< Back to ISS World Programs

AGENDA

ISS World North America is the world's largest gathering of North American Law Enforcement, Homeland Security, Defense, Public Safety and other members of the Government Intelligence Community as well as Telecom Operators responsible for cyber threat intelligence gathering, DarkNet monitoring, lawful interception and cybercrime investigations.

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 networks, the Internet and Social Networks.

Track 1: Advanced Hi-Tech Cyber Investigation Training by LEAs and Ph.Ds
Track 2: LEA, Defense and Homeland Security Intercept Training
Track 3: Social Network Monitoring and Cyber Threat Analytics Training

Track 4: Investigating Dark Webs and Associated Cybercurrency Transactions

Track 5: Artificial Intelligence Product Training for Law Enforcement and Government Intel

Track 6: Financial Crime Investigation Techniques and Products

Track 7: Quantum Computing Reality and Post-Quantum Cryptography Today

Note: Under each Track (1-7) below, you will note who is elligible to attend. (All attendees or LEA and Government Only)

ISS World North America Agenda from 2018 Program

ISS World North America 2019 Agenda and Registration Link Available June 2019

Track 1: Advanced HI-Tech Cyber Investigation Training Seminars Led by Law Enforcement Officers and Ph.D Computer Scientists

35 classroom training hours, presented by sworn law enforcement officers, Ph.D. Computer Scientists and nationally recognized cybercrime textbook authors and instructors. Distinguished ISS World Training Instructors include:

Charles Cohen**, Cohen Training and Consulting, LLC, also holds the position of Captain, **Indiana State Police
(6 classroom hours)

Mark Bentley**, Communications Data Expert, National Cyber Crime Law Enforcement, **UK Police
(9 classroom hours)

Michael Loughnane, *CAMS, CFE, Loughnane Associates, LLC and retired 27 year US Federal Law Enforcement Officer*
(5 classroom hours)

Todd G. Shipley *CFE, CFCE, President and CEO of Vere Software, Co-Author of, Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace and retired officer,* ***Reno NV, Police Department***
(6 classroom hours)

Matthew Lucas *(Ph.D., Computer Science), Vice President,* ***TeleStrategies***
(4 classroom hours)

Jerry Lucas *(Ph.D., Physics), President,* ***TeleStrategies***
(5 classroom hours)

Stephen Arnold*, Managing Partner,* ***Arnold.IT***
(2 classroom hours)

Jean Gottschalk*, Principal Consultant,* ***The Telecom Defense Limited Company***
(3 classroom hours)

Wednesday, September 5, 2018

Seminar #1
9:00-5:00

Online Social Media and Internet Investigations

Presented by: Charles Cohen, **Cohen Training and Consulting, LLC**; Charles Cohen also holds the position of Captain, Cyber Crimes Investigative Technologies Section, **Indiana State Police, USA**

9:00-10:00
Proxies, VPNs, and Dark Web: Identity Concealment and Location Obfuscation

10:15-11:15
Tor, onion routers, Deepnet, and Darknet: An Investigator's Perspective

11:30-12:30 PM

Tor, onion routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators

1:30-2:30 PM

Cellular Handset Geolocation: Investigative Opportunities and Personal Security Risks

2:45-3:45 PM

Collecting Evidence from Online Social Media: Building a Cyber-OSINT Toolbox (Part 1)

4:00-5:00 PM

Collecting Evidence from Online Social Media: Building a Cyber-OSINT Toolbox (Part 2)

Seminar #2

9:00-5:00

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, building their OSINT toolbox, and 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. How the system works for us, as investigators

10:15-11:15

Recognizing Traffic Data and digital profiling via social networks and devices - digital shadows

11:30-12:30 PM

WIFI, geolocation, and Mobile Data traces and tracking

1:30-2:30 PM

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

2:45-3:45 PM

Advanced Techniques in Tracing Suspects, and lateral problem solving

4:00-5:00 PM

Open Source Tools, resources and techniques - A walk through my free law enforcement open source tools site

Seminar #3

9:00-10:00

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

Presented by: *Dr. Matthew Lucas (Ph.D, Computer Science), 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 #4

10:15-11:15

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 # 5
11:30-12:30

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 session is about defeating the later.

Seminar #6
13:30-14:30

Understanding "The Very Basics" of Quantum Computing for Non-Engineers
Presented by: *Jerry Lucas, (Ph.D, Physics) President,* ***TeleStrategies***

This very basic, one-hour session is for cyber security and intelligence gathering professionals who must understand quantum computing technology basics to access artificial intelligence, machine learning as well as defeating encryption applications but do not have any significant advanced academic training in physics, mathematics nor engineering.

Seminar #7
14:45-15:45

Understanding "Defeating Encryption" with Quantum Computing for Non-Engineers
Presented by: *Jerry Lucas, (Ph.D, Physics) President,* ***TeleStrategies***

This one hour, session is for cyber security executives and specialists who have the responsibility of assessing the lead time they have before deploying quantum safe cryptography solutions but don't have a technical background. If you believe nation state security agencies are developing quantum computing to decrypt your past and future intercepted transmission sessions, this high-level webinar should be a must attend briefing.
And to do this you need to understand how a quantum computing circuit works when designed for the sole purpose of defeating public key encryption.

Seminar #8
4:00-5:00 PM

Understanding "Post-Quantum Cryptography" for Non-Mathematicians

Presented by: *Jerry Lucas (Ph.D, Physics) President,* ***TeleStrategies***

This one hour session is for cyber security exutives responsible for developing alternatives to todays cryptography infrastructure in response to the threat of quantum computing.

Thursday, September 6, 2018

Seminar #9

09:00-5:00 PM

Concerns and Considerations in Financial Crime Investigations

Presented by: *Michael Loughnane, CAMS, CFE,* ***Loughnane Associates, LLC*** *Mike is a former US Federal Law Enforcement Officer who specialized in complex fraud and cybercrime investigations and currently provides training to improve detection and investigations of fraud, money laundering and counter terror finance.*

09:00-10:00 AM

Criminal Essentials: The Needs of a Criminal Network

11:00-12:00 PM

Financial Crime Schemes in Money Laundering

1:00-2:00 PM

The Essentials of Trade Based Money Laundering

2:30-3:30 PM

How Does Money Actually Move?

4:00-5:00 PM

Follow the Money Beyond the Banks

Seminar #10

4:00-5:00 PM

Advanced Analytic Techniques for Deanonymizing Hidden Network Digital Currency Transactions and Messaging Using Open Source and Commercial Software

Presented by: *Stephen Arnold, Managing Partner,* ***Arnold.IT***

In this session, Stephen E Arnold reviews technology-centric methods for deanonymizing hidden network activities. Based on research conducted for US federal agencies and research to support his work as a commissioner for the Judicial Commission of Inquiry into Human Trafficking and Child Sex Abuse.

Friday, September 7, 2018

Seminar #11
8:30-9:30

Practitioners Guide to Understanding Cyber Attacks on Banks - Exploring Vulnerabilities from The Perspective Of The Hacker
Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***

This one-hour session will explore the viewpoints of both the banks perception of vulnerabilities, and that of the attacker. A follow-up session at 10:30 will address Practitioners Guide to Defending Banks Against Cyber Attacks.

Seminar #12
10:30-11:30

Practitioners Guide to Defending Banks Against Cyber Attacks – Identifying And Protecting Vulnerabilities To Frustrate The Thief, and Integrity Proof The Systems
Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***

This one-hour session will explore the protection of weak points and future proofing banks against cyber attacks.

Seminar #13
12:00-1:00 PM

What Investigators and Intelligence Professionals Need to Know about Amazon's Disruptive Streaming Data Marketplace and Policeware Services
Presented by: *Stephen Arnold, Managing Partner,* ***Arnold.IT***

In this presentation, research completed by Stephen E Arnold and his research team to support their work related to the Judicial Commission's activities reveals the capabilities of Amazon's entrance into the policeware and intelligence analytics markets. ("Policeware" is shorthand for the vendors who provide data gathered via OSINT methods, software to analyze and make sense of OSINT and nonpublic data, and how certain investigative work will be performed.)

Seminar #14
12:00-1:00 PM

Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations
Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***

Seminar #15
8:30-1:00 PM

Special SS7 Intercept, Vulnerabilties and Most Damaging SS7 Infrastructure Attacks over the Last 12 Months
Presented by *Jean Gottschalk, Principal Consultant,* ***The Telecom Defense Limited Company***

8:30-9:30 AM
SS7 Vulnerabilities and Intercept Options
There are two very important aspects of telco SS7 infrastructure law enforcement and interior 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.

10:30-11:30 AM
The Most Damaging SS7 Network Infrastructure Attacks over the Last 12 Months

12:00-1:00 PM
Intercept Implications of 4G/5G Diameter Signaling Replacing SS7
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.

(Full Pre-Conference Seminar Agenda Appears After Track 7)

ISS World Americas 2018 Conference Agenda

September 5-7, 2018

ISS World America Exhibit Hours:

Thursday, September 6, 2018: 10:00 AM-6:00 PM

Friday, September 7, 2018: 9:30 AM-12:00 PM

Thursday, September 6, 2018

8:15-8:30 AM	**Welcoming Remarks** *Tatiana Lucas, ISS World Program Director,* ***TeleStrategies***
8:30-9:00 AM	**Top Ten Internet Challenges Facing Law Enforcement and the Government Intelligence Co and Who at ISS World North America has Solutions** *Dr. Jerry Lucas, President,* ***TeleStrategies***

Track 1: Advanced Hi-Tech Cyber Investigation Training by LEAs and Ph.Ds

WHO CAN ATTEND: All attendees can attend Track 1 sessions, except for the sessions marked "*(LEA and Government Attendees Only)*". Those sessions are for Law Enforcement and Government Attendees only.

Wednesday, September 5, 2018

9:00-5:00 PM	**Online Social Media and Internet Investigations** *Charles Cohen, Cohen Training and Consulting, LLC Charles Cohen also holds the position of Captain,* ***Indiana State Police***
9:00-5:00 PM	**Practitioners Guide to Internet Investigations** *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police*** ***(LEA and Government Attendees Only)***
9:00-10:00	**Cryptocurrency 101: Introduction to What Technical Investigators Need to Know abou and Altcoin Transactions, Dark Web Commerce and Blockchain Analysis** *Dr. Matthew Lucas (Ph.D, Computer Science), Vice President,* ***TeleStrategies***
10:15-11:15	**Investigation Techniques for Unmasking TOR Hidden Services and Other Dark Web Op** *Dr. Matthew Lucas, (Ph.D Computer Science), VP,* ***TeleStrategies***
11:30-12:30 PM	**Defeating Network Encryption: What Law Enforcement and The Intelligence Communi to Understand** *Dr. Matthew Lucas (Ph.D Computer Science), Vice President,* ***TeleStrategies***

Friday, September 7, 2018

8:30-1:00 PM	**Special SS7 Intercept, Vulnerabilties and Most Damaging SS7 Infrastructure Attacks Last 12 Months** Presented by *Jean Gottschalk, Principal Consultant,* ***The Telecom Defense Limited Compa*** 8:30-9:30 AM **SS7 Vulnerabilities and Intercept Options** There are two very important aspects of telco SS7 infrastructure law enforcement and interio needs to understand. For law enforcement: you can locate and track a target anywhere in the they just turn on their cell phone. For Interior Security: large scale distributed denial of servi over SS7 can completely take down today's telecom networks. 10:30-11:30 AM **The Most Damaging SS7 Network Infrastructure Attacks over the Last 12 Months** 12:00-1:00 PM **Intercept Implications of 4G/5G Diameter Signaling Replacing SS7** As telecom service providers transition to IP based VoLTE and introduce 5G, SS7 will be repla diameter signaling. This session provides the technical basics of diameter, options for transiti to diameter and the new challenges facing law enforcement.

12:00-1:00 PM **Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations**
Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement, ***UK Pol***
(LEA and Government Attendees Only)

Track 2: LEA, Defense and Homeland Security Intercept Training

WHO CAN ATTEND: All attendees can attend Track 2 sessions, except for the sessions marked "*(LEA and Government Attendees Only)*". Those sessions are for Law Enforcement and Government Attendees only.

Wednesday, September 5, 2018

9:00-5:00 PM **Online Social Media and Internet Investigations**

Presented by *Charles Cohen,* ***Cohen Training and Consulting, LLC*** *Charles Cohen also h*

position of Captain, ***Indiana State Police***

This one day session provides an up-to-date understanding of how social networking sites

how members act and interact. Attendees will learn what information is available on variou

how to integrate that information into criminal investigations and criminal intelligence anal

Thursday, September 6, 2018

9:00-10:00 Session A **Lawful Interception in 5G Mobile Networks**
This session will elaborate the needs and the challenges of lawful interception in current and future wire networks. Network operators and law enforcement agencies will get practical advice and hear best prac techniques for the implementation of LI in 5G networks.
Presented by ***Utimaco TS GmbH***

9:00-10:00 Session B **Generate powerful evidence from PCAP, CDR/IPDR and Social Media data, all over a single in**

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

A typical investigation involves multiple interfaces & manual correlation, eventually resulting in disconn intelligence about the "Person of Interest".

What if you could bring data, tools and systems together on a single interface?

Experience Investigation Workbench, a seamless platform that assists investigators to collaboratively di evidence, profile suspects, build stories and solve cases rapidly.

Presented by*: Jitendra Verma- Director, Business Development,* ***ClearTrail Technologies***
(LEA and Government Attendees Only)

9:00-10:00 Session C
Scaling Security Clusters with SDN Technology: A Programmable Threat Intelligence Gatewa
Marc LeClerc, VP Strategy and Marketing, ***NoviFlow Inc.***

11:00-12:00 Session A
Digital Toolbox: the investigator's best friend
Presented by ***AREA***
(LEA and Government Attendees Only)

11:00-12:00 Session B
Next Generation Monitoring Center- Discover your suspects unlike ever before

Investigators struggle to derive insights from the massive & ever-expanding voice & encrypted IP comm
data. Moreover, the hardwired architecture of a traditional monitoring center poses limitations in allowi
seamless integration across the latest investigation tools, thereby leaving the investigators with limited
visibility and insufficient evidence.

What if there was a way to transform conventional, passive monitoring approach to generate relevant i
& build powerful evidence from thousands of voice calls & encrypted traffic?
Join us to explore a world of transformational monitoring solutions that bring sustainability within the L
make it future ready, now.

Presented by: *Manohar Katoch- AVP Business Development,* ***ClearTrail Technologies***
(LEA and Government Attendees Only)

11:00-12:00 Session C
Securing Your Online Presence During Investigations
Presented by ***Ntrepid Corp***

1:00-2:00 PM Session A
How Legislative Initiatives and Case Law in 2018 are Impacting the Going Dark Challenge:

- Cloud Act
- FOSTA
- Carpenter vs. United States
- Net Neutrality Elimination
- What are the Impacts for LEAs

Charles Cohen, Captain, ***Indiana State Police***
Jim Emerson, Chair, ***IACP Cybercrime and Digital Evidence Committee***
Ben Bawden, Partner, ***Brooks Bawden***

1:00-2:00 PM Session B
Data Fusion and Analytics for National Security and Intelligence
Presented by ***Yaana Technologies***
(LEA and Government Attendees Only)

2:30-3:00 PM Session A
How New International Initiatives are Impacting Cybercrime Investigations
This tutorial covers several new international extraterritorial legislative enactments, how they are relate
they are being reflected in new practices, industry standards, and potential CyberSecurity products. T
initiatives include new Cybercrime Convention and cloud evidence provisions, the EU Directives on e-Ev
transnational investigative orders, and new supporting public-private technical specifications.
Tony Rutkowski, EVP, ***Yaana Technologies***

2:30-3:30 PM Session B
Real Intelligence Analytics on top of ElasticSearch
Presented by ***NEXA Technologies***

3:00-3:30 PM Session A	**"The Risks of LEAs Using 4G Communications: How to prevent your location being disclosed"** There have been numerous vulnerabilities reported by media and researchers around 4G networks and protocol, Diameter. As already documented with SS7, the Diameter protocol allows for the same vulner addition to some new ones. Some of these vulnerabilities cannot be fixed, and will exist in 5G as well. The FCC CSRIC VI WG3 publi report on the risks of 4G communications in March of 2018. Since then, new vulnerabilities have been d This session examines the vulnerabilities that have been disclosed, and what this means to law enforcer officials who depend on 4G communications in their operations. *Travis Russell, Director CyberSecurity,* ***Oracle***
4:00-4:30 PM Session A	**"Is Your Phone Giving You Away?: Protecting your activity from prying eyes."** For several years, the Android operating system has been leaking highly sensitive information about the the device, to support the adtech industry. In 2018, some of this has finally come to light through inves around Facebook, and research on Google. Android devices disclose more than GPS coordinates. They also identify activities (such as walking, in a train, or running). Google can identify with an accuracy of 99% whether a customer has visited a store, what department they visited within the store. Learn what research has disclosed about the leakage of highly sensitive data from Android devices, and carrying a cell phone can be a bad idea. *Travis Russell, Director CyberSecurity,* ***Oracle*** ***(LEA and Government Attendees Only)***
4:00-4:30 Session B	**Navigating the Complexities of Communication Providers and Government Agencies for Legal** *Presented by* ***Yaana Technologies*** ***(LEA and Government Attendees Only)***
4:30-5:00 PM Session A	**"Is Being Connected Worth The Risk?: Prevent IoT from putting you at risk"** The Internet of Things (IoT) is everywhere. The promise of 5G is to provide mass connectivity, enabling low power devices to connect and transmit data. This promises to be disruptive in virtually every indust But what amount of risk are we willing to take with IoT? Can IoT place law enforcement at a higher risk before? These are questions no one really has an answer for today, but questions everyone is asking. This session will explore what 5G promises for IoT, the risks and vulnerabilities that come with it, and w means to law enforcement. *Travis Russell, Director CyberSecurity,* ***Oracle***

Friday, September 7, 2018

8:30-9:30 Session A	**Emerging Technologies for Mobile Communication** Farid Salehr, ***ACE***
8:30-9:30 Session B	**Finding Cyber Threats in Terrestrial and Submarine Optical Networks** *Presented by* ***NetQuest*** ***(LEA and Government Attendees Only)***

****Additional Track 2 Sessions to be announced****

Track 3: Social Network Monitoring and Cyber Threat Analytics Training

WHO CAN ATTEND: ***(LEA and Government Attendees Only)*** **Only Law Enforcement and Government attendees may attend Track 3 sessions**

Thursday, September 6, 2018

11:00-12:00 PM	**Triage first: analytics is the second priority for OSINT** *Presented by **Basis Technology***
1:00-2:00 PM Session A	**DataWalk: the next generation analytical platform** Investigative methods to exploit DeepWeb content; analyzing SOCMINT and OSINT data *Chris Westphal, Chief Analytic Officer, **DataWalk***
1:00-2:00 PM Session B	**Unmasking and Linking Bad Actors Across OSINT, SOCINT and DARKINT** Imagine finding all of the secret information bad actors never thought would be exposed. Now imagine finding this information faster than ever before, by fusing all data sources pertaining to y investigation into one unified portal, including historical identity record data you never knew existed. In this session, we will show you how to leverage a curated datalake of over ten billion identity records accumulated across the full Internet surface over several years, and to unmask bad actors and uncover rooted links for your investigations. By bringing together the right data sources and configuring the sys to your mission, you can drill down and find unexpectedly rich identity information such as date of birth addresses, IPs, nicknames and intriguing data such as personal tastes and preferences. *Presented by **4iQ***
2:30-3:30 PM	**L.I. Targeting respecting privacy.** *Presented by **AREA***
4:00-5:00 PM	**Publicly Available Information in the Digital Age** *Jeff Chapman, CEO, **Babel Street***

Friday, September 7, 2018

8:30-9:30 Session B	**Measuring the effects of Information Operations through specialized sentiment analysis** *Christopher Biow, Senior Vice President Global Private Sector, **Basis Technology***
10:30-11:30	**Profile, target and investigate the Darknet. Reinventing traditional HUMINT in the Digital Era** *Presented by **AREA***
12:00-1:00 PM	**Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations** *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement, **UK Police***
12:00-1:00 PM	**What Investigators and Intelligence Professionals Need to Know about Amazon's Disruptive Streaming Data Marketplace and Policeware Services** In this presentation, research completed by Stephen E Arnold and his research team to support their w related to the Judicial Commission's activities reveals the capabilities of Amazon's entrance into the pol and intelligence analytics markets. ("Policeware" is shorthand for the vendors who provide data gather OSINT methods, software to analyze and make sense of OSINT and nonpublic data, and how certain investigative work will be performed.) *Stephen Arnold, Managing Partner, **Arnold.IT***

****Additional Track 3 Sessions to be announced****

Track 4: Investigating Dark Webs and Associated Cybercurrency Transactions

WHO CAN ATTEND: All attendees can attend Track 4 sessions, except for the sessions marked "*(LEA and Government Attendees Only)*". Those sessions are for Law Enforcement and Government Attendees only.

Wednesday, September 5, 2018

9:00 -5:00 PM **A Real World Look at Investigations in the Dark Web**

Presented by: *Todd G. Shipley CFE, CFCE, President and CEO of* ***Vere Software****, Co-Author of, Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace and retired investigator,* ***Reno NV, Police Department***

(LEA and Government Attendees Only)

The aim of this 1 day seminar is to take the attendees from the basics of understanding the Dark W to access it to how to finding information hidden within it. The attendees will learn the best practic internet investigator when working in the Deep Web and the tools available to assist their investiga the Deep Web.

This exclusively Law Enforcement attendees only, as Practical examples, covert and investigative r will be given throughout the seminar.

9:00-10:00 **Cybercurrency 101: Introduction to What Technical Investigators Need to Know about Bi and Altcoin Transactions, Dark Web Commerce and Blockchain Analysis**

Matthew Lucas (Ph.D., Computer Science), Vice President, ***TeleStrategies***

10:15-11:15 **Investigation Techniques for Unmasking TOR Hidden Services and Other Dark Web Opera**

Matthew Lucas (Ph.D., Computer Science), Vice President, ***TeleStrategies***

11:30 -12:30 PM **Defeating Network Encryption: What Law Enforcement and The Intelligence Community Understand**

Matthew Lucas (Ph.D., Computer Science), Vice President, ***TeleStrategies***

1:30-2:30 PM **Cryptocurrency and blockchain technology: challenges and solutions for cyber investigat**
Michael DuBose, CEO of ***Crystal Blockchain Inc., Bitfury***
(LEA and Government Attendees Only)

Thursday, September 6, 2018

9:00-10:00 AM **Investigative methods to exploit DeepWeb content; analyzing SOCMINT and OSINT data**
Chris Westphal, Chief Analytic Officer, ***DataWalk***
(LEA and Government Attendees Only)

11:00 -12:00 PM **Unifying Darknets Into One Integrated Data Feed**
At the end of the presentation, participants will have a clear idea of the challenges and opportunities t machine-based monitoring of the dark web, as well as practical ideas on how to integrate unified craw data into cyber security technology.
Ran Geva, CEO, ***Webhose.io***
(LEA and Government Attendees Only)

1:00-2:00 PM Session B **DataWalk: the next generation analytical platform**
Chris Westphal, Chief Analytic Officer, ***DataWalk***
(LEA and Government Attendees Only)

1:00-5:00 PM Session A **Special Half Day DarkNet Seminar**

by Andrew Lewman, Vice President, DarkOWL and Former Exectuve Director, The TOR Project

1:00-2:00 PM

Indexing the dark net – how do you catalog and search something that is not meant to be e

scrubbed? What's possible?

Presented by:

Andrew Lewman, Vice President, ***DarkOWL***

2:30-3:30 PM

Case studies / examples in dark net investigations – de-anonymizing examples / approache

practices / lessons learned.

Presented by:

Andrew Lewman, Vice President, ***DarkOWL***

4:00-5:00 PM

Future directions - what's next in dark net infrastructure, dark markets and investigation

implications

Presented by:

Andrew Lewman, Vice President, ***DarkOWL***

4:00-5:00 PM Session B	**Advanced Analytic Techniques for Deanonymizing Hidden Network Digital Currency Transac and Messaging Using Open Source and Commercial Software** In this session, Stephen E Arnold reviews technology-centric methods for deanonymizing hidden netwo activities. Based on research conducted for US federal agencies and research to support his work as a commissioner for the Judicial Commission of Inquiry into Human Trafficking and Child Sex Abuse. *Stephen Arnold, Managing Partner,* ***Arnold.IT*** ***(LEA and Government Attendees Only)***

Friday, September 7, 2018

8:30-9:30 Session B	**Cryptocurrency and blockchain technology: challenges and solutions for cyber investigators** *Michael DuBose, CEO of* ***Crystal Blockchain Inc., Bitfury*** ***(LEA and Government Attendees Only)***
10:30-11:30 Session A	**The challenges we faced in creating an effective dark web crawler** When we set forth to create a crawler for the dark web, we initially believed it would be a "low hanging technological challenge. Little did we know we will fall down the rabbit hole. *Ran Geva, CEO,* ***Webhose.IO*** ***(LEA and Government Attendees Only)***
10:30-11:30 Session B	**The Practical Use of Blockchain Analytics for Collecting Digital Evidence of Criminal Acts** *Mark Blackman, Crystal Consultant,* ***Bitfury*** ***(LEA and Government Attendees Only)***
12:00-1:00 PM Session A	**What Investigators and Intelligence Professionals Need to Know about Amazon's Disruptive Streaming Data Marketplace and Policeware Services** In this presentation, research completed by Stephen E Arnold and his research team to support their w related to the Judicial Commission's activities reveals the capabilities of Amazon's entrance into the po and intelligence analytics markets. ("Policeware" is shorthand for the vendors who provide data gather OSINT methods, software to analyze and make sense of OSINT and nonpublic data, and how certain investigative work will be performed.) *Stephen Arnold, Managing Partner,* ***Arnold.IT*** ***(LEA and Government Attendees Only)***

Track 5: Artificial Intelligence Product Training for Law Enforcement and Government Intel

WHO CAN ATTEND: All attendees can attend Track 5 sessions, except for the sessions marked "*(LEA and Government Attendees Only)*". Those sessions are for Law Enforcement and Government Attendees only.

Thursday, September 6 2018

9:00-10:00	**Artificial Intelligence and Machine Learning Applications for Law Enforcement**

While still in very early stages of development, artificial intelligence (AI) and machine learning (ML) tech

have enormous potential to improve law enforcement capabilities and effectiveness.

This session is focused on the basics of AI and ML; what products are starting to emerge based on thes

technologies and what law enforcement can expect over time.

Specific topics include:

- Overview artificial intelligence (AI), deep machine learning and the underlying technology.
- The difference between AI/ML for law enforcement and enterprise applications.
- Key applications of AI/ML for law enforcement: Video analysis, face recognition, pattern analysis language processing, social media analytics, network forensics, robotics and cyber security.
- Example product offerings and what's in the development pipeline.

Followed by Audience Q&A

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

11:00-12:00 **AI Powered Web Intelligence**

The increasing usage of social media platforms, mobile apps and deep web sources have resulted in a s

growth in illegal activities over the internet.

AI-Powered Web Intelligence is an advanced new technology which enables extraction of targeted intell

from Big Data using machine learning algorithms – in a click of a button.

We will present our web investigation solution used by Law Enforcement and National Security agencies

designated for targets profiling, social connections mapping, situational awareness and more.
Udi Levy, CEO, ***Cobwebs Technologies***
(LEA and Government Attendees Only)

1:00-2:00 PM **Understanding "Quantum Computing and Artificial Intelligence" for Non-Data Scientists**
Data science has been rapidly growing over the past decade, and its applications have become ubiquito daily lives. As these applications consume more data and need faster response times, new technologies algorithms are needed to meet the computational demands. Quantum computing is a highly promising technology that could present significant opportunities to accelerate the training of machine learning alg and improve data science methods
Dr. Maxwell Henderson, Senior Data Scientist, ***QxBranch***

2:30-3:30 PM **Real-life use cases for analyzing unstructured data to investigate terror & criminal activities new AI-driven technologies**
The way terrorists, gang members and other criminals connect, interact, recruit and spread propaganda changed in today's digital world. The internet has opened a new 5th dimension of warfare, and law enfo agencies must stay one step ahead of the game. Solutions based on artificial intelligence, machine lear behavior pattern analysis and augmented analytics allow those responsible for our safety to regain cont supercharge their investigative efforts. We'll be discussing these solutions in a riveting session using re use cases as examples.
Hendrik Van Der Meulen, Industry Executive, ***Voyager Analytics***
(LEA and Government Attendees Only)

Thursday and Friday Vendor Sessions TBA

Track 6: Financial Crime Investigation Techniques and Products

WHO CAN ATTEND: All attendees can attend Track 6 sessions.

Thursday, September 6, 2018

9:00 - 5:00 PM	**Special "Best Practices for Financial Crime Investigators" Sessions** Presented by: *Michael Loughnane, CAMS, CFE,* ***Loughnane Associates, LLC*** *and retire* *year* ***US Federal Law Enforcement Officer*** 09:00-10:00 AM **Criminal Essentials: The Needs of a Criminal Network** 11:00-12:00 PM **Financial Crime Schemes in Money Laundering** 1:00-2:00 PM **The Essentials of Trade Based Money Laundering** 2:30-3:30 PM **How Does Money Actually Move?** 4:00-5:00 PM **Follow the Money Beyond the Banks**

Friday, September 7, 2018

8:30-9:30 Session A	**Partnerships to Positive Action (Banking Secrets Revealed)** This presentation will specifically the workings of the banking industry and describe the type of informa data banks can develop while working their customer identification programs, transaction monitoring, a investigation of possible suspect activity, that may or may not make its way to law enforcement. *Steve Gurdak, CAMS, Group Supervisor,* ***Washington Baltimore HIDTA****,* ***Northern Virginia Financi*** ***Initiative (NVFI)***
8:30-9:30 Session B	**Practitioners Guide to Understanding Cyber Attacks on Banks - Exploring Vulnerabilities fron** **Perspective Of The Hacker** *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***
10:30- 11:30 Session A	**Putting it Together: The Value of The Professional Analyst** This presentation will discuss that with the dramatic increase of sophisticated processes used in financia crimes, it is even more important that law enforcement analysts develop capabilities to develop logical inferences that are useful in criminal case development and prosecution. We will discuss the balance be reliance on modern computing tools and digital analytics, and the need to apply understanding of crimi finance, criminal behavior and the requirement of criminal procedure, diminish the quality of investigati *Robert C. Bacon, 42 Infantry Division Headquarters First Sergeant,* ***NewYork National Guard and Ne*** ***Police Department Narcotics Drug Division***

10:30-11:30 **Practitioners Guide to Defending Banks Against Cyber Attacks – Identifying And Protecting Vulnerabilities To Frustrate The Thief, and Integrity Proof The Systems**
Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement, ***UK Police***

Track 7: Quantum Computing Reality and Post-Quantum Cryptography Today

WHO CAN ATTEND: All attendees can attend Track 7 sessions.

Pre-Conference Track Quantum Computing Tutorials

Wednesday, September 5, 2018

1:30-2:30 PM **Understanding "The Very Basics" of Quantum Computing for Non-Engineers**
Presented by: *Jerry Lucas (Ph.D, Physics) President,* ***TeleStrategies***

2:45-3:45 PM **Understanding "Defeating RSA, Blockchain and Today's Cryptography" with Quantum Compu Non-Engineers**
Presented by: *Jerry Lucas (Ph.D, Physics) President,* ***TeleStrategies***

4:00-5:00 PM **Understanding "Post Quantum Cryptography" for Non-Mathematicians**
Presented by: *Jerry Lucas (Ph.D, Physics) President,* ***TeleStrategies***

Post-Quantum Cryptography (PQCrypto) Sessions

Thursday, September 6, 2018

9:00-10:00 **Preparing for the quantum era**
Quantum computers will bring an unprecedented computing power to the world.
What are they? How can we benefit from quantum computers? When?

While it is too soon to know the full breadth of applications and implications of quantum computing, one known:
They will decimate the current cryptographic foundations of our information and communication techno

The path to designing and deploying new foundations is long and hard, though progress is being made.

Will we be ready in time? Will this be part of our technology lifecycle management (and lead to more ro systems), or crisis management (and lead to weaker systems)? How will this impact blockchains? What should we do now?
Dr. Michele Mosca, Institute for Quantum Computing, ***University of Waterloo***

1:00-1:30 PM **Integrating Quantum Resistant Algorithms Into Applications**
Lessons Microsoft has learned from our prototype integrations into real-life protocols and applications (s TLS, SSH, and VPN), and Microsoft experiments on a variety of devices, ranging from IoT devices, to cl servers, to HSMs. I'll discuss the Open Quantum Safe project for PQC development, and related open-s of OpenSSL, OpenSSH, and OpenVPN that can be used to experiment with PQC today. I'll present a den (key exchange + authentication) PQC TLS 1.3 connection. This work sheds lights on the practicality of P

encouraging early adoption and experimentation by the security community."
Christian Paquin, ***Microsoft***

2:30-3:30 PM **Quantum-Safe VPN Appliance Solutions**
Dr. Michele Mosca, CEO, ***evolutionQ***
Tyson Macaulay, Chief Product Officer, ***InfoSec Global***

4:00-4:30 PM **NIST Post-Quantum Cryptography Standards Update**
In recent years, there has been a substantial amount of research on quantum computers – machines th
quantum mechanical phenomena to solve problems that are difficult or intractable for conventional com
large-scale quantum computers are ever built, they will be able to break the existing infrastructure of p
cryptography. NIST has initiated a process to develop and standardize public-key cryptographic algorit
are capable of protecting sensitive government information well into the foreseeable future, including af
advent of quantum computers. In this talk, I will provide an update on the NIST post-quantum crypto
"competition".
Dr. Dustin Moody, Mathematician, ***NIST***

4:35-5:00 PM **Open Quantum Safe Project Update**
Dr. Vlad Gheorghiu, ***University of Waterloo***

5:00-6:00 PM **Networking Reception**

Friday, September 7, 2018

8:30-9:30 **Hardware Security Modules (HSMs) Solutions for PQ Crypto**
It is important to highlight the need for HSMs to implement the hash-based signatures that are being st
through RFCs in the IETF along with the likelihood that NIST will adopt one or both of these as a USG st
There are also challenges that come with this approach including 1) the need to maintain state regardin
number of signatures issued as a critical security component, 2) the key generation process for hash-ba
signatures may take a significant amount of time, 3) larger key sizes. Also addressed will be protection
timing attacks for hash-based signatures in an HSM.
Roberta Faux, Director of Research, ***Envieta***

10:30-11:30 **Challenges in securing the IoT in a Post Quantum World**
This talk will look at what makes securing the IoT such a challenge, even against today's hackers, with
focus on addressing security at the device level. After a brief review of what the coming of quantum co
mean to the security methods now used, we will look at the potential crypto tools and what may be ava
address future security in the IoT.
Louis Parks, CEO, ***Secure RF***

12:00-1:00 PM **A Quantum Future Starts with Quantum Key Distribution (QKD) Today**
This presentation will introduce Quantum Xchange's technology for transmitting data securely over unli
distances, how this technology that is based on the laws of quantum physics is not weakened by quantu
computing or mathematical discoveries and promises unprecedented secrecy, as well as the company's
building the first QKD network that will eventually span the entire US.
John Prisco, CEO, ***Quantum Xchange***

Quantum Computing Sessions

Thursday, September 6, 2018

11:00 AM - 12:00 PM **Introduction to Quantum Computing, Prototype Applications, and Cybersecurity Analytics**
This talk gives a brief overview of the two primary quantum computing architectures being developed c
describes the D-Wave architecture at a high level, and reviews the growing number of prototype applica
developed by early D-Wave users. Finally, we describe some early uses of the D-Wave system for cybe

analytics.
Steve Reinhardt, Director of Customer Applications, ***D-Wave International***

1:00-2:00 PM **Understanding "Quantum Computing and Artificial Intelligence" for Non-Data Scientists**
Data science has been rapidly growing over the past decade, and its applications have become ubiquito daily lives. As these applications consume more data and need faster response times, new technologies algorithms are needed to meet the computational demands. Quantum computing is a highly promising technology that could present significant opportunities to accelerate the training of machine learning alg and improve data science methods
Dr. Maxwell Henderson, Senior Data Scientist, ***QxBranch***

2:30-3:00 PM **US Election 2016: Conventional Polling Models Predicted a Hillary 99% Chance of Winning: N a Quantum Computing Model Prediction**
This presentation will provide a practical example fo a quantum machine learning algorithm to model th Presidential election, showing potential in how quantum computing can be harnessed to advance machi
Dr. Maxwell Henderson, Senior Data Scientist, ***QxBranch***

3:00-3:30 PM **The 200-city World Capital Traveling Salesman Problem: Python Programming for a D-Wave Computer**
Joel M. Gottlieb, Ph.D., Senior Pre-Sales Analyst, ***D-Wave***

Track 1: Advanced HI-Tech Cyber Investigation Training Seminars Led by Law Enforcement Officers and Ph.D Computer Scientists

32 classroom training hours, presented by sworn law enforcement officers, Ph.D. Computer Scientists and nationally recognized cybercrime textbook authors and instructors. Distinguished ISS World Training Instructors include:

Wednesday, September 5, 2018

Seminar #1

9:00-5:00 PM

Online Social Media and Internet Investigations

Presented by: Charles Cohen, **Cohen Training and Consulting, LLC**; Charles Cohen also holds the position of Captain, Cyber Crimes Investigative Technologies Section, **Indiana State Police, USA**

9:00-10:00

Proxies, VPNs, and Dark Web: Identity Concealment and Location Obfuscation

10:15-11:15

Tor, onion routers, Deepnet, and Darknet: An Investigator's Perspective

11:30-12:30

Tor, onion routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators

1:30-2:30 PM

Cellular Handset Geolocation: Investigative Opportunities and Personal Security Risks

2:45-3:45 PM

Collecting Evidence from Online Social Media: Building a Cyber-OSINT Toolbox (Part 1)

4:00-5:00 PM

Collecting Evidence from Online Social Media: Building a Cyber-OSINT Toolbox (Part 2)

Seminar #2

9:00-5:00 PM

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, building their OSINT toolbox, and 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. How the system works for us, as investigators

How it works. Why it works. How it works for us .How data traffic leaves a trace ; What the internet is; what is an IP and how is it significant to trace a person. IPv4 and IPv6 – understanding the changes- the benefits and pitfalls for the investigator. The internet has millions of copies of data on it - why, and where can we find this. Tracking and evaluating data. MAC adders tracking.

10:15-11:15

Recognizing Traffic Data and digital profiling via social networks and devices - digital shadows

What data is available. How to harvest and analyze it. Best practice to identify suspects and build profiles. Good practice, virtual data 'housekeeping' and tradecraft .Data collection and interrogation, significance and value. IP usage, exploitation and dynamics; IP plotting and analysis how to look for suspect mistakes and exploit them (where they show their id). Dynamic approaches to identifying suspects through internet profiles. What investigators get from tech and service providers, and how to analyze it. Investigator capabilities and opportunities.

11:30-12:30

WIFI, geolocation, and Mobile Data traces and tracking

A detectives look at Wi-Fi, attribution, cell site data, GPRS location services and technology. How an investigator can track devices, attribute suspects locations, devices and movement. Unique communication identifiers. Dynamic live time tracing. Geo location services and uses. Online Surveillance and tracking movement and speed.

1:30-2:30 PM

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

How suspects are using emerging and new technologies.

An introduction to where technology is going, and how Law enforcement can use this to our advantages. dynamic and pro-active problem solving. Darknet, (Deep web) , TOR and IRC use. VOIP, Skype and FaceTime exploits. Advanced data sniffing and profile building. TOR systems, applications and ways to coax offenders out of the system.

2:45-3:45 PM

Advanced Techniques in Tracing Suspects, and lateral problem solving

Using innovative and dynamic methods to trace offenders. Tricks used by suspects and how to combat them- Play them at their own game?. Covert internet investigations. Proxy servers and hiding. Managing collateral intrusion. Reverse and social engineering. Thinking outside the box. Lateral thinking. Possible missed opportunities. Profile building and manhunts through device footprints, speed and movement.

4:00-5:00 PM

Open Source Tools, resources and techniques - A walk through my free law enforcement open source tools site

"Just google it" doesn't work anymore. A look at good tradecraft, practice and methodology in profiling, tracking and tracing digital footprints and shadows on the internet, by means of best

available tools. A look at a selection of 200+ tools available on Mark's open source law enforcement tools website, that search engines can't see, with login and password provided during the session. Do's and do nots. Best tools for best results. When was the last time you 'googled' something in an investigation, and it returned 5 results, all specifically relating to your suspect? This session will teach you how.

Seminar #3

9:00-10:00

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

Presented by: *Dr. Matthew Lucas (Ph.D, Computer Science), 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)
- Popular Altcoins used by Criminals and the New Challenges Facing Law Enforcement

Seminar #4

10:15-11:15

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 # 5

11:30-12:30

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 #6

1:30-2:30 PM

Understanding "The Very Basics" of Quantum Computing for Non-Engineers

Presented by: *Jerry Lucas, (Ph.D, Physics) President,* ***TeleStrategies***

This very basic, one-hour session is for cyber security and intelligence gathering professionals who must understand quantum computing technology basics to access artificial intelligence, machine learning as well as defeating encryption applications but do not have any significant advanced academic training in physics, mathematics nor engineering.

Specifically, this session covers:

- What potentially makes quantum computers more powerful than today's electronic computers: qubits, superpositioning, entanglement & interference (light on quantum mechanics)
- A one-to-one functional comparison of a general-purpose computer with an application specific quantum circuit designed to do but one thing, for example defeating today's public key encryption (light on computer technology)
- Qubit gates and circuits explained (light on the physics and mathematics)
- The basics of the three leading quantum computing architectures: Ion Traps, Superconducting Circuits and Annealing and the advantages and disadvatages of each.

- The key development challenges: qubit error correction, decoherence, algorithms and more.

- Leading general purpose quantum computing hardware options supported by IBM, Microsoft & Google for artificial intelligence, machine learning and optimization applications and the projected development time for each.

Seminar #7

2:45-3:45 PM

Understanding "Defeating Encryption" with Quantum Computing for Non-Engineers

Presented by: *Jerry Lucas, (Ph.D, Physics) President,* ***TeleStrategies***

Countless news articles have been written about quantum computers, the magic of entangled qubits and all the new business opportunities that will be created with these general-purpose computing machines. But what is not addressed in these articles is you don't need a general purpose quantum computer to defeat today's cryptography. While these general-purpose machines are likely years away from deployment, an application specific quantum circuit designed for one purpose only, e.g. defeating today's public key encryption may be but a few years away.

"Keep it simple but not that simple"
- Albert Einstein

This one hour, session is for cyber security executives and specialists who have the responsibility of assessing the lead time they have before deploying quantum safe cryptography solutions but don't have a technical background. If you believe nation state security agencies are developing quantum computing to decrypt your past and future intercepted transmission sessions, this high-level webinar should be a must attend briefing.

And to do this you need to understand how a quantum computing circuit works when designed for the sole purpose of defeating public key encryption.

- Matching qubits, entanglement and interference with quantum computing hardware.

- A Step-by-Step walk through of what goes on within a quantum circuit designed to process a small public encryption key as numerical input, probablistic measurements along the way through the delivery of numerical private key as output thereby defeating encryption (light on physics and mathematics as well)

- Quantum computer challenges with decrypting large public keys (e.g. RSA 2048 class) and the performance metrics (number of entangled qubits, logic gates, longevity, etc.) cyber security specialists need to be monitoring.

- Leading quantum computer hardware options supported by IBM, Microsoft & Google vs. defeating encryption only, application specific quantum circuit architectures.

Seminar #8

4:00-5:00 PM

Understanding "Post-Quantum Cryptography" for Non-Mathematicians

Presented by: *Jerry Lucas (Ph.D, Physics) President,* ***TeleStrategies***

This one hour session is for cyber security executives responsible for developing alternatives to todays cryptography infrastructure in response to the threat of quantum computing.

This session assumes attendees do not have the math background to understand the complexity of post-quantum algorithms but must be able to analyze PQ Crypto options under devleopment.

A. What are the leading PQ Crypto Algorithm Schemes under consideration explained without complex math

    a. Code-Based
    b. Lattice-Based
    c. Hash-Based
    d. Multivariate
    e. Supersingular Elliptic - Curve Isogeny

B. How to compare PC Crypto Algorithm Schemes regarding resource requirements, key sizes, etc.

    a. Signatures
    b. Public-Key Encryption
    c. Key Sized
    d. Key Pair Generation Time
    e. Ease of drop in Deployment

C. Quantum Key Distribution (QKD) Options

a. The quantum physics behind QKD
b. QKD option with Polarized light over a fiber path
c. Why Eve cannot successfully eavesdrop on Bob and Alice photon interexchange
d. What's needed for commercial, third party operation
e. What the QKD option can't do that PC Crypto algorithms can't and visa versa

D. Hardware Security Module (HSM) Options:

a. What's a Hardware Security Module (HSM), benefits and security infrastructure areas of deployment
b. What are Trusted Platform Modules (TPMs), relationship with HSM: and impact on existing cyber security infrastructure

Thursday, September 6, 2018

Seminar #9
9:00-10:00

Artificial Intelligence Technology: What Law Enforcement Needs to Know

Artificial intelligence and machine learning products are beginning to emerge in the law enforcement marketplace. But what exactly can they do, and how can they improve the effictiveness of LE?
This Session is focused on what is AI/ML; it’s the potential to help the LE community; and a hype vs. reality check. Topics include:

- What's artificial intelligence (AI) and machine learning (ML)?
- How AI/ML compares to legacy data analytic and mining products.
- The difference between AI/ML for law enforcement and government intel vs. private enterprise and commercial products.
- Potential applications of AI/ML for law enforcement (e.g., body-worn generated video analysis, social network communication connecting the dots, exposing cyber adversaries, pattern analytics and more)

- Emerging product offerings

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

Seminar #10

09:00-5:00 PM

Concerns and Considerations in Financial Crime Investigations

Presented by: *Michael Loughnane, CAMS, CFE,* ***Loughnane Associates, LLC*** *Mike is a former US Federal Law Enforcement Officer who specialized in complex fraud and cybercrime investigations and currently provides training to improve detection and investigations of fraud, money laundering and counter terror finance.*

The purpose of financial crime can be to generate or protect criminal profit. Locally or internationally, criminals face a continuous challenge of building structure to protect against the efforts of law enforcement and make their profits useable without fear of getting caught. Criminals will therefore build business and financial structures to mask their activities as well as launder money.

In this 1 day seminar we will discuss the tools and methods criminals use and the law enforcement response. Each presentation describes different elements of financial crime and business models used by criminals as well as law enforcement methods and tactics to identify and disrupt them. We will discuss the essentials in criminal networks, key players, money laundering, and trade based money laundering. We will describe how information can be found as money is moved around the world and how investigators can make best use of this knowledge. This training is aimed primarily at the investigator and analyst, but also has application to the law enforcement, intelligence, and financial regulatory community.

09:00-10:00 AM

Criminal Essentials: The Needs of a Criminal Network

11:00-12:00 PM

Financial Crime Schemes in Money Laundering

1:00-2:00 PM

The Essentials of Trade Based Money Laundering

2:30-3:30 PM

How Does Money Actually Move?

4:00-5:00 PM

Follow the Money Beyond the Banks

Seminar #11

4:00-5:00 PM

Advanced Analytic Techniques for Deanonymizing Hidden Network Digital Currency Transactions and Messaging Using Open Source and Commercial Software

Presented by: *Stephen Arnold, Managing Partner,* ***Arnold.IT***

In this session, Stephen E Arnold reviews technology-centric methods for deanonymizing hidden network activities. Based on research conducted for US federal agencies and research to support his work as a commissioner for the Judicial Commission of Inquiry into Human Trafficking and Child Sex Abuse.

Friday, September 7, 2018

Seminar #12

8:30-9:30

Practitioners Guide to Understanding Cyber Attacks on Banks - Exploring Vulnerabilities from The Perspective Of The Hacker

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

This one-hour session will explore the viewpoints of both the banks perception of vulnerabilities, and that of the attacker. A follow-up session at 10:30 will address Practitioners Guide to Defending Banks Against Cyber Attacks.

- What is the current typical attack
- Vulnerabilities leak points, and weak points
- Hacking the Bank by traditional social engineering
- Man in the middle/mobile (MITM)
- Man in the Browser (MITB) attacks
- DDOS, Zeus, Zbot, and other exploits
- BHO poisoning (browser helper objects)
- DNS poisoning
- Pineapple and Rasberry Pi devices
- Clickjacking
- Formgrabbers
- Cloning and contactless card vulnerabilities
- PCI-DSS attacks and vulnerabilities
- The hackers point of view

Seminar #13

10:30-11:30

Practitioners Guide to Defending Banks Against Cyber Attacks – Identifying And Protecting Vulnerabilities To Frustrate The Thief, and Integrity Proof The Systems

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

This one-hour session will explore the protection of weak points and future proofing banks against cyber attacks.

- PCI-DSS security and tightening
- WiFi encryption to avoid MITM
- Pen testing
- Dynamic virus signatures and monitoring
- End user verification and login
- Customer vulnerabilities and verification
- Quantum Dawn and Waking Shark II (wargaming) benefits
- Future proofing and horizon scanning
- Playing the hacker at his own game.

Seminar #14

12:00-1:00 PM

What Investigators and Intelligence Professionals Need to Know about Amazon's Disruptive Streaming Data Marketplace and Policeware Services

Presented by: *Stephen Arnold, Managing Partner,* ***Arnold.IT***

In this presentation, research completed by Stephen E Arnold and his research team to support their work related to the Judicial Commission's activities reveals the capabilities of Amazon's entrance into the policeware and intelligence analytics markets. ("Policeware" is shorthand for the vendors who provide data gathered via OSINT methods, software to analyze and make sense of OSINT and nonpublic data, and how certain investigative work will be performed.)

Seminar #15

12:00-1:00 PM

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

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

Seminar #16

8:30-1:00 PM

Special SS7 Intercept, Vulnerabilties and Most Damaging SS7 Infrastructure Attacks over the Last 12 Months

Presented by *Jean Gottschalk, Principal Consultant,* ***The Telecom Defense Limited Company***

8:30-9:30 AM

SS7 Vulnerabilities and Intercept Options

There are two very important aspects of telco SS7 infrastructure law enforcement and interior 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.

10:30-11:30 AM

The Most Damaging SS7 Network Infrastructure Attacks over the Last 12 Months

12:00-1:00 PM

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

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.