

Managing Cyber Risk through Recovery Driven Resilience



February 14, 2011
Marshall Hall 155
National Defense University
and
George Mason University
Fort Lesley J. McNair





Managing Cyber Risk through Recovery Driven Resilience



Part of the Cyber Resilience Workshop Series
Marshall Hall, Room 155, Fort Lesley J. McNair, Washington, DC 20319
February 14, 2012

Tuesday, February 14th - Risk and Recovery

0800-0830 Registration and Networking

0830-0840 Welcome

- **Dr. James Keagle**, Distinguished Research Fellow, Center for Technology and National Security Policy, National Defense University

0840-0900 Introduction

- **Dr. Arun Sood**, Professor & Co-Director, International Cyber Center, George Mason University

0900-0945 Keynote Speaker

- **Lt. Gen (Ret.) Harry D. Raduege Jr.**, Chairman, Deloitte Center for Cyber Innovation; Director, Deloitte Services LP, former Director of the Defense Information Systems Agency

0945-1000 Question and Answer Session

1000-1015 Coffee Break

1015-1115 Panel: Requirements and Forms of Resilience

- **Moderator: Dr. James Keagle**, Distinguished Research Fellow, CTNSP
- **Dr. Sam Liles**, Associate Professor, CI&IO, National Defense University
- **Dr. Shari Pfleeger**, Director of Research, Institute for Information Infrastructure Protection, Dartmouth College
- **Dean Weber**, Chief Technology Officer, CSC

1115-1215 Panel: Implementation of Recovery Driven Resilience

- **Moderator: Dr. Vitalij Garber**, Consultant to Director, Joint Capability Technical Demonstrations
- **Dr. Tim Gibson**, Assistant Director, Cyber Systems, Draper Laboratory
- **Dr. Arun Sood**, Professor, ICC, George Mason University

1215-1230 Closing Remarks



SPEAKER BIOGRAPHIES



Dr. Vitalij Garber

Vitalij Garber is currently Adjunct Professor and Senior Fellow at the George Mason University International Cyber Center. He retired as Director, Interoperability, Department of Defense, after being in private sector as CEO of Garber International Associates, which he founded in December 1983. He has started several successful companies and has extensive industrial experience in forming international partnerships and joint ventures. He served on many Defense Science Board task forces dealing with future operations and interoperability. From January 1981 through November 1983, Dr. Garber was the Assistant Secretary General at NATO for Defense Support. Dr. Garber served as the permanent Chairman of the Conference of National Armaments Directors and the Senior NATO C2 Committee. Previously, Dr. Garber was the Deputy Under Secretary of Defense for International Programs and Technology. He was responsible for all Department of Defense international activities in research, development, and acquisition. Dr Garber received his BS and MS Degrees in Physics from the University of Minnesota (1959 and 1962), Ph.D. from the University of Alabama (1966), and performed post-doctoral work at Harvard University (1966-67). He served as an Army Officer, and completed the U.S. Army Infantry Officer's Leadership, the Airborne, and the Armor Officers' Career Courses. After his military service, Dr. Garber was with the Army Missile Command Laboratories in Huntsville, Alabama, where he specialized in optimum control theory.

Dr. Timothy Gibson

Tim Gibson is the Assistant Director of Cyber Systems at Draper Laboratory. Prior to his work at Draper, Dr. Gibson was the Director of Cyber Security Development at Hewlett-Packard where he served as a subject matter expert and internal consultant within HP for cyber security, networking technologies, intellectual property rights language in contracts and proposals, and ITAR issues. Before that, Dr. Gibson worked as a Program Manager at the Defense Advanced Research Projects Agency (DARPA) where he developed concepts and ideas for new research projects as well as acted as a subject matter expert on multi-level security, anti-tamper technologies, cryptographic systems, and satellite data throughput. Dr. Gibson has also performed in a number of high profile positions at the National Security Agency, Department of Defense, and US Pacific Command. Dr. Gibson received his PhD in Computer Science from the University of Maryland after serving with the U.S. Army in a number of roles.

Dr. James Keagle

Dr. James M. Keagle is the Director of the Transforming National Security seminar series at the Center for Technology and National Security Policy at the National Defense University. Prior to this position, Dr. Keagle served for nine years as the National Defense University's Provost (effective 2004) and Vice President for Academic Affairs (effective 1999). Prior to



SPEAKER BIOGRAPHIES



these positions, he served as a professor of National Security Strategy at NDU. In that role Dr. Keagle worked as a research faculty member assisting with NDU's modeling and simulation and work with interagency education and training. Accepting an appointment to the U.S. Air Force Academy, he graduated 2nd academically in his class in June 1974. Following graduation, he went to the University of Pittsburgh to complete his Master's of Arts degree in political science and earned a graduate certificate in Latin American studies (1975). After a tour as a munitions maintenance officer, Dr. Keagle went on to become an assistant professor of political science at the U.S. Air Force Academy. In 1980, he went on to Princeton University where he completed both a Master's of Arts degree (1981) and Ph.D. (1982) in politics. He proudly notes his honorary Ph.D from the Military Technical Academy of Romania--the only United States citizen so honored. Following his extensive education, Dr. Keagle's next six tours were political-military assignment that included direct access and interaction with Cabinet-level government officials on national security related matters. These assignments included work for two Combatant Commanders as a senior strategist; for the Office of Secretary of Defense pertaining to Cuba; Deputy Director, Office of the Secretary of Defense Bosnian Task Force; and for the Deputy Under Secretary of the Air Force in International Affairs as Senior Strategist. Military. For the last two years he has led multiple NATO and Defense Education Enhancement Teams to Georgia, Azerbaijan, and Montenegro. Since leaving military service, Dr. Keagle has held the position of adjunct professor at a number of institutions to include: Syracuse University, American University, Central Michigan University, Catholic University, University of Colorado, and Lake Superior State College. He also holds an honorary professorships with Transilvania University in Brasov, Romania, as well as the Mongolian Defense University--again, the only American so honored . Dr. Keagle and wife Kay are the proud parents of three adult children.

Dr. Samuel Liles

Samuel Liles, is an associate professor at National Defense University. Previously he was a tenured associate professor of computer information technology at Purdue University Calumet. He teaches information assurance and security. Samuel created an extensive laboratory for information assurance and security including a virtual laboratory environment at Purdue University Calumet. As a researcher his interest is in cyber warfare as a form of low intensity conflict. Currently Samuel Liles completed his PhD at Purdue University primarily studying cyber conflict, issues of cyber conflict, information assurance and security, and cyber forensics.

Dr. Shari Pfleeger

Shari Lawrence Pfleeger is the Director of Research for the Institute for Information Infrastructure Protection at Dartmouth College, a consortium of leading universities,



SPEAKER BIOGRAPHIES



national laboratories and nonprofit institutions dedicated to strengthening the cyber infrastructure of the United States. From 2002 to 2010, Shari was a senior researcher at the RAND Corporation, a not-for-profit company doing high-quality, high-impact research in the public interest. At RAND, she worked on policy and decision-making issues that helped organizations and government agencies understand whether and how information technology supports their mission and goals. From 1982 to 2002, Dr. Pfleeger was president of Systems/Software, Inc., a consultancy specializing in software engineering and technology. From 1997 to 2000, she was also a visiting professor at the University of Maryland's computer science department. She was founder and director of Howard University's Center for Research in Evaluating Software Technology (CREST), and was a visiting scientist at the City University (London) Centre for Software Reliability, principal scientist at MITRE Corporation's Software Engineering Center, and manager of the measurement program at the Contel Technology Center. Dr. Pfleeger is currently an associate editor of IEEE Security and Privacy. For several years, she was associate editor-in-chief of IEEE Software, where she edited the Quality Time column, and then associate editor of IEEE Transactions on Software Engineering. From 1998 to 2002, she was a member of the editorial board of Prentice Hall's Software Quality Institute series. A member of IEEE, the IEEE Computer Society, and the Association for Computing Machinery, Pfleeger was elected to the executive committee of the Technical Council on Software Engineering from 1996 to 2000.

LTG (Ret) Harry Raduege

Lieutenant General Harry D. Raduege, Jr. (USAF, Ret), is chairman of the Deloitte Center for Network Innovation, part of Deloitte LLP. He retired after serving 35 years in the U.S. military. He worked in the areas of technology, including telecommunications, space, information and network operations. He served more than 17 years in joint duty assignments. In his last position, he led Department of Defense netcentric operations as the director of the Defense Information Systems Agency. General Raduege was also appointed by the secretary of defense as the commander of the Joint Task Force for Global Network Operations, and as deputy commander for Global Network Operations and Defense for the U.S. Strategic Command. In these roles, he was the first commander assigned responsibility for directing the operation and defense of the Global Information Grid to ensure timely and secure netcentric capabilities across the entire department. He also served as the manager of the National Communications System and led the nation's efforts to prioritize the restoration of telecommunications throughout New York City and the Pentagon following the 9/11 attacks. General Raduege currently serves as a senior counselor to The Cohen Group; on the World Board of Governors of the United Services Organizations (USO); on the Executive Council of the Network Centric Operations Industry Consortium (NCOIC); as co-chair of the Center for Strategic and International Studies' (CSIS) Commission on Cyber Security for



SPEAKER BIOGRAPHIES



the 44th Presidency; as a member of the Center for U.S. Global Engagement's National Security Advisory Council and; on the Board of Directors and Executive Committee of Armed Forces Communications and Electronics Association (AFCEA) International. He also serves as an advisor to the Defense Science Board, and is a member of the Board of Trustees and chairs the Technology Committee for Capital University in Columbus, Ohio.

Dr. Arun Sood

Dr. Arun Sood is Professor of Computer Science in the Department of Computer Science, and Co-Director of the International Cyber Center at George Mason University, Fairfax, VA. His research interests are in security architectures; image and multimedia computing; performance modeling and evaluation; simulation, modeling, and optimization.

He and his team of faculty and students have developed a new approach to server security, called Self Cleansing Intrusion Tolerance (SCIT). We convert static servers into dynamic servers and reduce the exposure of the servers, while maintaining uninterrupted service.

This research has been supported by US Army, NIST through the Critical Infrastructure Program, SUN, Lockheed Martin, Commonwealth of Virginia CTRF (in partnership with Northrop Grumman). Recently SCIT technology was winner of the Global Security Challenge (GSC) sponsored Securities Technologies for Tomorrow Challenge. GSC is associated with London Business School. Since 2009 Dr. Sood has directed an annual workshop on Cyber Security and Global Affairs with Office of Naval Research support. Dr. Sood has held academic positions at Wayne State University, Detroit, MI, Louisiana State University, Baton Rouge, and IIT, Delhi. His has been supported by the Office of Naval Research, NIMA (now NGA), National Science Foundation, U.S. Army Belvoir RD&E Center, U. S. Army TACOM, U.S. Department of Transportation, and private industry. He was awarded grants by NATO to organize and direct advance study institutes in relational database machine architecture and active perception and robot vision. Dr. Sood received the B.Tech degree from the Indian Institute of Technology (IIT), Delhi, in 1966, and the M.S. and Ph.D. degrees in Electrical Engineering from Carnegie Mellon University, Pittsburgh, PA, in 1967 and 1971, respectively.

His research has resulted in more than 160 publications, 4 patents, 3 additional patent applications, and his resume including publications list is available at <http://cs.gmu.edu/~asood>.

Mr. Dean Weber

Mr. Weber is a director and cyber solutions enterprise architect at CSC, where he provides vision and guidance for solution development within the company's Cyber Security Laboratories. With more than 30 years of experience in information and physical security, he joined CSC after serving as Chief Technology Officer at Applied Identity, which recently was sold to Citrix. Earlier, he was Chief Security Architect at Teros; a leading manufacturer



SPEAKER BIOGRAPHIES



of application security gateways, also acquired by Citrix. He was responsible for developing and implementing solution deployments including assessment and intelligence gathering at TruSecure/ICSA Labs (now Verizon Business Security Solutions). Mr. Weber helped found a large Midwestern reseller-integrator specializing in secure architectural design and deployment for both public- and private-sector clients, and he served for many years as its technical vice president. Additionally, he spent several years in the U.S. Navy working in physical and electronic security. Mr. Weber is a frequent speaker at information security events such as InfoWorld, ITEC, InfoSec Europe, InfraGard, Secret Service Security Roundtable, ISSA, and various focus engagements.

Managing Cyber Risk through Recovery Based Resilience
Administrative Information
14 Feb 2012

Welcome: On behalf of National Defense University's Center for Technology & National Security Policy and the George Mason University International Cyber Center, we would like to welcome you to Managing Cyber Risk through Recovery Based Resilience workshop. This event will be facilitated at Marshall Hall, National Defense University (NDU), Fort Lesley J. McNair, Washington, DC.



NATIONAL DEFENSE UNIVERSITY
Lincoln Hall, Building 64
Fort Lesley J. McNair
300 5th Avenue SW, Marshall Hall
Washington, DC 20319-5066

Arcitc Collaborative Workshop Overview

The purpose of this unclassified, not-for-attribution event is to critically examine strategies for meeting the challenge of increasing the resilience of national cyber assets with a focus on delivering service even in the presence of a successful attacker in the system. Current protective measures are largely reactive and rely on our ability to identify vulnerabilities in our system. Such strategies, while useful, are imperfect and intrusions are inevitable. To achieve a higher level of resilience, we must look for other methods to supplement current strategies in cyber security, which allow continuity of service despite intrusions. This workshop will examine alternatives such as ones based on restoration and recovery oriented computing, fault and intrusion tolerance, intrusion avoidance and malware removal, rapid reconfiguration and diversity, along with the issues of capital and operations costs, policy requirements, human factors and information overload among others.

Registration:

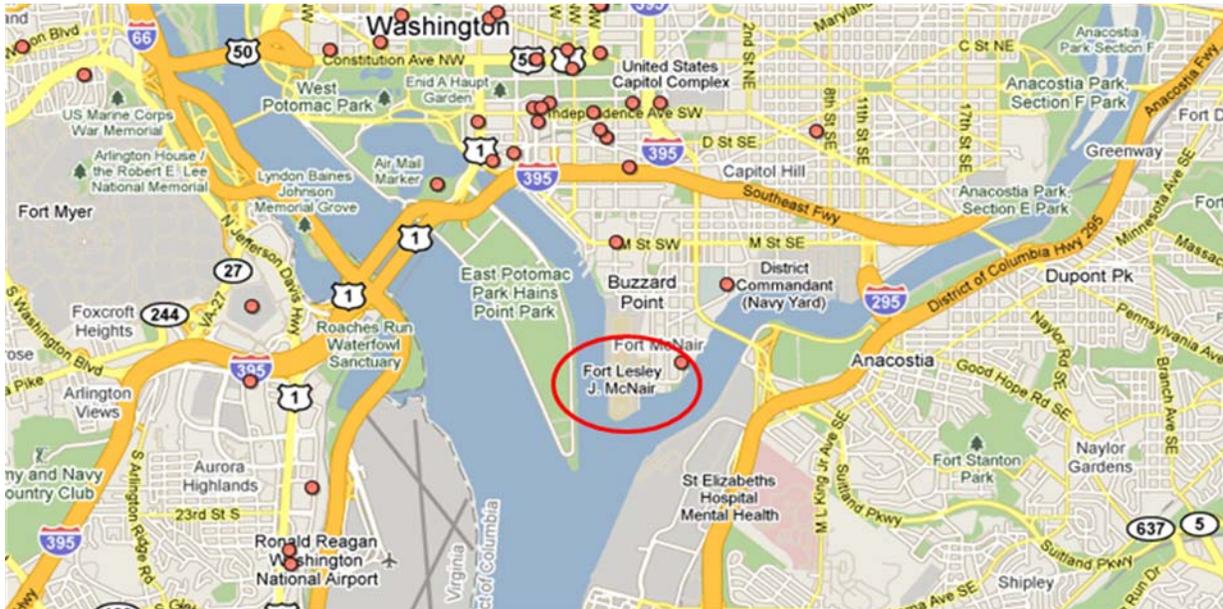
If you have not already done so, please [click here to register](http://tinyurl.com/7uaegm9) (or copy the address at the bottom to your browser address line)

<http://tinyurl.com/7uaegm9>

Managing Cyber Risk through Recovery Based Resilience
Administrative Information
14 Feb 2012

Additional Information

Fort McNair / NDU:



Identification: Picture ID is required for access to Fort McNair.

Directions [GOOGLE Maps Link \(With placemarks\)](#)

Directions to National Defense University, Fort McNair, Washington DC:

METRO: NDU is located about 1/3 mile from the Waterfront-SEU Metro Station on the Green Line. Leaving the station, walk down 4th Street (South) three blocks until it ends and becomes P Street SW. The Fort McNair main / ceremonial gate will be visible. The following link is a detailed map and photo of the Waterfront-SEU Metro Station:

http://www.wmata.com/rail/station_detail.cfm?station_id=83

To enter Fort McNair, visitors without a DOD vehicle sticker will be required to show either a current DOD picture identification badge, a state issued driver's license with photo, or a passport. Depending on the risk assessment, the Military Police may ask you for a second form of identification. If this should occur, visitors may use two of the three mentioned above.

TAXI: Ask the driver to take you to the intersection of 2nd and Q Streets SW. From this entrance to Fort McNair, visitors can either proceed through the security checkpoint with the taxi or get out of the taxi and walk one block to the main entrance of Lincoln Hall. (Phone numbers for Taxi Cab below)

DRIVING: Visitors without a DOD vehicle sticker must use the 2nd Street gate, east of the main gate.

Managing Cyber Risk through Recovery Based Resilience
Administrative Information
14 Feb 2012

From Arlington and points South and West (via 14th Street Bridge): Follow I-395 North across the Potomac River to the Maine Avenue exit. Go over the 14th Street Bridge staying to the left. The road splits - left to Route 1 and right to I-395 North. Follow Route 1 towards 14th Street and the Mall, but after the split get in the right lane. Take the right-side exit for Maine Avenue. At the light, turn right onto Maine Avenue. Continue on Maine Avenue – past the Washington Marina, several seafood stores, and restaurants on the right. Maine Avenue changes name to M Street where it curves to the left, near the Arena Stage. Turn right on 4th Street (Waterfront-SEU Metro/Safeway is on the left). Continue (south) three blocks until it ends and becomes P Street SW. The Fort McNair main / ceremonial gate will be plainly visible. This entrance is usually closed to visitor's vehicles. Follow the brick wall to the second entrance, 2nd Street Gate.

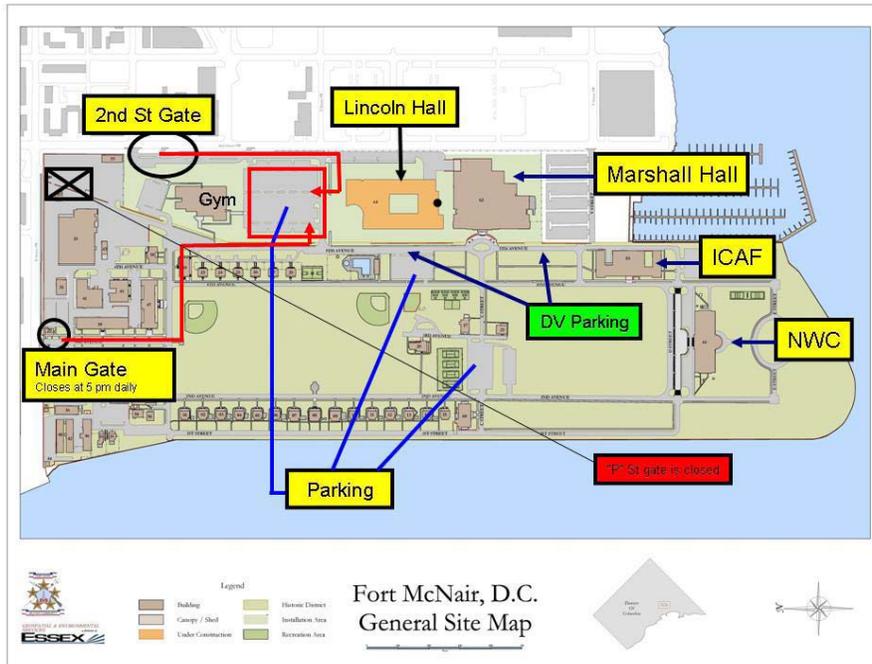
From Alexandria or Anacostia (via Woodrow Wilson Bridge): Follow I-295 North to the South Capitol Street exit. Proceed across the South Capitol Street Bridge, staying to the right. Bear right coming off the bridge, avoiding the underpass, and turn left on to M Street SW at the traffic light. Continue West on M Street SW to 4th Street SW. Turn left (South) on to 4th Street SW.

From Maryland, Prince George's County and Eastern Montgomery County: Follow the Capitol Beltway (I-495 or I-95) to the Baltimore/Washington (B/W) Parkway exit. Proceed Southbound on the B/W Parkway. As you approach Washington, the B/W Parkway will become I-295 South; continue on I-295 to the Suitland Parkway exit. Exit at the Suitland Parkway and immediately exit on to I-295 Northbound. After joining I-295 North, exit at the South Capitol Street exit. Proceed across the South Capitol Street Bridge, staying to the right. Bear right coming off the bridge, avoiding the underpass, and turn left on to M Street SW at the traffic light. Continue West on M Street SW to 4th Street SW. Turn left (South) on to 4th Street SW.

From the Fort McNair Main Gate: Continue straight ahead on 3rd Avenue until it ends at B Street. Turn left on to B Street and proceed 2 blocks to 5th Avenue (If walking, you can turn right on 4th Avenue). Turn right on 5th Avenue. The large building, ahead, on the left side of 5th Avenue, Lincoln Hall, next is Marshall Hall. Eisenhower Hall is one block further down 4th and 5th Avenue. Lincoln Hall is connected to Marshall Hall. Park in one of the lots marked below.

From the Fort McNair 2nd Street Gate: After passing through the security checkpoint area, turn right onto the street in front of Lincoln Hall. Park in one of the lots marked below.

Managing Cyber Risk through Recovery Based Resilience
Administrative Information
14 Feb 2012



Transportation: Participants using private automobiles are encouraged to carpool, as parking is very limited with the University in session.

Phone numbers for taxis -

- Capital Cab: 202-636-1600
- Diamond Cab: 202-387-4011
- Red Top Cab: 202-328-3333

Lodging: There are no visitors' quarters on Fort McNair. Federal employees and military personnel on TDY orders can access the following internet site, <http://www.fedtravel.com/home.html> for hotels offering the government per diem rates. Call Fort Myer Billeting Office, 703-696-3576 or DSN 426-3576, to request a Statement of Non-availability.

Military lodging in the surrounding area:

- Fort Myer - 703-696-3576 or DSN 426-3576
- Bolling AFB, DC - 202-767-5316
- Andrews AFB, DC - 301-981-4624
- Naval District, DC - 202-563-6950
- Fort Belvoir, VA - 800-295-9750

Civilian participants can access the following link to assist in lodging plans. NDU does not endorse any of these establishments.

<http://washington.travelhero.com/index.cfm/country/US/state/DC/city/Washington/aid/937/index.html>.

Meals: Lunch will be pay-as-you-go. Lincoln Hall cafeteria has a wide selection of lunch items, costing approximately \$7.00 to \$10.00, depending on selection. Light refreshments, including coffee, juice, and bottled water, will be available for the morning and afternoon breaks.

Uniform:

The dress for the event is business casual / warrior dress.

Managing Cyber Risk through Recovery Based Resilience
Administrative Information
14 Feb 2012

Classified Documents Handling:

This Workshop is an UNCLASSIFIED event; therefore, no classified documents will be used.

Internet Access:

There is no access to the internet or internet services within Marshall Hall during the event.

Electronic Devices:

Electronic devices may be used in the foyer of Marshall Hall. Workshop facilitators will ask that all cellular and electronic devices be turned off during working group venues.

Event Support Contacts:

Technical Points of Contact:

Dr. Arun Sood, GMU, asood@gmu.edu

For Registration or Logistics Questions:

James Burchill, NDU, james.burchill@ndu.edu