## Seminar #13
## 16:45-17:45

## TLS/SSL Decryption Workshop

Presented by: *Vladimir Vesely, Researcher, FIT-BUT,* ***Bruno University of Technology***

The presentation introduces methods how to decrypt TLS/SSL connection. Focus is on man-in-middle attack employing TLS/SSL proxy and other ways how to obtain session's private keys.

Speaker will demonstrate how to decrypt intercepted traffic using open-source tools like Wireshark and NetFox Detective.

## Thursday, 15 June 2017

## Seminar #14
## 12:00-13:00

## Bitcoin Interception Experience

Presented by: *Vladimir Vesely, Researcher, FIT-BUT,* ***Brno University of Technology***
This session surveys interception options of the Bitcoin network. Namely, it investigates what kind of data may be collected from intercepted traffic of Bitcoin clients, miners and relevant services (online wallets, exchanges, payment gateways). Moreover, two real-life use-cases (involving Bitcoin fraud and ransomware) are presented together with the used methodologies.

## Seminar #15
## 12:00-13:00

## Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations

Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***

**PRE-CONFERENCE SESSIONS DESCRIPTION AT THE END OF AGENDA POSTING**

---

## Wednesday, 14 June 2017

# Welcoming Remarks

| | |
|---|---|
| 8:15-8:30 | *Tatiana Lucas, ISS World Program Director,* ***TeleStrategies*** |
| 8:30-9:00 | **Top Ten Internet Challenges Facing Law Enforcement and the Intelligence Community World Europe has Solutions**<br>*Dr. Jerry Lucas, President,* ***TeleStrategies*** |

---

## ISS World Europe Exhibit Hours:

**Wednesday, 14 June 2017**: 10:00 - 18:00

**Thursday, 15 June 2017**: 9:30 - 12:30

---

# Track 1: Lawful Interception and Criminal Investigation Training

This track is for Telecom Operators and Law Enforcement/Intelligence/Defense Analysts who are responsible for specifying or developing lawful intercept network infrastructure.

## Tuesday, 13 June 2017

11:30-12:00 **How-to simulate Cyber Kill Chain to challenge Forensic tools and Analysts**
*Christian Hirsch, System Engineer Wireless & Security,* ***IXIA***

12:00-12:30 **Perform your own world class traffic analytics with the leading DPI engine**
*Alexander Müller,* ***Rohde&Schwarz***

13:45-16:00 **LI/RD Standards Update**
*Gerald McQuaid, Chairman,* ***ETSI/TC LI***
*Alex Leadbeater, Chairman,* ***3GPP SA3LI***
*Carmine Rizzo,* ***ETSI***

16:15-17:15 **How to assure reliable and safe mediation between the network infrastructure and monitori**

Reliable and safe mediation of signalisation and collected information between network infrastruc centres is a must – but it is a challenging task. In the modern networks, which are serving voice ar communications and where the access can be fixed or mobile, there is a variety of different systen vendors of several generations. On the other side, the users at the monitoring centres are expecting stable interface for their daily work.

The presentation shows how to cope with these challenges, how to assure safe end-to-end path of without intrusion possibility and how to record all attempts to access the system. Universal end-to supporting variety of interfaces with integrated security mechanism is the answer to minimize the implementation time, optimize the maintenance costs and to assure extensions and enhancements

*Miro Udir, Solution Manager,* ***Iskratel***

## Wednesday, 14 June 2017

9:00-10:00 Session A **Current and Future Standardization Challenges: Encryption, Network Function Virtua Computing and More**
*Alex Leadbeater, Chairman, SA3 LI and EU Data Retention Compliance Manager,* ***BT***

9:00-9:30 Session B **Findings from Voice Biometrics deployments**
*Radim Kudla,* ***Phonexia***

| | |
|---|---|
| 11:30-12:00 Session A | **Lawful interception in modern and future Wireless Networks like 5G**<br>*Presented by **Utimaco TS GmbH*** |
| 11:30-12:00 Session B | **Analytics - Digital Investigative Platform Overview**<br>*Presented by **Cellebrite*** |
| 14:00-14:30 | **High-Speed NAT Logging**<br>*Presented by **Utimaco TS GmbH*** |
| 14:30-15:00 | **Advantages of Optical Transport Layer 1 Encryption**<br>*Presented by **STORDIS GmbH*** |
| 15:30-16:00 | **Digital Spread: a new era of ultra low power consumption audio transmitters**<br>*Presented by **DEM Solutions*** |
| 16:00-16:30 | **"Vitok-CLUSTER": NoSQL database intended for specialized processing of the inform high-speed communication channels.**<br>*Roman Khokhlov, Head of Information Security Department, **NORSI-TRANS*** |
| 16:45-17:15 | **Vlatacom Personal Crypto Devices for Voice, Text and File Encryption**<br>*Dr. Miroslav Peric, **Vlatacom Institute*** |

### Thursday, 15 June 2017

| | |
|---|---|
| 8:30-9:00 | **Perform your own world class traffic analytics with the leading DPI engine**<br>*Alexander Müller, **Rohde&Schwarz*** |
| 9:00-9:30 | **100% Signal Visibility within next generation communications networks**<br>*Presented by **Lumacron*** |
| 10:30-11:00 | **100GE Network Traffic Interception**<br>*Presented by **Netcope*** |
| 11:00-11:30 | **Implementing lambda architecture with Vitok-Cluster for real-time analytics and bat data mining queries.**<br>*Alexander Shtokhov, Project Manager, **NORSI-TRANS*** |

---

# Track 2: OSINT Automation Training for Cyber Threat Detection

This track is for Intelligence Analysts and Law Enforcement agents who have to "connect the dots" between people, places and other entities by searching through massive amounts of unstructured data from various sources using visual analytics, semantic technologies, data mining, OSINT and other intelligence gathering tools and techniques

### Tuesday, 13 June 2017

| | |
|---|---|
| 15:00-15:30 | **Handling Cyber crime Darkweb Automatic Analytics**<br>*Presented by **MER Group*** |

## Wednesday, 14 June 2017

9:00-9:30 **Generate powerful evidences from PCAP, CDR/IPDR and Social Media, all from a single in**

Agencies have to deal with variety of data like PCAP, CDR/IPDR and Open Source Data etc. coming fro

A typical investigation of such data involves manual correlation using different tools that eventually lea

intelligence and doesn't provide a single view of a "Person of Interest".

What if you could bring data, tools and systems together on a single interface?
Experience a seamless Investigation Workbench that assists investigators to collaboratively disco suspects, build stories and solve cases rapidly.

*Presented by **ClearTrail Technologies***

9:30-10:00 **Tovek Tools – building knowledge from multisource data**
*Presented by **TOVEK***

12:00-12:30 **Voice Biometrics and Speech Technologies. A whole new offering for Criminal ID and Intel**
*Presented by **Agnitio. Now part of Nuance***

14:00-14:30 **Untangling the Criminal Web Using Neo4j, World's Most Popular Graph Database**
*Presented by **Graph Aware***

14:30-15:00 **A Unique Collection of Internet-related Open Source Intelligence and How it can be Exploi**

You'll see a powerful collection of open source Internet intelligence data at work and see how so it to track cyber crime and enrich their existing tools to make sense of what is happening on the I investigations. If cyber investigation is now part of your workload, you're going to love this sessi lots of new ideas.

*Presented by **Packet Forensics***

15:30-16:00 **Safeguarding Yourself with a Modern Multi-Modal Data Platform**

Analytics of both new and legacy data for security, compliance, and privacy, requires a mix of cl hybrid solutions and advanced analytics. There's only one proven enterprise analytics platform th infrastructure agnostic, on-premises, off-premises and machine learning at scale including Text A seamlessly works with data in Hadoop, AWS S3, SAN, RDBMS and more in a proven industry s Pivotal Greenplum.

*Dave Kloc and Franck Sidi, Pivotal, **Dell EMC***

## Thursday, 15 June 2017

11:00-11:30 **Handling Multi-language OSINT & COMINT**

As agencies need for real-time information for quick decision making increases, they face terms of data collection and usage.

How can they handle the exponential amounts of foreign-language information collected f in different formats whereas they lack of linguistic skills and expertise?

This session will include live product demonstrations.

*Emmanuel Tonnelier, Director of Intelligence Solutions,* ***SYSTRAN***

---

# Track 3: Bitcoin and Dark Web Investigation Training

This track is for Criminal Investigators, Interior Security and Private Enterprise Investigators who have to understand Bitcoin, Blockchain, TOR and Dark Web Transactions

## Tuesday, 13 June 2017

16:15-17:15 **Bitcoin Interception Experience**

This session surveys interception options of the Bitcoin network. Namely, it investigates w be collected from intercepted traffic of Bitcoin clients, miners and relevant services (online payment gateways). Moreover, two real-life use-cases (involving Bitcoin fraud and ransom together with the used methodologies.

*Vladimir Vesely, FIT-BUT,* ***Brno University of Technology***

## Wednesday, 14 June 2017

9:00-10:00 **Bitcoin 101: Introduction to What Technical Investigators Need to Know about Bitcoin Tr Web Commerce and Blockchain Analysis**
*Dr. Matthew Lucas, Vice President,* ***TeleStrategies***

11:30-12:00 **Demystifying the Dark Web Through Automated Data Monitoring, Collection and Intellig**
*Avi Kasztan, CEO,* ***Sixgill***

12:00-12:30 **Cryptocurrency Miner Detection in your Organization's Network**

Ways to automatically detect cryptocurrency miners in computer network who are exploiting res organization (usually free of charge electricity and reliable Internet connectivity comparing to h Methodology on how to detect devices running mining software from the Netflow records. Runn which can tell you whether a given IP address is the mining pool/client or not.

*Vladimir Vesely, FIT-BUT,* ***Brno University of Technology***

17:15-17:45 **Bitcoin Hide and Seek:**
In depth analysis of the services used to prevent bitcoins tracking, with a focus on new decentral mixing systems, and technologies to counter them
*Presented by* ***Neutrino.nu***

## Thursday, 15 June 2017

10:30-11:30 **Bringing Transparency to Bitcoin transactions**

This presentation will outline the cutting edge analysis techniques that Chainalysis employs to clu addresses together and the different attribution strategies employed. Finally, using an example we typical path an investigation may follow to get to a real world person.

*Michael Gronager, CEO,* ***Chainalysis***

12:00-13:00 **Case Studies: Blockchain analysis in action**

A case study focused presentation outlining the major threat actors and the anonymization techniq step through some investigations outlining how to get leads in cases or look for corroborative evi step through some best practice when searching for Blockchain evidence, minimising the time wa investigation.

*Michael Gronager, CEO,* ***Chainalysis***

---

# Track 4: Defeating Encryption and IT Intrusion Product Training

This track is only open to Law Enforcement, Public Safety and Government Intelligence Community Attendees

## Tuesday, 13 June 2017

9:00-9:30 **Gaining Valuable Intelligence from Encrypted Communications**
*Uri Weil, Presale Team Leader, EMEA,* ***Verint***

9:30-10:00 **Mastering Your Web Intelligence Investigations by Shining Light on the Social and Dark W**
This session introduces a new version of the Verint Web Intelligence Center, an end-to-end Web analytics solution for open-source intelligence specialists. The system provides Web analysts wit platform and expert workflows through which they can accelerate their investigations, from case requests, big web-data analytics, and active Web Intelligence missions. The live demo simulates case in which the analyst examines the link between radical Islam terror attacks and charity funds information coming from social networks and the Dark Web.
*Adiel Horesh, Director of Business Development, Fusion and Web Intelligence Solutions,* ***Verint***

10:15-11:15 **FinFisher™: Hacking the Human Element**
*Presented by* ***FinFisher***

12:00-12:30 **Efficient Cryptanalysis Infrastructure - Doing more with less**
*Presented by* ***SciEngines***

13:45-14:45 **FinFisher™: Keeping up with the Pace - New Hacking Tools & Techniques for Practical Op**
*Presented by* ***FinFisher***

## Wednesday, 14 June 2017

| | |
|---|---|
| 9:00-9:30 | **Cyber Intelligence Solutions - Challenges and Opportunities**<br>*Presented by **Wintego*** |
| 11:30-12:00 | **Effective use of Malware in support of Investigations**<br>*Pavel Krcma Head of Malware Research, **Intecs GmbH*** |
| 14:00-15:00 | **FinFisher™: Cyber Solutions For The Fight Against Crime**<br>*Presented by **FinFisher*** |
| 16:45-17:45 | **TLS/SSL Decryption Workshop**<br>*Vladimir Vesely, Researcher, FIT-BUT, **Brno University of Technology*** |

### Thursday, 15 June 2017

| | |
|---|---|
| 8:30-9:30 | **New challenge Network Monitoring: IPv4 disambiguation and rich metadata SIGINT in th**<br>*Presented by **AREA*** |
| 10:30-11:30 | **How-to Verify, Optimize and Improve SSL Decryption and Internet Data Interception (Liv**<br>*Phil Trainor, Security & Test Sales Director, **IXIA*** |
| 12:00-13:00 | **Accelerated Password Cracking using GPU Cards**<br>The lecture would summarize password-cracking use-cases and employed formats, current GPU existing (non)-commercial cracking tools. Moreover, we have developed three interesting open-s password cracker employing OpenCL; b) controller of distributed cracking task for both our crac used Hashcat; c) hardware platform delivering the same performance comparing to industry solut of their price.<br>*Vladimir Vesely, Researcher, FIT-BUT, **Brno University of Technology*** |

---

# Track 5: LEA, Defense and Intelligence Analyst Training and Product Demonstrations

This training is only open to Law Enforcement, Public Safety and Government Intelligence Community Attendees.

### Tuesday, 13 June 2017

| | |
|---|---|
| 9:00-17:15<br>Session A | **Practitioners Guide to Internet Investigations**<br>*Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement, **U*** |
| 9:00-10:00<br>Session B | **Speech processing technologies for OSINT and COMINT**<br>*Presented by **Vocapia Research*** |
| 10:15-11:15 | **Case Management Platform based on artificial intelligence technology**<br>*Massimiliano Romeo, Marketing & Sales Director, **Cy4Gate S.r.l.*** |
| 11:30-12:00 | **How tactical sensing devices can provide a value add for SIGINT intercept and qual**<br>*Presented by **Group 2000 Nederland B.V.*** |

| | |
|---|---|
| 13:45-14:45 | **Lawful Interception in 2017. VoLTE and encrypted services like Facebook, Gmail a new approach to the IP investigation**<br>*Presented by **IPS*** |
| 15:00-16:00 | **How to Render the Ultimate Intelligence Gathering Tool Useless**<br>*Presented by **Kaymera*** |
| 16:15-17:15 | **International Optic Fiber Analysis: Signals, Protocols, Metadata and Content all in**<br>*Presented by **VASTech*** |

## Wednesday, 14 June 2017

| | |
|---|---|
| 9:00-10:00 | **LIVE DEMO: Face & Voice recognition to identify people in video surveillance, phon media**<br>*Presented by **ATIS systems*** |
| 11:30-12:00 | **How to quickly and efficiently identify suspects - Live demonstration analyzing compl from multiple Monitoring Centers**<br>*Presented by **trovicor*** |
| 12:00-12:30 | **Real-time target location tracking - Live demonstration detailing how to generate inte location information**<br>*Presented by **trovicor*** |
| 12:00-12:30<br>Session B | **Data Fusion and Analytics for National Security and Intelligence**<br>*Lee Holmes, **Yaana Technologies*** |
| 14:00-15:00<br>Session A | **Tracking Location and calls of foreign nationals through the use of a passive strategic system**<br>*Presented by **VASTech*** |
| 14:00-15:00<br>Session B | **Big Data and Machine Learning for Intelligence: Cerebro NG**<br>*Presented by **Advanced Systems*** |
| 14:00-15:00<br>Session C | **Hushmeeting: creating an iron-clad and quantum-safe communication environment.**<br>Preventing attacks, detecting intruders and collaborating within a backdoor-free and malwa communication framework. Real use cases and attacking scenarios.<br>*Presented by **Feedback Italia s.r.l.*** |
| 15:30-16:30<br>Session A | **Internet Records Intelligence: Collection, Storage, Disclosure and Analysis**<br>*Curt Schwaderer, **Yaana Technologies*** |
| 15:30-16:00<br>Session B | **Advanced Intelligence Solutions for Monitoring the Illegal Immigration Influx in Eur**<br>The recent influx of illegal and undetected immigration into European countries has created security reality, which cannot be managed with the tools of yesterday.<br>This presentation showcases some of the most advanced intelligence approaches and techno effectively address and tackle this growing challenge.<br>*Moshe Samocha, Marketing Director, **Verint*** |
| 15:30-16:00<br>Session C | **Virtual ISP – ISP independent Inline Interception Capabilities**<br>*Presented by **RayZone Group*** |
| 16:00-16:30<br>Session B | **Demonstrating the Art of Counter Terrorism - Mass Investigation Scenario For Natio Organizations** |

While security organizations are using technology – the terrorists are exploiting it. Being di
information and more clues and many more suspects.
In this session, we will see how to use actionable intelligence to create a list of suspects and
right ones.
*Moshe Samocha, Marketing Director,* ***Verint***

16:00-16:30 Session C — **Smartphones users next generation strategic intelligence gathering system**
*Presented by* ***RayZone Group***

16:45-17:15 Session A — **Active Interception on LTE/5G**
*Curt Schwaderer,* ***Yaana Technologies***

16:45-17:15 Session B — **SDN Delivers Services Differentiation**
*Presented by* ***STORDIS GmbH***

16:45-17:45 Session C — **Putting together forensic puzzles using PathFinder - comprehensive business analytics**
*Egor Ivanov, Head of Department,* ***BaltInfoCom LLC***

17:15-17:45 Session A — **Bulk Geolocation: Finding the Unknown Actors**
*Dave Grootwassink,* ***Yaana Technologies***

## Thursday, 15 June 2017

8:30-9:30 Session A — **Generate powerful evidences from PCAP, CDR/IPDR and Social Media, all from a single**

Agencies have to deal with variety of data like PCAP, CDR/IPDR and Open Source Data etc. coming f

A typical investigation of such data involves manual correlation using different tools that eventually l

intelligence and doesn't provide a single view of a "Person of Interest".

What if you could bring data, tools and systems together on a single interface?
Experience a seamless Investigation Workbench that assists investigators to collaboratively dis
profile suspects, build stories and solve cases rapidly.

*Presented by* ***ClearTrail Technologies***

8:30-9:30 Session B — **Next generation LI-MC: extracting intelligence from Meta-Data with easy-to use DPI and capabilities in a unique platform.**
*Presented by* ***RCS S.p.A.***

10:30-11:00 Session B — **How to uncover patterns in communication - Live demonstration on utilizing email analys corruption**
*Presented by* ***trovicor***

10:30-11:30 Session C — **GoldenSpear Int Fusion Centre – Combining WEBINT, Cyber collection, and Tactical In holistic target profiles**
*Presented by* ***S2T***

12:00-12:30 Session A — **Connecting the Dots for a Coherent Intelligence Picture - Target Investigation Scenario f Enforcement Organizations**
While you are searching, they are planning; while you are pursuing, they are hiding. In this sess
how Actionable Intelligence can be used in every step of the way to expose new evidence and c
our complex digital world.
*Uri Weil, Presale Team Leader, EMEA,* ***Verint***

12:00-13:00 Session B — **Secure & Anonymous Communication: Driven by Global Threats**
*Presented by* ***Yaana Technologies***

12:30-13:00 **Intelligence Fusion Center – Access, Understand and Share Knowledge. A Practical Dem**
Session A This session introduces the new Verint Intelligence Fusion Center (IFC), a unified and comprel window for the investigation of terror and crime. Based on access to virtually all data sources ( border crossings, official databases, HUMINT information, SIGINT and more), the IFC syster investigators to analyze and connect events, persons, locations and associations – even from se data and events. The demonstration illustrates an investigation about several bomb explosions, multiple data sources are used to solve the case.
*Adiel Horesh, Director of Business Development, Fusion and Web Intelligence Solutions,* ***Veri***

---

# Track 6: Social Network Monitoring and Big Data Analytics Training and Product Demonstrations

This track is only open to Law Enforcement, Public Safety and Government Intelligence Community Attendees

## Tuesday, 13 June 2017

9:00-10:00 **Actionable Intelligence with the SDL Government Language Platform**
Session A

One of the most complex – and often overlooked – tasks for Intelligence Analysts is handling r From streamlining internal translation processes, using standardized and centralized terminolog amounts of data automatically into actionable output, handling data in multiple languages is a t correct approach and tools. Learn how the SDL Government Language Platform offers end-to- language processing tools for Intelligence, Defense and Law Enforcement organizations

*Presented by Patrick Vanderper,* ***SDL***

9:00-10:00 **Facilitating the Analyst's Work through Robotic Process Automation and Deep and Dark**
Session B *Presented by* ***Kofax***

10:15-10:45 **Automatic Exploitation of Social Network, Deep and Dark Web to complement traditiona Interception Infrastructure**
*Presented by* ***IPS***

10:45-11:15 **How Public Sentiment can be influenced through propaganda campaigns on Social Media**
*Presented by* ***IPS***

11:30-12:30 **The New Forensic Investigator Toolbox: from Tactical to Open Source Investigations**
Session A *Presented by* ***AREA***

11:30-12:30 **OBTIGO – A Revolutionary Data Fusion System for Intelligence**
Session B *Presented by* ***WIP***

11:30-12:00 **Extremist communication: what is out there, how to collect it, what it does, how to make s**
Session C **to counter it -** ***OSINT from a practitioners view***
*Presented by* ***Gamma Group***

12:00-12:30 **Evidence-based, operational mission management - from the simple to the sophisticated**
Session C *Presented by* ***Gamma Group***

13:45-14:45 Session A **Confronting the multi-dimensional challenges of the new cyber world**

In the rising content-less world, locating and monitoring targets identities is almost impossible. security, tunnel encryption and temporary IDs create a new era in which most of the informatio uniquely related to identity. This challenge is even greater when you have to protect your organ unpleasant "malware surprises" sent to you by your target. Today's zero-days might disappear t

The key to solve this new 3d Puzzle is having a sophisticated Big Data analysis module that kn leads from the "Anonymous information" and crossing it with tactical capabilities to reconstruc Live Demonstration: We will practice this methodology by analyzing an example based on Bit CYBERBIT'S Pattern analysis of anonymous transaction , crossing it with IP-related correlatio investigation process to identify the hidden target.

*Presented by **CyberBit***

13:45-14:45 Session B **AI Powered Web Intelligence**
Extracting intelligent insights using machine learning algorithms
*Presented by **Cobwebs Technologies***

15:00-16:00 **Full target tracking: from Clearweb Monitoring to Darkweb poisoning and de-anonymiz**
*Presenetd by **InTheCyber***

16:15-17:15 **Analysing and Presenting complex Geospatial data to a Jury - Case study presentation of**

**Complex data - especially communications data records with ANPR, phone downloads, geo social media extracts - is time-consuming to analyse and even harder to present in an eas format to enable a jury to make just decisions.**

The presentation will show how GeoTime can simply import data from all the leading brand extractio geospatial (and non-geospatial) data on the map and in its 3D temporal views, enable the analyst to events using automatic pattern detection tools - e.g. Places frequented more than x times, meetings travel, attribution - and document these findings within GeoTime, taking snapshots of important vie movement and exporting all to a court-ready PowerPoint.

Law enforcement investigators around the world have used GeoTime to close cases and achieve just

*Presented by **JTOL***

## Wednesday, 14 June 2017

9:00-10:00 Session A **Monitoring and handling online campaigns and their influence**
*M Alexander, **BAE Systems Applied Intelligence***

9:00-10:00 Session B **The Voyager - Open Source & Social Media Intelligence powered by WEB-IQ.**

New way of OSINT. Make the target visible, stay hidden.

*Eldert van Wijngaarden – IQ - Internet Intelligence*
*Martin Uher – **AEROSPACE & DEFENSE SOLUTIONS***

11:30-12:00 Session A **Bridging discipline gaps in the hunt for perpetrators: Bringing together Metadata, OSI SIGINT, Dark Web, Surveillance techniques and various other capabilities to support**
*Presented by **Gamma Group***

12:00-12:30 Session A **Dark Web - Can Governments afford not knowing? Hunting criminals on the dark side**
*Presented by **Gamma Group***

11:30-12:30 Session B **Post Trojan Infiltration: The new Digital Undercover Agent**
*Presented by **AREA***

14:00-15:00 Session B **GoldenSpear Deep WEBINT – Reaching the Deepest corners of the Deep Web and the DarkNet**
*Presented by **S2T***

## Thursday, 15 June 2017

8:30-9:00 Session A **Sprinting the First Mile: The Art of Rapid Collection and Knowledge Expansion**
*Presented by **WIP***

8:30-9:00 Session B **TA-9, Utilizing big data gathered from different sources for entity-driven investigation**
*Presented by **RayZone Group***

8:30-9:30 Session C **Cloud Investigation with UFED Cloud Analyzer**
*Presented by **Cellebrite***

9:00-9:30 Session A **HIWIRE – Avatar-based Best of Breed Web Intelligence**
*Presented by **WIP***

9:00-9:30 Session B **Fighting illegal cellular interception with advanced methods and algorithms**
*Presented by **RayZone Group***

10:30-11:00 Session A **Handling Multilingual Big Data with automated translation (SDL)**

Big Data is not just characterized by volume, variety and velocity, but it also comes in a Multil
Translating limitless amounts of Multilanguage data can only be achieved by using ultra-fast, s
automated translation tools. Learn how SDL helps Intelligence, Defense and Law Enforcement
automatically translate social media and secure data to actionable output, handling intelligence
like informal Arabic and Arabizi and enforcing terminology and dictionaries, on a highly scala
server platform.

*Claudiu Stiube, **SDL***

12:00-13:00 **Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations**
*Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement, **UK Po***

12:00-13:00 **The Voyager - Open Source & Social Media Intelligence powered by WEB-IQ.**

New way of OSINT. Make the target visible, stay hidden.

*Eldert van Wijngaarden – IQ - Internet Intelligence*
*Martin Uher – **AEROSPACE & DEFENSE SOLUTIONS***

12:00-13:00 **AI Powered Web Intelligence**
Extracting intelligent insights using machine learning algorithms
*Presented by **Cobwebs Technologies***

---

# Track 7: Mobile Signal Intercept and Electronic Surveillance Training and Product Demonstration

This track is for Law Enforcement, Interior Security and the Government Intelligence Community who must work with cellular and mobile satellite operators regarding mobile location, electronic surveillance and RF intercept.
This track is only open to Law Enforcement, Public Safety and Government Intelligence Community Attendees.

## Tuesday, 13 June 2017

| | |
|---|---|
| 9:00-10:00<br>Session A | **Mobile Communication and wireless networks - Geolocation and Analysis for Investi**<br>*Wolfram Koerver, **S.E.A. Datentechnik*** |
| 10:15-11:15<br>Session A | **Turning Personal Communications Devices into Cyber-Secured Communication & C**<br>**Situational Awareness Platforms**<br>*Presented by **Providence Europe BV*** |
| 10:15-11:15<br>Session B | **Portable sensors kit for tactical use**<br>*Presented by **Pro4tech*** |
| 10:15-11:15<br>Session C | **Introduction of the TeleMonD Covert Tracking System**<br>*Presented by **I.T.P. Novex*** |
| 11:30-12:30 | **Portable sensors kit for tactical use**<br>*Presented by **Pro4tech*** |
| 15:00-16:00 | **Proliferation of Surveillance Techniques and Vulnerabilities in the Mobile Environm**<br>*Presented by **Inpedio*** |
| 16:15-17:15 | **New way of intelligent identification and localization from mobile devices**<br>*Presented by **SIM*** |

## Wednesday, 14 June 2017

| | |
|---|---|
| 9:00-10:00<br>Session A | **VSAT Interception made easy**<br>*Presented by **VASTech*** |
| 9:30-10:00<br>Session B | **The SpearHead Wi-Fi MitM platform - Best-in-class range performance with beamformi**<br>**technology**<br><br>Discover how the SpearHead platform and its unique technology expand operational reach with interception ranges, accurate target location, wide Man-in-the-Middle toolset and open design t infection system. |

*Presented by **WiSpear***

12:00-12:30 Session A **GSM Tactical Interception System for 3G and 4G**
*Presented by **Advanced Systems***

11:30-12:30 Session B **NeoSoft data traffic analyser for Mobile Monitoring**
*Presented by **NeoSoft AG***

14:00-14:30 **RDE Inmarsat Monitoring Solutions**
RDE looks back on more than 20 years of experience in solutions for satellite communication i
satellites of the fourth generation Inmarsat covers most of the world with services for voice and
communication, especially in areas without telecommunication infrastructure. To have access t
communication for intelligence purposes, Rheinmetall offers turnkey solution for monitoring In
and BGAN services.
*Kai Linsmann, **Rheinmetall***

15:30-16:30 Session A **Acquisition from Smart phone and WiFi-Data, incl. GeoLocalization**
*Presented by **Secure Information Management***

15:30-16:30 Session B **A Passive Radio System and Analytics Platform for Gaining Deep Insight from Public Wi**

Passively collect and react to the presence of RF signals using a small form factor sensor. Auto
analyze protocols to gain knowledge about individuals. Correlate sensor data (and where availa
data) to build a pattern of life and uncover group affiliations. This session will include live dem
world scenarios.

*Presented by **Packet Forensics***

15:30-16:00 Session C **Virtual Reality and Tactical Location Finding**
*Presented by **Darkblue Telecommunication Systems***

15:30-16:30 Session D **Preparing for EWF operations on wireless / VoIP networks with network analysis tools**
*Presented by **EXFO Homeland Security***

16:45-17:45 Session A **Command and Control Center for covert field operations using Audio, Video and GPS fe**
*Presented by **IPS***

16:45-17:15 Session C **Tactical Wi-Fi Interception - Identify, Acquire, Intercept.**

In this session we will go over the challenges, limitations and operational solutions in tactical W
missions. We will cover the following: identifying targets, acquiring them and manipulating W
to extract intelligence.

*Presented by **Jenovice***

17:15-17:45 Session C **Title TBA**
*Presented by **Squarehead***

## Thursday, 15 June 2017

8:30-9:30 **IMSI Catcher, Target localization, Active and Passive Interception, Basics and Optio**
*Presented by **NeoSoft AG***

10:30-11:30 **Miniature Surveillance Capabilities Through Wireless Solutions**
*Presented by **Covidence***

| | |
|---|---|
| 12:00-13:00 | **Session Title TBA**<br>*Presented by **PIC SIX*** |

---

# Track 8: Information Security and Defense with Quantum Safe Cryptography

This track is for Government and Private Sector Security Executives charged with developing a transition plan from today's Crypto Systems ( which can be defeated with the arrival of Quantum Computers) to Quantum Safe Cryptography specifically Quantum Key Distribution ( QKD) fiber optic networking or the alternative Quantum Resistant Cyryptography (QRC) based on new crypto algorithms.

## Wednesday, 14 June 2017

| | |
|---|---|
| 9:00-10:00 | **Quantum Computing and Defeating Encryption: Myths vs. Realities for Cyber Secu Makers**<br>*Jerry Lucas ( Ph.D, Physics), President, **TeleStrategies*** |
| 11:30-12:00 | **Industry overview on the State of Quantum Safe Cryptography and Standards**<br><br>This presentation will cover the work of ETSI (the European Telecommunication Standa studying academic proposals for next generation, quantum safe cryptography and develo guidance and migration paths for industry on the suitability of the various proposals for d<br><br>*Michael Groves, Vice Chairman, **ETSI QSC and member of UK CESG***<br>*and invited **ETSI QSC Industry Group*** |
| 14:00-15:00 | **Next Generation Security with Quantum Resistant Cryptography (QRC) Deployme**<br><br>Cryptography as we know it today ceases to be effective when the quantum age begins. V examples, we explore the new solutions that will replace and update your existing system them, and how to make the transition.<br><br>*Mike Brown, CTO, **ISARA*** |
| 16:00-16:30 | **Next Generation Information Security with Quantum Key Distribution ( QKD) Dep**<br>*Presented by Bruno Huttner, Quantum Safe Product Manager, **ID Quantique*** |

---

# Training Seminars Led by Law Enforcment Officers and Ph.D Computer Scientists

## Tuesday, 13 June 2017

## Seminar #1
## 09:00-17:15

## Online Social Media and Internet Investigations

Presented by: *Charles Cohen,* ***Cohen Training and Consulting, LLC*** *Charles Cohen also holds the position of Captain, Office of Intelligence & Investigative Technologies,* ***Indiana State Police, USA***

09:00-10:00

**Understanding Cell Handset Geolocation: What Investigators Need to Know**

10:15-11:15

**Open Source Intelligence (OSINT) Collection Tools:  Creating an Inexpensive OSINT Toolbox**

11:30-12:30

**Metadata Exploitation in Criminal Investigations**

13:45-14:45

**Conducting Covert Online Observation and Infiltration Activities: Challenges and Opportunities for Investigators**

15:00-16:00

**Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators**

16:15-17:15

**Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators (continued)**

## Seminar #2
## 9:00-17:15

## Practitioners Guide to Internet Investigations

Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***

The aim of this 1 day seminar is to take the attendees from the basics of understanding the Internet, how to find data, through to a full understanding of best practice of an Internet investigator, having awareness and knowledge of all the tools available to achieve this. It is aimed primarily at the investigator, delivered from the perspective of detective, to empower them to have the best methodology and tradecraft to profile and catch suspects.

This is exclusively Law Enforcement only, as Practical examples, covert and investigative methodology and tradecraft will be given throughout the seminar.

09:00-10:00

**The Internet, and how suspects leave a Digital Footprint**

10:15-11:15

**Recognizing Traffic Data and digital profiling**

11:30-12:30

**WIFI, geolocation, and Mobile Data traces**

13:45-14:45

**Awareness of Emerging Technologies, Masking Tech and Tools, TOR and proxies**

15:00-16:00

**Advanced Techniques in Tracing Suspects, and lateral problem solving**

16:15- 17:15

**Open Source Tools, resources and techniques**

## Seminar #3
## 9:00-12:30

## Understanding ISS Technologies and Products Deployed in Telecommunications Networks for Lawful Interception and Mass Surveillance

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies***

This half-day seminar covers how criminals and terrorists communicate over today's public telecommunications wireline and wireless networks, over the top Internet services and social networks. This seminar is ideal for law enforcement, interior security, public safety and others who need to understand the ISS technologies and products used to lawfully intercept electronic communications and conduct mass network surveillance as discussed at ISS World Conference sessions and by exhibitors.

9:00-10:00

**Introduction to Wireline and IP Infrastructure and Related ISS Products for Lawful Interception and Mass Surveillance**

10:15-11:15

**Understanding Mobile Wireless Infrastructure, and Related ISS Products for Lawful Interception and Mass Surveillance**

11:30-12:30

**Understanding the Internet Over-the-Top (OTT) Services and Related ISS Products for Mass Intelligence Gathering and Surveillance**

## Seminar #4
## 13:45 -14:45

## SS7 Vulnerabilities and Intercept Options

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies*** *and a* ***Distinguished Telecom Technology Expert to be announced***

There are two very important aspects of telco SS7 infrastructure law enforcement and inteior security needs to understand. For law enforcement: you can locate and track a target anywhere in the world if they just turn on their cell phone. For Interior Security: large scale distributed denial of service attacks over SS7 can completely take down today's telecom networks.

- SS7 Infrastructure Architecture Basics and Law Enforcement Challenges with Current SS7 Architecture
- How difficult is it to obtain access to the SS7 network? What is required?
- SS7 Attack Vectors and Protocol Attack Scenarios
- How to Achieve a Call Intercept remotely, from a different country, without physical access to the phone
- What Else: Inbound Call Forwarding, SMS Intercept, Denial of Target Service and more!

## Seminar #5
## 15:00-16:00

## Intercept Implications of 4G/5G Diameter Signaling Replacing SS7

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies*** *and a* ***Distinguished Telecom Technology Expert to be announced***

As telecom service providers transition to IP based VoLTE and introduce 5G, SS7 will be replaced with diameter signaling. This session provides the technical basics of diameter, options for transitioning SS7 to diameter and the new challenges facing law enforcement.

## Seminar #6
## 16:15-17:15

## The Implications of multi-IMSI and OTA for Law Enforcement and the Government Intelligence Community

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies*** *and a* ***Distinguished Telecom Technology Expert to be announced***

The era of SIM Cards with static IMSIs issued by cellular operators is changing. Deployment of multi-IMSI as well as network programmable (OTA) SIM cards will create new challenges for law enforcement. This session looks at the implications of multi-SIM and OTA for LEAs and Intel analysts.

- Understanding IMSIs, MSISDNs and Subscribers
- Growth of multi-IMSI and Multi-MSISDN and Impact on Law Enforcement Target Tracking
- Over The Air (OTA), Billing Fraud, Softsim Vulnerabilities and more!

## Seminar #7
## 13:45-14:45

## Investigation Techniques for Unmasking TOR Hidden Services and Other Dark Web Operations

Presented by: *Matthew Lucas, (Ph.D Computer Science), VP,* ***TeleStrategies***

TOR networks are notoriously effective at hiding the online identity of criminals, terrorists and others who are up to no good. The other side that receives less attention are TOR hidden services. These are services that leverage TOR's anonymizing capabilities to mask the identity of criminally-hosted online services - forming the basis of just about all illegal gambling sites, drug markets, child exploitation material, firearm sales, terrorism propaganda, and more.

- How TOR hides IP addresses/identity/location
- TOR hosting, What is .ONION and content analysis

## Seminar #8
## 15:00-16:00

## Defeating Network Encryption: What Law Enforcement and The Intelligence Community Needs to Understand

Presented by: *Dr. Matthew Lucas (Ph.D Computer Science), Vice President,* ***TeleStrategies***

The starting point to defeating encryption is to separate techniques addressing stored encrypted data such as with the Apple iPhone issue. The other challenge is defeating encrypted data in transit (e.g. Telegram, Whatsapp, etc.) or Network Encryption. This webinar is about defeating the later. When it comes to defeating network encryption the technical community separates into two camps. Those who want to impede law enforcement and the government intelligence community from defeating network encryption: IETF, Silicon Valley and hundreds of third party encryption services. And your camp, those who want to investigate criminals and terrorist group who depend on network encryption.

## Seminar #9
## 16:15-17:15

## Bitcoin Interception Experience

Presented by: *Vladimir Vesely, Researcher, FIT-BUT,* ***Brno University of Technology***

This session surveys interception options of the Bitcoin network. Namely, it investigates what kind of data may be collected from intercepted traffic of Bitcoin clients, miners and relevant services

(online wallets, exchanges, payment gateways). Moreover, two real-life use-cases (involving Bitcoin fraud and ransomware) are presented together with the used methodologies.

## Wednesday, 14 June 2017

## Seminar #10
## 9:00-10:00

## Bitcoin 101: Introduction to What Technical Investigators Need to Know about Bitcoin Transactions, Dark Web Commerce and Blockchain Analysis

Presented by: *Dr. Matthew Lucas, Vice President,* ***TeleStrategies***

This 101 training seminar is an introduction to Bitcoin, how the system is used to support criminal activities (e.g. Dark Web) and why technical investigators need to understand the basic Bitcoin transaction mechanism (Blockchain) to successfully defeat 21st century criminals and terrorist actions. Specifically, this introduction to Bitcoin for technical investigators addresses:

- Bitcoin Basics for Technical Investigators
- Understanding Bitcoin Infrastructure, Blockchain and Bitcoin Mining
- How Criminals and Terrorists Use TOR and Dark Web
- Bitcoin Cryptography Demystified (For Non-Math Majors)
- Bitcoin 2.0 and the New Challenges Facing Law Enforcement

## Seminar #11
## 9:00-10:00

## Quantum Computing and Defeating Encryption: Myths vs. Realities for Cyber Security Decision Makers

Presented by: *Jerry Lucas (PhD, Physics) President,* ***TeleStrategies***

The sole reason nation state governments are investing billiions of dollars in quantum computing development is to defeat today's crypto systems. On the otherhand the sole reason nation state governments as well as the venture capital community are investing in quantum safe cryptograph is to defeat quantum computers. If you have responsibilities for sifting through the myths and realities of quantum computing and/or quantum safe cryptography product readiness claims but don't have a degree in physics nor math, this webinar is for you.

Part 1: Quantum Computing and Defeating Encryption

The first myth is all quantum computer architectures under development are addressing the same problems. The reality some companies like Volkswagen, Airbus and Google are supporting quantum computer projects that are not designed to nor capable of cracking encryption. While others, like

nation state governments are supporting quantum computer architectures designed solely for defeating encryption. The other reality some quantum computer architectures forming the basis for someones Ph.D thesis in Physics, if developed at a large enough scale to crack today's encryption would require a dedicated nuclear power plant just to provide the required electrical power. Part 1 topics include:

Quantum Mechanic Principles used in developing computers described with pictures and metaphors (e.g. no math): Quantum Entanglement, Superpositioning, Heisenberg Uncertainty Principle, etc.

Qubits: What mathematically and physically are Qubits, Entangled Qubits and Quantum Gates, Why Quantum Computers can reduce the time to crack todays Public Key Cryptography from thousands of years with conventional computer systems to a few hours with future Quantum Computers,

Defeating Encryption Algorithms: Understanding the classic encryption defeating algorithms: (Shor algorithm example using simple math), Which algorithms are best suited to defeat RSA & AES, Why Bitcoin Cryptography is the most vulnerable, e.g. the first crypto system to be cracked (or hacked) with quantum computing.

Quantum Computer Hardware: From Qubit Gates to Computer Processors, Options under development, NMR, Ion Traps, Quantum Dots, etc., What companies are investing besides Google and IBM, Why the key performance factor is "number of entangled Qubits", and the number when reached (60?) makes today's encryption systems totally obsolete.

D-Wave: The most visible company in Quantum Computing today, What is different about their approach, What's Adiabatic Computing, NP class problems and Why this architecture is good for optimization problems but not promising for encryption key cracking.

Part 2: Quantum Safe Crytpography for Defeating Quantum Computers

There are two quantum safe crytpography development camps. the first focusses on "Quantum Resistant Algorithms or QRA" and the second focuses on "Quantum Key Distribution or QKD". The QRA group promote the concept, it's just a software upgrade, e.g. replace PKI and more with a QRA module. Where is QKD requires special puprose fiber optic or satellite based networks infrastructure.

The 64 dollar question: are the proposed QRA really quantum safe, given there are no mass commercial products deployed at this point for the hackers to go after nor agreed upon standards. The reality, until QRA are proven bullet proof, both QRA and QKD are being supported by nation state governments. Part 2 topics include:

Option 1: Quantum Resistant Algorithms:

- Review of leading candidate areas from a hi-level math perspective (Hash, Lattice and Code Based, Singular Elliptic Isogency and Mutlivariate Cryptography), emphasis on their pros and cons for use in various applications and implementation type issues and giving a sense of current academic progress in each area and Google's work on quantum resistant algorithms.

- Standards progress to date
- Summary of commercial solutions under development

Option 2: Quantum Key Distribution:
The session introduces the principles and QKD and discusses its integration into a quantum-safe security infrastructure. It covers the following: Principles of QKD (quantum channel, authentication, key distribution); current field trail implementations; point-to-point versus point-to multipoint systems; Increasing the distance range with Trusted Nodes and free space key distribution; Some use cases (government, finance, data centers...); Roadmap for the future of QKD.

## Seminar #12
## 12:00-12:30

## Cryptocurrency Miner Detection in your Organization's Network

Presented by: *Vladimir Vesely, FIT-BUT,* ***Brno University of Technology***
Ways to automatically detect cryptocurrency miners in computer network who are exploiting resources of their organization (usually free of charge electricity and reliable Internet connectivity comparing to households). Methodology on how to detect devices running mining software from the Netflow records. Running a web service which can tell you whether a given IP address is the mining pool/client or not.

## Seminar #13
## 16:45-17:45

## TLS/SSL Decryption Workshop

Presented by: *Vladimir Vesely, Researcher, FIT-BUT,* ***Bruno University of Technology***
The presentation introduces methods how to decrypt TLS/SSL connection. Focus is on man-in-middle attack employing TLS/SSL proxy and other ways how to obtain session's private keys. Speaker will demonstrate how to decrypt intercepted traffic using open-source tools like Wireshark and NetFox Detective.

## Thursday, 15 June 2017

## Seminar #14
## 12:00-13:00

## Bitcoin Interception Experience

Presented by: *Vladimir Vesely, Researcher, FIT-BUT,* ***Brno University of Technology***

This session surveys interception options of the Bitcoin network. Namely, it investigates what kind of data may be collected from intercepted traffic of Bitcoin clients, miners and relevant services (online wallets, exchanges, payment gateways). Moreover, two real-life use-cases (involving Bitcoin fraud and ransomware) are presented together with the used methodologies.

## Seminar #15
## 12:00-13:00

## Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations

Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***

*Click here to return to the home page*