



The Cyber Security Forum Initiative (CSFI) <http://www.csfi.us/> and NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) <http://www.ccdcoe.org/> will be presenting a unique workshop on the online recruitment of volunteers for enhancing the instruments of cyber power of nations and organizations. This is a great opportunity to learn more about methodologies, lessons learned, deliverables, coordination and volunteerism in cyberspace.

The workshop will take place at the 3rd International Conference on Cyber Conflict, June 7-10, 2011 in Tallinn, Estonia. CSFI members will have a special discount. Register at: <https://www.ccdcoe.org/reg/457117215>.

## **RECRUITING CYBER POWER WORKSHOP**

JUNE 7-10, 2011 in Tallinn, Estonia

## Rain Ottis (Estonia)

Rain Ottis is a scientist at the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. He has previously served as an officer in the Estonian Defence Forces, where he focused on cyber defence training and awareness programs. He is a graduate of the US Military Academy and Tallinn University of Technology. His research interests include cyber conflict, especially the role of non-state actors.

### **Presentation: Politically Motivated Cyber Attacks**

Rain will present his research on politically motivated cyber-attacks by non-state groups, discussing the various ways they can be organized, their strengths and weaknesses, as well as some potential countermeasures.

## Alexander Klimburg (Austria)

Alexander Klimburg is a Fellow at the Austrian Institute for International Affairs and has acted as an advisor to government on national security issues, especially within Cyber Security, Critical Infrastructure Protection (CIP), and EU Common and Foreign Security Policy (CFSP). Mr. Klimburg has partaken in international and intergovernmental discussions, has acted as an advisor to the Austrian delegation at the OSCE and has been a member of various national and EU-level policy and working groups. Mr. Klimburg has consulted to various national governments and governmental institutions and works closely with the Austrian Office of the National Security Council.

### **Presentation: Mobilising Cyber Power**

Cyber crime, cyber terrorism and cyber warfare share a common technological basis, tools, logistics and operational methods. They can also share the same social networks and have comparable goals. The differences between these categories of cyber activity are often razor thin or only in the eye of the beholder. From the perspective of a cyber warrior, **cyber-crime** can offer the technical basis (software tools and logistic support) and cyber terrorism the social basis (personal networks and motivation) with which to execute attacks on the computer networks of enemy groups or nations.

## Roger Kuhn (USA)

Roger Kuhn graduated from the United States Coast Guard Academy in 1989 earning a commission as an Ensign and a Bachelor of Science degree in Electrical Engineering (EE). Mr. Kuhn was selected to serve as ONR Science Advisor (SA) to Naval Network Warfare Command (NETWARCOM). In August 2010, following the establishment of Fleet Cyber Command/Commander, 10th Fleet (FLTCYBERCOM/C10F), he was re-selected as the 1st ONR SA assigned to FLTCYBERCOM/C10F.

Among his many professional credentials, Mr. Kuhn is an experienced & registered DoD IA professional (Certified Information Systems Security Professional) and a recognized member of the NSWC Dahlgren Division's Science and Technology community, having earned & executed over \$3.0M in ONR & OSD applied science grants pertaining to mobile wireless networking technologies.

### **Presentation: The Conceptual Construct for Developing a Cyber Operations Workforce**

## Joint Presentation by Paul de Souza, Don Eijndhoven, and Anand Shah

### Paul de Souza (USA) 🇺🇸

Paul de Souza is the Founder/President/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 with offices in Washington, DC. 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. Paul presents all over the world on cyber warfare issues and works as a cyber security advisor to many organizations and governments around the world.

### Don Eijndhoven (Holland) 🇳🇱

Don Eijndhoven is the CEO of Argent Consulting, a Dutch Cyber Security firm; a Security & Infrastructure Architect; and is a resident blogger at ArgentConsulting.nl, InfoSecIsland, IT GRC Forum and International Cyber Threat Task Force (ICTTF). Mr. Eijndhoven is a long-time CSFI member and EMEA-region Assistant Secretary. He currently serves as the Lead Project Manager on two CSFI projects: CSSF and the Cyber Entities project.

### Anand Shah (USA) 🇺🇸

Anand Shah is a law student at Emory University School of Law – Juris Doctor Candidate, 2012 and Summer 2011 Associate at SNR Denton LLP – Internet & Data Protection practice in Washington, DC. His legal interests include Cyber Warfare, Intellectual Property, Technology Commercialization, Internet Policy, Cyber Crime, and International Humanitarian Law. Mr. Shah's research experience includes CCDCOE's Manual on International Law Applicable to Cyber Warfare (The Tallinn Manual) – Research Assistant to the Group of Experts. His work experience includes the following: government (e.g., U.S. Dept. of Justice), academia (e.g., Prof. Michael Schmitt), and private-sector (e.g., Rohm & Haas Co.-Dow Chemical).

Anand Shah is currently serving as the Lead Project Manager for CIAP (Cyber Intelligence Analysis Project) – CSFI.

## Presentation: Recruiting Cyber Power

This presentation will cover the details of how CSFI manages to recruit and retain volunteers and create deliverables through the power of social networking. Topics such as volunteer motivation, shared issues, vetting process, collaborative platform, group communication, and information dissemination will be covered.



*Tallinn is ranked as a global city and has been listed among the top 10 digital cities in the world. Tallinn is a European Capital of Culture for 2011, along with Turku, Finland.*



## Jeffrey S Bardin (USA)

Since 1982 Jeff Bardin has worked in leadership positions for organizations such as General Electric, Lockheed Martin, and Marriott International. He also served as the Security Manager for the Centers for Medicare and Medicaid (LMI), Chief Security Officer for Hanover Insurance, the Chief Information Security Officer for Investors Bank & Trust, and the Director, Office of Risk Management for EMC. Mr. Bardin is currently the Chief Security Strategist for Treadstone 71.

In 2007 Jeff Bardin was awarded the RSA Conference Award for Excellence in the Field of Security Practices. The Bardin-led security team from Hanover Insurance also won the 2007 SC Magazine Award – Best Security Team competing against such organizations as Barclays Global and the Department of State.

Jeff Bardin sits on the Board of Directors for Boston Infragard, was a founding member of the Cloud Security Alliance, is a member of the Cyber Security Forum Initiative and sits on the RSA Conference Submission Selection Committee. Mr. Bardin published his first book, *The Illusion of Due Diligence* in 2010 and has co-authored other books such as the *Computer and Information Security Handbook* and *Understanding Computers*, and has published articles for magazines such as *The Intelligencer*.

Jeff Bardin served in the USAF as a cryptologic linguist (overseas and at the NSA), the USANG as an officer, holding a Top Secret SCI/SBI clearance. He has BA in Special Studies - Middle East Studies & Arabic Language from Trinity College as well as a MS in Information Assurance from Norwich University. He is also a professor of masters programs in cyber intelligence/counter-intelligence at Utica College and information security at Clark University. Mr. Bardin also holds the CISSP, CISM and NSA-IAM certifications.

## **Presentation: Hacktivism and National Security**

Hacktivism, cyber vigilantes, cyber militias, and anonymous volunteerism have taken hold with active offensive cyber operations. Citizen groups are battling governments and cyber militias are battling each other using cyber intelligence and counterintelligence techniques. A lack of common approach and less centralized oversight to offensive cyber operations exists among law enforcement, government and intelligence organizations. This seminar will explore some of the participants in these battles, their methods, as well as the proliferation of virtual small arms.