

"A good mixture of speakers and lively discussions."

Estonian Ministry of Defence, 2010 Cyber Defence Attendee

# CYBER DEFENCE

## Analysing Global Cyber Threats

16th & 17th May 2011, Istanbul Marriott Hotel, Turkey

### Our expert speakers include:



**Brigadier General Robert Rego**, Chief, Space and Cyberspace Operational Integration, **Headquarters USAF Space Command**



**Colonel Gérald Vernez**, Deputy Director, National Cyber Defence, **Swiss Armed Forces**



**Colonel Charles Williamson**, Deputy Staff Judge Advocate, **Headquarters US Air Force in Europe**



**Major Manik Jolly**, Commander, Cyber Security Cell, **Indian Army**



**Mehmet Eris**, Senior Researcher, **National Research Institute of Electronics and Cryptology (TUBITAK), Turkey**



**Suleyman Anil**, Head of Cyber Defence, Emerging Security Challenges Division, **NATO HQ\***



**Roger Halbheer**, Worldwide Chief Security Advisor, **Microsoft**



**Zahri Hj Yunos**, Chief Operating Officer, **CyberSecurity, Malaysia**



**Roger Kuhn**, Science Advisor to Fleet Cyber Command (FLTCYBERCOM)/Commander, 10th Fleet (C10F), Office of Naval Research, **US Navy**



**Dr. Udo Helmbrecht**, Executive Director, **European Network and Information Security Agency (ENISA)**



**Heli Tiirmaa-Klaar**, Senior Advisor, Policy Planning Department, **Ministry of Defence, Estonia**



**Yael Shahar**, Director, Database Project Institute for Counter-Terrorism, **IDC Herzliya, Israel**



**Dr. Markus Dürig**, Head of Division, IT Security, **Federal Ministry of the Interior, Germany**



**Peter Zinn**, Senior High Tech Crime Advisor, **National Police Services Agency (KLPD), Netherlands**



**Senior Representative**, Defence Security Branch, **Ministry of Defence, Italy**

Sponsored by



### PLUS A POST CONFERENCE INTERACTIVE WORKSHOP



Preparing for the next generation of ICS targeted attacks ...What Did We Learn from Stuxnet?

Wednesday 18th May 2011, Istanbul Marriott Hotel  
In Association With: **The Cyber Security Forum Initiative**



[www.cyber-defence.com](http://www.cyber-defence.com)

Register online or alternatively fax your registration to +44 (0) 870 9090 712 or call +44 (0) 870 9090 711

BOOK BY THE 28TH FEBRUARY AND SAVE £300



- 8.30 Registration & Coffee
- 9.00 **Chairman's Opening Remarks**  
**Geoff Harris**, Management Counsel, **Information Systems Security Association (ISSA), UK**
- 9.10 **OPENING KEYNOTE ADDRESS**  
**Mission Assurance: Thoughts on Cyber Defence**
- The world continues to increase its reliance on cyber infrastructure in every aspect of daily life
  - Bad actors recognize the low-cost opportunity this presents leading to an exponential increase in the threats we face
  - Mission assurance identifies mission critical cyber pathways, and provides mitigation alternatives and contributes to mission success
- Brigadier General Robert Rego**, Chief, Space and Cyberspace Operational Integration, **Headquarters USAF Space Command**
- 9.40 **Best Practice Cyber Defense, Based on Network Intelligence and Communications Metadata**
- The challenges of government cyber defence
  - Detecting cyber threats by scanning traffic
  - Using DPI & Network Intelligence to build a second line of cyber defence
  - Examples of technical implementations
  - Using communication metadata to detect suspicious traffic
- Erik Larsson**, VP, Marketing, **QOSMOS**

**NATIONAL DEFENCE**

- 10.20 **Turkish Cyber Defence & Malware Threat Trends**
- Malware problem definition
  - History of fight between computer virus authors and antivirus researchers
  - Current scale of malware problem
  - Malware ecosystem
  - Upcoming threats and research at TUBITAK
- Mehmet Eris**, Senior Researcher, **National Research Institute of Electronics and Cryptology (TUBITAK), Turkey**
- 10.50 Morning Coffee
- 11.10 **Setting up a National Cyber Defence Programme**
- About what threat characteristics are we talking about? Is it really only about IT?
  - Which level/part of the society is concerned? Can we separate civilian and military stakes?
  - Who are the players we should talk to? Can we limit our effort to the national level?
  - How does the threat evolve? Are today's solutions still valuable for tomorrow?
- Colonel Gérald Vernez**, Deputy Director, National Cyber Defence Project, **Swiss Armed Forces**
- 11.40 **Italy's National Cyber Defence Initiative**
- Latest programme updates and developments
  - What is the threat to critical infrastructure?
  - The cyber threat is evolving
  - What is the government's role?
  - International lessons
  - Challenges to come and future evolution
- Senior Representative**, Defence Security Branch, **Ministry of Defence, Italy**

- 12.10 **Analysing Open Source Cyber Intelligence**  
**Paul De Souza**, Founder, **Cyber Security Forum Initiative (CSFI)**
- 12.40 Networking Lunch
- 2.00 **DDoS as a Cyber Threat**
- Rising threat in 2010 of DDoS attacks
  - The fall-out from the Wikileaks attacks
  - Specific DDoS threats to Turkey
  - Precautions to prevent DDoS and BotNets
- Huzeyfe Onal**, Information Security Specialist, **Information Security Academy, Turkey**
- 2.30 **Cyber Operations**  
**Roger Kuhn**, Science Advisor to Fleet Cyber Command (FLTCYBERCOM)/Commander, 10th Fleet (C10F), **Office of Naval Research, US Navy**
- 3.00 **International Cooperation for Cyber Defence**
- Cyber Defence capability updates
  - International cyber security initiatives
  - National and international cooperation initiatives
  - The advantages of cyber interoperability
- Heli Tiirmaa-Klaar**, Senior Advisor, Policy Planning Department, **Ministry of Defence, Estonia**
- 3.30 Afternoon Tea
- 4.00 **Fighting Through the Law - Legal Aspects of Cyber Operations**
- An overview of the law of war for cyber operations
  - Challenges in creating international law and analyzing interpretation
  - Successes and failures of treaties on cyber law
  - Vision for the future for international collaboration in legislature
- Colonel Charles Williamson**, Deputy Staff Judge Advocate, **Headquarters US Air Force in Europe**

**CYBER TERRORISM**

- 4.30 **Fighting Cyber Terrorism - An Indian Approach**
- Cyber terrorism - Definition, scope and effects
  - Where the real problem lies
  - Moving beyond technology
  - Need for training - how, who and what
  - Strategy required at Global and regional levels
- Major Manik Jolly**, Commander, Cyber Security Cell, **Indian Army**
- 5.00 **Fourth-Generation Warfare: Terrorism and Counter-Terrorism in Cyber Space**
- The changing nature of warfare
  - Growing emphasis on perception and psychology
  - Are non-state actors the necessary 'victors' in a Fourth Generation War?
  - What role does intervention on the part of third parties have on the outcome of Fourth Generation Conflicts?
- Yael Shahar**, Director, Database Project Institute for Counter-Terrorism, **IDC Herzliya**
- 5.50 **Chairman's Closing Remarks and Close of Day One**

• Register online at [www.cyber-defence.com](http://www.cyber-defence.com) • Alternatively fax your registration to -

Supported by



8.30 Registration & Coffee

9.00 **Chairman's Opening Remarks**  
**Geoff Harris**, Management Counsel, **Information Systems Security Association (ISSA), UK**

**KEYNOTE ADDRESS**

9.10 **The Cyber Defence Response in Malaysia**  
 • Current cyber security threats posed in Malaysia  
 • Terrorism vs cyber terrorism  
 • Malaysia's Critical National Information Infrastructure  
 • The use of ICT and cyberspace by terrorists  
 • Malaysia's National Cyber Security Policy  
**Zahri Hj Yunos**, Chief Operating Officer, **CyberSecurity Malaysia**

**SPECIAL ADDRESS**

9.40 **NATO's Role in Cyber Defence**  
**Suleyman Anil**, Head of Cyber Defence, Emerging Security Challenges Division, **NATO \***

**CYBER CRIME & BUSINESS CONTINUITY**

10.10 **The Economy of Cybercrime**  
 • What are the general IT trends that impact cyber security?  
 • What is the economy behind Cybercrime?  
 • What can we as societies/industries/governments do to fight it?  
**Roger Halbheer**, Worldwide Chief Security Advisor, **Microsoft**

10.40 Morning Coffee

11.00 **Introduction to ENISA and its Activities**  
 • Key activities for 2011  
 • ENISA's role in protecting Critical Information Infrastructure  
 • The European Cybersecurity Exercise – conclusions and further development  
 • ENISA and Cloud Computing  
 • Conclusions  
**Dr. Udo Helmbrecht**, Executive Director, **European Network and Information Security Agency (ENISA)**

11.30 **Taking Down a Botnet - A Case Study**  
 • Cybercrime grows at a large rate. So does the fight against it. But is that enough?  
 • New cooperation and methods are needed to combat cybercrime  
 • The Dutch National High Tech Crime Unit  
 • The takedown of "Bredolab" and the arrest of its maker  
 • What more can be done?  
**Peter Zinn**, Senior High Tech Crime Advisor, **National Police Services Agency (KLPD), Netherlands**

12.00 **The Global Cyber Threats From a Banking Sector Perspective**  
 • The threats posed to banks  
 • The need to develop more intelligence sharing between critical national infrastructure and government  
 • Solutions - working together on common threats  
**Tim Hind**, Head of Intelligence, **Barclays Global Retail Bank (Technology)**

12.30 Networking Lunch

**SOLUTIONS & INITIATIVES**

1.50 **Internet Protocol Version 6**  
 • Main design goals and features  
 • Implementation hurdles  
 • Security issues  
 • IPv6 attack scenarios  
**Lou Giannelli CISSP**, Senior Adversary Cyber Threat Analyst, **US Air Force**

2.20 **German IT Security Architecture**  
**Dr. Markus Dürig**, Head of Division, IT Security, **Federal Ministry of the Interior, Germany**

2.50 **The German Anti Botnet Initiative**  
 • Benefits of the programme  
 • The role of ISPs in order to curb malware and particularly Botnets  
 • The role of the government in setting incentives  
 • Collaboration with German Internet industry  
**Heinz-Jürgen Treib**, Division of IT Security, **Federal Ministry of Interior, Germany**

3.20 Afternoon Tea

3.40 **DNS Security Extensions (DNSSEC)**  
 • Benefits of DNSSEC  
 • Protection from cache poisoning  
 • Relevance in protecting critical infrastructure  
 • Protecting Critical Infrastructure from Malware  
**Ron Broersma**, Chief Engineer of the Defence Research and Engineering Network (DREN), SPAWAR, **US Navy**

4.10 **US-NATO Information Sharing - Improving Alliance Cyber Defence Capabilities**  
 • Implementing Cyber Defence policy in a multinational environment  
 • Current Cyber Defence information sharing framework  
 • Improving Cyber Defence tactics, techniques and procedures  
 • Maturing and developing Cyber Defence technologies  
**Daniel John Mills**, Chief, U.S. National Technical Experts Office (NATO), **Defense Information Systems Agency (DISA)**

4.40 **Automated Run-Time Analysis of Malicious Codes**  
 • Benefits of automated system in a massive file analysis problem  
 • Observe malware on simulated internet (Anexa, Product of SEI)  
 • Provide analytical results of the behaviour of malware  
 • Create classification of the malware to address the source  
**Hasan Yasar**, Engineering and Development, Digital Investigations and Intelligence, US-CERT, **Carnegie Mellon University**

5.10 **Chairman's Closing Remarks and Close of Conference**

Subject to final confirmation \*

+44 (0) 870 9090 712 or call +44 (0) 870 9090 711 • REGIONAL DISCOUNTS AVAILABLE •



# Full Day Interactive Workshop

Wednesday 18th May 2011, 9.00-17.00,  
Istanbul Marriott Hotel

## Preparing for the next generation of ICS targeted attacks...What Did We Learn from Stuxnet?

In Association with



### Why Attend this Workshop?

- Learn about how a successful cyber attack was launched against the industrial control systems used to protect critical infrastructure
- See how potential attackers can launch similar attacks on other control systems
- Understand how to apply technical and administrative controls to protect control systems from future attacks

### Workshop Key Objectives:

- Analyse the key aspects of the Siemens Stuxnet worm as it relates to infection, installation, propagation, and control
- Discuss current industrial control system vulnerabilities that can be exploited by cyber attackers
- Review what vendors have done to identify and attempt to prevent Stuxnet infections on industrial control systems
- Evaluate various administrative and technical security controls that can be used to mitigate future Stuxnet-like attacks
- Demonstrate how Stuxnet intellectual property can be used to exploit other control system platforms

### Benefits of Attending:

- Increase your understanding of how vulnerable industrial control systems are to cyber attacks and how these attacks can be used as a cyber weapon
- Improve your knowledge of potential security controls or countermeasures that can be implemented to mitigate the risk of a potential attack
- Understand the actions that can be performed once an industrial control system is compromised

### About your workshop leaders:



**Paul de Souza** is the Founder Director of CSFI (Cyber Security Forum Initiative) and its divisions CSFI-CWD (Cyber Warfare Division) and CSFI-LPD (Law and Policy Division). CSFI is a non-profit organization with headquarters in Omaha, NE. Paul has over 11 years of cyber security experience and has worked as a Chief Security Engineer for AT&T where he designed and approved secure networks for MSS. Paul has also consulted for several governments, military and private institutions on best network security practices.



**Joel Langill**, CSFI SCADA Engineer/SCADAhacker.com Founder. Joel is an industrial control systems security specialist and founder of SCADAhacker.com. His employers include major companies such as General Electric, Shell Oil Company, Honeywell Process Solutions, and ENGlobal Automation, offering him a rare and insightful expertise in the risks and mitigation of cyber vulnerabilities in industrial control systems. Most recently he has played a central role in the analysis and implications of the Stuxnet worm, including new methods of mitigating current and future attacks on critical infrastructure. He is a Certified Ethical Hacker, Certified Penetration Test, Cisco Certified Network Associate, and TÜV Functional Safety Engineer.

Sponsored by



**Qosmos** delivers software development kits and intelligent IP probes which recognize thousands of protocols and metadata attributes for the most accurate picture of network activity. Going beyond DPI technology, Qosmos Network Intelligence products are used by developers, Solution Vendors and Systems Integrators to enhance government cyber security and interception solutions.

[www.qosmos.com](http://www.qosmos.com)

## SMi's Defence and Security Forward Schedule

### FEBRUARY

#### **Offsets 2011**

7th & 8th February 2011  
Sheraton Sofia Hotel Balkan, Sofia

#### **Mobile Deployable Communications**

28th February & 1st March 2011  
Marriott Prague, Prague

#### **Border Security 2011**

28th February & 1st March 2011  
Sheraton Sofia Hotel Balkan, Sofia

### APRIL

#### **MilSpace 2011**

4th & 5th April 2011  
Radisson SAS Hotel, Paris Boulogne, Paris

#### **CBRN-E Asia Pacific**

11th & 12th April 2011  
Grand Copthorne Waterfront Hotel,  
Singapore

### MAY

#### **MilSatCom Asia**

23rd & 24th May 2011  
Swissôtel Merchant Court, Singapore

### JUNE

#### **International Software Radio**

6th & 7th June 2011  
Copthorne Tara Hotel, London

#### **Maritime Domain Awareness**

20th & 21st June 2011  
Crowne Plaza Hotel, London

# CYBER DEFENCE

Conference: 16th & 17th May 2011, Istanbul Marriott Hotel, Turkey Workshop: 18th May 2011, Istanbul Marriott Hotel

## 4 WAYS TO REGISTER

ONLINE at [www.cyber-defence.com](http://www.cyber-defence.com)

FAX your booking form to +44 (0) 870 9090 712

PHONE on +44 (0) 870 9090 711

POST your booking form to: Events Team, SMi Group Ltd, Great Guildford Business Square, 30 Great Guildford Street London, SE1 0HS, UK

--	--

Unique Reference Number	
Our Reference	LVX36

### DELEGATE DETAILS

Please complete fully and clearly in capital letters. Please photocopy for additional delegates.

Title: Forename: \_\_\_\_\_

Surname: \_\_\_\_\_

Job Title: \_\_\_\_\_

Department/Division: \_\_\_\_\_

Company/Organisation: \_\_\_\_\_

Email: \_\_\_\_\_

Address: \_\_\_\_\_

Town/City: \_\_\_\_\_

Post/Zip Code: Country: \_\_\_\_\_

Direct Tel: Direct Fax: \_\_\_\_\_

Mobile: \_\_\_\_\_

Switchboard: \_\_\_\_\_

Signature: Date: \_\_\_\_\_

I agree to be bound by SMi's Terms and Conditions of Booking.

#### ACCOUNTS DEPT

Title: Forename: \_\_\_\_\_

Surname: \_\_\_\_\_

Email: \_\_\_\_\_

Address (if different from above): \_\_\_\_\_

Town/City: \_\_\_\_\_

Post/Zip Code: Country: \_\_\_\_\_

Direct Tel: Direct Fax: \_\_\_\_\_

### Terms and Conditions of Booking

**Payment:** If payment is not made at the time of booking, then an invoice will be issued and must be paid immediately and prior to the start of the event. If payment has not been received then credit card details will be requested and payment taken before entry to the event. Bookings within 7 days of event require payment on booking. CD Roms will not be dispatched until payment has been received.

**Substitutions/Name Changes:** If you are unable to attend you may nominate, in writing, another delegate to take your place at any time prior to the start of the event. Two or more delegates may not 'share' a place at an event. Please make separate bookings for each delegate.

**Cancellation:** If you wish to cancel your attendance at an event and you are unable to send a substitute, then we will refund/credit 50% of the due fee less a £50 administration charge, providing that cancellation is made in writing and received at least 28 days prior to the start of the event. Regrettably cancellation after this time cannot be accepted. We will however provide the Conference documentation on CD ROM to any delegate who has paid but is unable to attend for any reason. Due to the interactive nature of the Briefings we are not normally able to provide documentation in these circumstances. We cannot accept cancellations of orders placed for Documentation or CD ROM as these are reproduced specifically to order. If we have to cancel the event for any reason, then we will make a full refund immediately, but disclaim any further liability.

**Alterations:** It may become necessary for us to make alterations to the content, speakers, timing, venue or date of the event compared to the advertised programme.

**Data Protection:** The SMi Group gathers personal data in accordance with the UK Data Protection Act 1998 and we may use this to contact you by telephone, fax, post or email to tell you about other products and services. Unless you tick here  we may also share your data with third parties offering complementary products or services. If you have any queries or want to update any of the data that we hold then please contact our Database Manager [databasemanager@smi-online.co.uk](mailto:databasemanager@smi-online.co.uk) or visit our website [www.smi-online.co.uk/updates](http://www.smi-online.co.uk/updates) quoting the URN as detailed above your address on the attached letter.

### EARLY BIRD DISCOUNT

Book by the 28th February and save £300

### CONFERENCE PRICES

I would like to attend: (Please tick as appropriate)	Fee
<b>MILITARY, GOVERNMENT &amp; PUBLIC SECTOR RATE</b>	
<input type="checkbox"/> Conference & Interactive Workshop	£1498.00
<input type="checkbox"/> Conference only	£899.00
<input type="checkbox"/> Interactive Workshop only	£599.00
<b>COMMERCIAL ORGANISATIONS</b>	
<input type="checkbox"/> Conference & Interactive Workshop	£2098.00
<input type="checkbox"/> Conference only	£1499.00
<input type="checkbox"/> Interactive Workshop only	£599.00
<b>PROMOTIONAL LITERATURE DISTRIBUTION</b>	
<input type="checkbox"/> Distribution of your company's promotional literature to all conference attendees	£999.00 + VAT £1198.80

### GROUP DISCOUNTS AVAILABLE

The Conference fee includes refreshments, lunch, conference papers and CD ROM containing all of the presentations.

### VENUE Istanbul Marriott Hotel, Turkey

Please contact me to book my hotel

Alternatively call us on +44 (0) 870 9090 711, email: [hotels@smi-online.co.uk](mailto:hotels@smi-online.co.uk) or fax +44 (0) 870 9090 712

### CD ROMS/DOCUMENTATION

I cannot attend but would like to purchase the following CD ROMs/paper copy documentation: (Shipped 10-14 days after the event)	Price	Total
<input type="checkbox"/> The Conference Presentations on CD ROM	£499.00 + VAT	£598.80
<input type="checkbox"/> The Conference Presentations - paper copy (or only £300 if ordered with a CD ROM)	£499.00 -	£499.00

### PAYMENT

Payment must be made to SMi Group Ltd, and received before the event, by one of the following methods quoting reference X36 and the delegate's name. Bookings made within 7 days of the event require payment on booking, methods of payment are below. Please indicate method of payment:

- UK BACS Sort Code 300009, Account 00936418
- Wire Transfer Lloyds TSB Bank Plc, 39 Threadneedle Street, London, EC2R 8AU Swift (BIC): LOYDGB21013, Account 00936418 IBAN GB48 LOYD 3000 0900 9364 18
- Cheque We can only accept Sterling cheques drawn on a UK bank.
- Credit Card  Visa  MasterCard  American Express

All credit card payments will be subject to standard credit card charges.

Card No:

Valid From   /   Expiry Date   /

CVV Number    3 digit security on reverse of card, 4 digits for AMEX card

Cardholder's Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

I agree to be bound by SMi's Terms and Conditions of Booking.

Card Billing Address (if different from above): \_\_\_\_\_

### VAT

VAT at 20% is charged on CD ROMs and Literature Distribution for all UK customers and for those EU customers not supplying a registration number for their own country here: \_\_\_\_\_