Chesapeake Chapter INCOSE
International Council on Systems Engineering

Print Issue
Forward to a Friend
Go to Back Issues
Vol. 1 Issue 11

November 2010 E-Newsletter

Welcome to our special Cyber-Security issue. We've filled it with all kinds of information dealing with the war taking place in Cyber Space. All to set the stage for our upcoming Cyber-Security Panel set for our November 17th Dinner meeting. If you can't read the whole Newsletter right now don't forget you can get to it again by going to the INCOSE Chesapeake Chapter's website, click Library tab and then click eNewsletters submenu. Also don't forget the Events in the Area section in the right hand column. Some events will be happening in a few days so check them out now. Near the bottom of this newsletter are some other articles dealing with the upcoming Elections for next year's Board of Directors, and a special joint AIAA/INCOSE meeting that will revisit the search for Amelia Earhart. I hope you'll enjoy our efforts here and we always welcome any feedback. ~~ Paul B Martin, CSEP; INCOSE Chesapeake Communications Officer

---

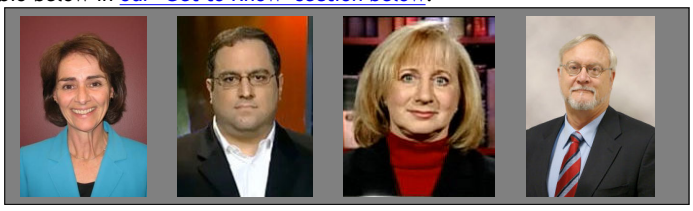
Dinner Meeting - Wednesday 17 November 2010

Panel: Cyber-Security

"What do you believe are the essential elements of a cyber security strategy that are necessary to fight and win today's cyber war? Are we winning the cyber war?"

Note: In order to give enough time for our panel members to express their views on this important topic, this meeting is scheduled to run later then usual -- Dinner will still be 6 - 7pm but the Panel will run from 7 to **8:30pm.**

Moderator:Our very own, Past President, Glenn Townson, CISSP - ISSEP. Read his bio below in our "Get to Know" section below.



Panelists

- **Maureen Baginski**, *VP Intelligence Services/Senior, National Security Advisor, Serco Inc.*
- **Dr. Richard F. Forno**, *Graduate Program Director, Cybersecurity, University of Maryland Baltimore County*
- **Dr. Julie E. Mehan**, *Vice President of Cybersecurity, Lunarline Inc.*
- **Larry Strang**, *VP Cybersecurity Initiatives, TASC Inc.*

Location: Applied Physics Laboratory, Johns Hopkins University; 11100 Johns Hopkins Rd Laurel MD 20723 (Main Entrance - Lobby 1)

Meal: Celebrate an early Thanksgiving - Turkey and Stuffing; Mashed Potatoes and Gravy; Green Beans and Cranberry sauce

Reservations:

- **By website:** Credit card via PayPal, go to our **>>Registration Page<<** for details on the presentation, more about the panelists, cost details,

November 2010

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

In this Issue

- Next Dinner Meeting
- A Word from our President
- Get to Know Pass President Glenn Townson, CISSP - ISSEP
- Last Month's Meeting
- Chapter News: 2011 Election
- Feature Article: Cybersecurity Education: Key to Informed Decisions
- Book Reviews: Crimes and Wars in the Cyber-Space
- Cyber Coverage in the Media
- Special Feature: Common Factors in Unsolved Mysteries
- Members List with Ten Years Standing

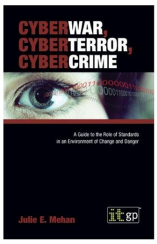
This is the monthly newsletter for INCOSE Chesapeake, a local chapter of INCOSE International. We are a not-for-profit organization dedicated to providing a forum for professionals practicing the art and science of Systems Engineering in the Northern & Central Maryland & Southern Pennsylvania area.

cancellations, and directions

Presentation ONLY: FREE (no reservations necessary)

This month we have several door prizes:

Dr. Mehan has donated a signed copy of each of her books:



- *The Definitive Guide to Certification & Accreditation,* published by ITGP in Fall 2009
- *CyberWar, Cyber Terror, and Cybercrime: International Standards for Detect, Defend and Respond*, published by ITGP in Spring 2008

CyberCore Technologies has graciously donated a $150 gift card to Ruth's Chris Steak House

CyberCore TECHNOLOGIES

A Word from our President

CYBERTOPICA 2010

by George Anderson

On November 17, 2010, the Chesapeake Chapter is scheduled to host what I predict will be a most successful panel discussion on Cyber- security. I am predicting success based not only on the participation of learned guest panelists but also on the value of the expected dialog with our highly trained and experienced membership. The catalyst for making my prediction is that the subject is just beginning to peak on the journalistic hype curve.

I have recently read articles in the New Yorker magazine, the USAF Air University Review, and several Northrop Grumman Company pamphlets that are soberly defining the problem and recommending solutions to Cybersecurity issues. My first reaction to reading much of this is to wonder how we got ourselves in such a vulnerable position so quickly. Are we so vapid that we designed, developed, and now operate, networks that legions of script kiddies* around the world can exploit largely unopposed and unidentified?

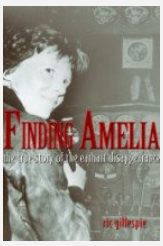
The sky is falling crowd always tells a good story but I have utmost confidence in the long-term stability of our infrastructure. My confidence is based on the history of technical progress and more specifically on the ubiquitous history of locks. We have a great deal more insight into the life cycle of locks than of information technology.

Mechanical locks are known to predate the ancient Egyptians and have been continually improved as new materials and manufacturing methods became available. The basic principles of operation are notably common and a person trained in lock picking today is right at home manipulating a lock dating from antiquity.

By comparison, the first modern network could be considered the telegraph. Even by today's standards this system had a number of admirable advantages: it was simple, standardized, and completely interoperable. Added to this, the user interface was easy to learn and required mastery of only simple repetitive skills.

To explain further, the telegraph key and sounder were the standard user interface that when connected to a single wire and a battery constituted the network. Any number of user interfaces could be connected and the control of

Mark your Calendars with these upcoming events:



INCOSE Chesapeake Chapter and AIAA Baltimore Section Special Presentation ***Finding Amelia A challenge in Systems Engineering***

Date: **Saturday, 20 Nov 2010 8AM to 3PM**
Speaker: **Ric Gillespie**
Location: **The Engineers Club** at the Garrett-Jacobs Mansion; Baltimore, MD
Special Registration Page >>HERE<<

Our End-of-the-Year Holiday Dinner/Awards Ceremony

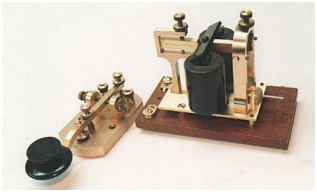
Date: **Thursday, 16 Dec 2010 6 - 10PM**
Sit-Down Meal: **Either Beef Tenderloin Forester or Maryland Crab Cakes.**
Location: **The Engineers Club** at the Garrett-Jacobs Mansion; Baltimore, MD
Join us for an enchanted evening of fine food, glitzy awards and stimulating conversation with friends and colleagues.
Special Registration Page >>HERE<<

The Chesapeake Chapter is always looking for volunteers to speak at our upcoming meetings! Please contact our Programs Director, Mr. Donald York, if you would like the opportunity to speak or can recommend someone.

The Chesapeake Chapter of INCOSE is proud to recognize the following organizations for sponsoring our endeavors to expanding the understanding and appreciation of Systems

traffic was based only on operator protocol. Any person attaching his key and sounder to "the wire" could read and send traffic. This dictated that some sort of message encryption was needed and indeed many commercial systems were developed over the lifecycle of the telegraph to satisfy this requirement.

The hacker problem really began when systems evolved to the point where the human interface was reduced and many actions were made autonomous. This got even worse when processing and control capabilities were able to transit the network in addition to message traffic without human participation or notification.



The internet protocol network is currently the ultimate example of system autonomy and provides an opportunity for any participant to maliciously control or operate components of systems owned and operated by others.

Human intervention could mitigate some risks but the speed of data flow on today's networks requires automation to successfully watch over the performance of existing systems.

What, then, do locks have to teach us about the future of the Internet?

At least five items come to mind.

1. The security of locks was increased only by adding expensive features many of which interfered with the operator's ease of use.
2. Locks adopted an encryption system that had to be easy to implement, standardized for ease of logistics support, and maintainable by existing skill sets.
3. Locks were routinely compromised "picked" by experts shortly after being put in service.
4. The number of expert lock picks was always small in relation to those who imitated their methods and were able to duplicate their success.
5. The mature state of the lock industry today consists of multiple tiers of lock design based on the vulnerability to picking. Most household locks are medium security based on a tradeoff between cost and the estimated population of imitators who can successfully attack the lock. If a high value location needs protection, then the lock must exclude all imitators and delay, but not defeat, the expert.
6. The overall lesson learned from locks is: the determined expert can be delayed but almost never defeated. Contrast the few experts to the vastly more numerous imitators and the associated risk analysis points to a medium design as the most useful class of locks.

If this evolution comparison is valid, the solution to the Cyber threat will be a never-ending expansion of our knowledge of vulnerabilities and constant improvement of the corrective tools and processes just as we have seen in the extended development cycle of the lock.

*A script kiddie is an unsophisticated operator who uses software code and systems developed by someone else to carry out illegal or quasi-legal probes, information transfer and code alteration in a victim's network. A complete listing of known mischief is much longer and is currently growing unchecked.

Return to top.

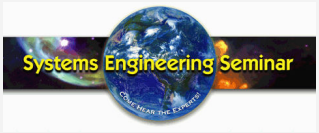
Get to Know ...

Glenn Townson, CISSP - ISSEP

Mr. Townson has more than 35 years of experience designing, maintaining, protecting, and certifying information technology in Commercial, DoD, and Federal systems. He holds the Certified Systems Security Professional (CISSP) and the Information Systems Security Engineer (ISSEP) certification and is the Director of Systems Engineering at

Engineering in the local area:

Events in the Area:



NASA's Goddard Space Flight Center

Date: November 2, 2010, 1:00 pm
Presentation: *Common Sense Engineering and the BP and Upper Big Branch Oil Spills*
Speaker:
Beverly A. Sauer, Ph.D.
More Info Here

IEEE Baltimore Section

Event: IEEE Senior Member Grade Elevation Day
Date: Nov 6, 2010, 9 AM to 2 PM
Location: National Electronics Museum -- Pioneer Hall
Do you qualify as a Senior Member? *You are invited to an important event - an opportunity to apply for IEEE Senior Member grade!*
More Info Here

Event: IEEE Baltimore Communications Society Meeting
Presentation: *The Capabilities of the Undersea Telecommunications Industry. Presented by Neal S. Bergano*
Date: Tuesday, Nov 9, 2010, 5:30PM
Location: National Electronics Museum

Event: IEEE Baltimore Power & Energy

Secure Technologies Group, Arnold, MD. He started his career in the US Air Force as a Crypto Technician. He has supported the Department of State (DoS) for 7 years from engineering the Command, Control, Communications, Computers (C4I) for US Embassies and Consulates OCONUS along with CONUS government facilities. Engineered and managed the intrusion Detection Program for DoS. As an Information Systems Security Manager (ISSM) for the Counterintelligence Field Activity, supervised Information System Security Officers (ISSO's) ensuring systems, facilities, and personnel met all policy and government regulations. He served as Senior Certifier analyzing and documenting the security posture of systems developed by and for the National Security Agency. Currently Mr. Townson is a SETA Senior Systems Security Engineer contractor supporting the Enterprise Security Management development for the Global Information Grid (GIG).

Return to top.

Did You Miss Last Month?

Lecture: Human Systems Integration and the Systems Engineer

Mr. John Winters, Senior Human Factors Engineer at Basic Commerce and Industries (BCI), discussed the primary goals of Human Systems Integration (HSI)in a thoughtful and engaging way. Lessons in HSI Grammar, importance of Diverse Disciplines for integrating HSI successfuly, and designing to meet the demands of the Flexible and Inflexible Users.

Find out more for yourself by downloading Winters' brief today.>>HERE<<

Visit our Library section of our Website to also find other copies of presentation materials from previous meetings or other gatherings of interest. Poke around and see if anything looks interesting.

Return to top.

Feature Article

Cybersecurity Education: Key to Informed Decisions

by Dr. Richard Forno

As a national issue, cybersecurity neither is a sensational nor spooky issue despite its frequent portrayal in the media as such. Indeed, there are important reasons for us to be concerned: critical infrastructures and our military are daily targets of opportunity for our adversaries in cyberspace, as are many of our mobile devices, bank accounts, and personal computers. And that's just for starters.

Not to mention, we tend to overlook the many cybersecurity problems we bring upon ourselves by rushing to embrace new technologies without doing our own comprehensive analysis of their respective risks and rewards. Then, when problems occur, we scramble to acquire new cybersecurity products and services to make up for our lack of analysis and planning while asking "how did this happen?"

Unfortunately, many of today's cybersecurity discussions and decisions are reationary in nature and based on fear, uncertainty, and sensationalism instead

Society Event
Date: Nov 9, 2010, 11 AM to 1 PM
Location: Fort Smallwood Building, Conference Rooms 1, 2 & 3
Curtis Bay, MD 21226
Presentation: *Future of coal power in Baltimore. Presented by Jim Perry*
RSVP:Joshua.Skillman@ieee.org by Friday, November 5th

National Electronics Museum
History of the Nation's Defense Electronics

Event: National Electronics Museum Meeting Notice
Date: Wednesday, November 3, 2010
Time: 7:00 PM - 8:30 PM
Location: National Electronics Museum
Cost: $10 ($5 Members)
Presentation: *Steam Coffin: Captain Moses Rogers and the Steamship Savannah Break the Barrier*
Speaker: John Laurence Busch
More Info Here

Averill M. Law & Associates

Event: Simulation Modeling for System Design and Analysis
Date: November 15-19, 2010
This course is designed for systems analysts, operations research analysts, engineers, military planners, computer scientists, and technical managers who would like to use simulation to design and optimize real-world systems.
More Info Here

Chapter News

2011 Elections for the Board of Directors

We are preparing to distribute the ballots for the 2011 board member vacancies.

This year, we have only two vacancies, Gundars Osvalds for President Elect and Glenn Gillaspy for Treasurer. Go now to our chapter's

>>Election Page<<

and read the candidates bio's and also an article by our President, George Anderson dealing with upcoming election and discussion of the chapter's bylaws. And be on the look out for a ballot by e-mail.

Return to top.

of calm, rational, objective analysis and understanding. And so the cycle of cybersecurity confusion continues.

How can we overcome this situation?

Here's a radical but simple idea to get the process started: learn how to talk and work together within our own organizations. Executives and engineers tend not to interact with each other, speak in different languages when they do, and otherwise suffer from understandable generational differences. However, as pertains to cybersecurity concerns, differences aside, they all need to understand the reality of the operational cybersecurity environment and what it means for their organization. This will help prevent fear and sensationalism from replacing sanity and reason in our cybersecurity planning.

In many cases, that means asking tough questions and being prepared to offer (and accept) equally tough but honest answers. But you have to know where to look, what to ask, and what it means for your respective organization. Unfortunately, as pertains to cybersecurity, doing so requires knowledge and familiarity with things beyond a person's primary career expertise either as an engineer or executive.

The obvious way to facilitate such understanding is to ensure those involved at all levels with cybersecurity matters receive an appropriate, common, and holistic understanding of the cybersecurity environment. This basic framework should begin with the traditional cybersecurity and technology concerns and then place them within an organizational context to reinforce the reality that regardless of the organization's size, "all cybersecurity is local" and that cybersecurity activities are not exclusively a technical undertaking. In other words, we must bridge the knowledge and communications gap between executives and engineers.

Once that foundation is established, those involved with cybersecurity matters also must have the ability to transform the detailed issues they are dealing with into actionable, understandable knowledge for managers and policymakers to use in decision-making. By the same token, managers and executives need to comfortably understand both the risks and rewards of the technology landscape in order to make decisions based on factual assessments of reality instead of a sense of fear based on fantasy to effect appropriate cybersecurity preparedness.

In other words, cybersecurity is an interdisciplinary environment that requires a mix of both technical and non-technical expertise and competencies. They key is developing a program of relevant and comprehensive cybersecurity education that can provide students with common knowledge and fresh thinking that will enable them to appreciate the "big picture" aspects of the issue and hopefully create a cadre of corporate leaders and technicans with a critical and objective perspective of technology and cybersecurity issues for their organizations. Within this program must be instructional elements pertaining to leadership, management, and organizational communication to ensure all involved with cybersecurity matters can work effectively and "from the same sheet of paper."

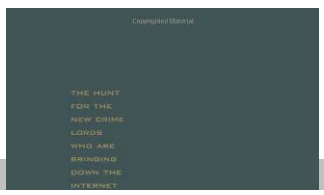
Such preparation can enable cybersecurity practitioners and executives alike to make informed decisions about cybersecurity matters from a position of quiet knowledge and confidence, not sensationalism and fear.

Dr. Richard Forno is the director of the UMBC graduate cybersecurity program. He can be reached at richard.forno@umbc.edu.

Return to top.

Book Reviews

Crimes and Wars in the Cyber-Space



by Mark Kaczmarek

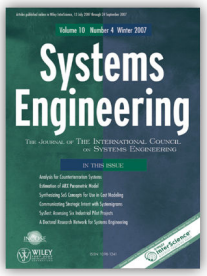
Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet *by Joseph Menn*

SE Education

Also check out other Systems Engineering training opportunities at our Education page

Return to top.

Discover *Systems Engineering*

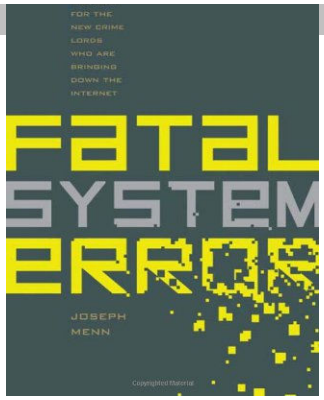


Read the current issue free on-line for a limited time: Click Here

Check out these articles:

- *An extended enterprise architecture for a network-enabled, effects-based approach for national park protection (pages 209-216)*
- *Lunar architecture and technology analysis driven by lunar science scenarios (pages 217-231)*
- *Integrating humans with software and systems: Technical challenges and a research agenda (pages 232-245)*

As a member of INCOSE you have online Access to the current and past issues of The Journal of Systems Engineering via the Wiley InterScience site. Search the archives and download papers of interest. Registration on the Wiley site is required. Instructions for accessing the SE Journal can be found in INCOSE



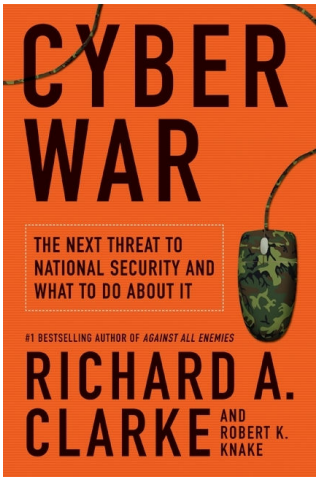
The book starts off with extortion of an off shore gambling site … either pay up or have a DDOS (Distributed Denial Of Service) attack and lose big $ every day !!?? The specialist, Barrett Lyon, shows up and finally is able to thwart the hackers. But bigger fish are on the sites of the evil hackers … The Superbowl – one of the heaviest betting events for the entire year and the hackers have targeted multiple sites. The Crime Lords put out malware that sits on servers and then at a specified time sends requests from all over the earth to a company or Government web site to cripple any legitimate activity.

Now help from across the "Big Pond", Andy Croker - Britain's NHTCU (National Hi-Tech Crime Unit) detective – watched the money flow to a Western Union in Latvia. Only to find out that this isn't the only drop. But the money is then transferred into Russia and the trail goes cold. Now the efforts of crossing international boundaries and laws to capture these modern day Crime Lords are shown.

The author has also spoken with Vint Cerf, one of the co-authors of the Internet Protocol for his insight as well as Eugene Kaspersky, of Kaspersky Labs. Kaspersky also offers his opinion on the network attack regarding the Russian and Georgian conflict.

This book describes how these dirty rotten scoundrels operate - plenty scary if you do any work on the net. After reading this book, you may agree that the best thing is to sell everything and live in a cave in Borneo to avoid having any issues with these Crime Lords. This book is a very interesting read.

Cyber War: The Next Threat to National Security and What to Do About It *by Richard A. Clarke*



This book opens up with the activity of the Israeli raid on the Syrian nuclear processing plant in 2008. F-15s and F-16s were among the attack aircraft. Yet not a single shot was fired by the Syrian air defense system. Why? The authors provide several plausible scenarios about the possibilities of what type of premeditated cyber attack occurred to cause the Russian made Syrian air defense system to not react to the Israeli attack. One scenario was that a reconnaissance UAV had been painted by the Syrian RADAR and sent a return signal with an undetected SW upgrade that allowed the Israeli attack to go unnoticed. I suspect that the authors know which scenario actually occurred but are leaving it up to the reader to choose the correct one.

Another area of discussion was the Russian skirmish with Georgia back in 2008. Georgia suffered a cyber attack at various levels when the skirmish occurred. Russian officials deny any influence citing that some over zealous patriots may have decided to assist their country in a time of need.

Author Clarke has served under several Presidential administrations. He certainly has had visibility into the cyber realm of the US and has influenced policy. He does provide his concerns regarding the US military, Government and business computer networks as well as his suggestions on what policies are needed for the US. The stand up of the new US Cyber Command is also discussed

Connect

With Connect you can also download the Vol 13 Issue 3: October 2010. *INCOSE's Twentieth Anniversary International Symposium*

Clink on image above and Log-In today.

Return to top.

Members List with Ten Years Standing (Joined in 2000)

- **Robert L. Tucker**
- **Paul B. Martin** Serco
- **Michael J Kardas** Northrop Grumman
- **Gundars Osvalds** Northrop Grumman
- **William R. McWhirter** Retired
- **Richard M. Day** JHU/APL

Please note that these members will receive a 10 year award at the December 16th Dinner/Awards Ceremony. Join us at our end-of-the-year Holiday party as we recognize those who have helped us realize INCOSE's mission to push SE out into the front of the public debate.

Return to top.

Table Talk

SE Career Market Trends

Mike Thompson the founder and owner of the The Turas Group will have a discussion topic table at our next Dinner dealing with Job Searching in the area and within the SE field. Join him at his table and ask questions and swap job hunting stories with others, all while your enjoying your Turkey dinner.

The INCOSE Foundation - where you make the difference

Foundation Extends Deadline for JHU/APL Alexander Kossiakoff Scholarship to December 1, 2010.

The Johns Hopkins University / Applied Physics Laboratory Alexander Kossiakoff Scholarship, in partnership with the

as well.

This book at times seems to read like a Tom Clancy novel, however the scenarios are very real. With the stand up of the new Cyber Command, this book is right at the knife's edge of the upcoming Cyber War for next decade. I highly recommend this book to anyone interested in computers and their network vulnerabilities. Some scenarios can be frightening when one ponders how serious some of the ramifications can be to our Nation, or any nation of the free world.

Return to top..

SE in the News

Cyber Coverage in the Media

by Glenn Gillaspy

Cyber is covered in the mass media. Here are several examples in newspapers, magazines and network television:

1. New Yorker Magazine, 2008, an extensive interview with the Director of National Security (DNI), Admiral Mike McConnell, in an article caled "The Spymaster"
2. CBS 60 Minutes, fall, 2009, Admiral Mike McConnell, former DNI, interviewed in "Cyber War: Sabotaging the System"
3. Spring 2010, The Washington Post, Admiral McConnell indicates "We are fighting a cyber war - and losing"
4. Summer 2010 re-runs: CBS airs the same segment of Admiral McConnell (see #2 above)
5. Winter 2010, Richard Clarke, who warned of 9/11, warns of cyber war where refineries, public transportation and electric and gas utilities malfunction
6. Articles in The Baltimore Sun that led to a federal court case that is in progress
7. Seymour M. Hersh, "Annals of National Security, the Online Threat: Is Cyber War Real?" New Yorker Magazine, Nov 1, 2010

   Discussion of ongoing cyber activities:

   - The April Fools Day incident in 2001 where a Chinese interceptor collided with a US EP-3E Aires II reconnaissance aircraft; the crew was briefly detained, then released, the aircraft was not released and the equipment and software was compromised. The extent of the compromise was not obvious until 2008.
   - Military vs. civilian cyber responses by the N.S.A. and Dept. of Homeland Security (D.H.S.), and others; the comparative advantages and drawbacks; Hersh hints that parties who would benefit from a war call it cyber war but analysts and academics use different terms: espionage, compromise(s), etc.
   - The distinction between cyber espionage and cyber war where espionage can lead to war, but not usually; the turf and money battles
   - The relationship between Cyber Command's General Alexander and Howard Schmidt, the President's cyber czar
   - The Microsoft patch for the Stuxnet attack
   - N.S.A. attacker and defender staffs and capabilities
   - Contributions from: Marc Rotenberg, former Senate aide and president of the Electronics Privacy of Information Center; Whitfield Diffie, encryption expert; and Jeffrey Carr, publisher of "Inside Cyber Warfare"

Return to top.

INCOSE Foundation, carries an award of $5,000, an internship and a plaque. Follow this link to learn more about this award application procedure. Questions can be submitted to Dr. William Ewald, Chief Executive Officer of the INCOSE Foundation, at wewald@icfi.com

Return to top.

This Newsletter is to serve our members and is open to all for contributions. Do you have an interesting idea for an article? A review of a new book related to engineering? Let us know. We'd love to hear about. It may wind up in a future issue of our Newsletter.

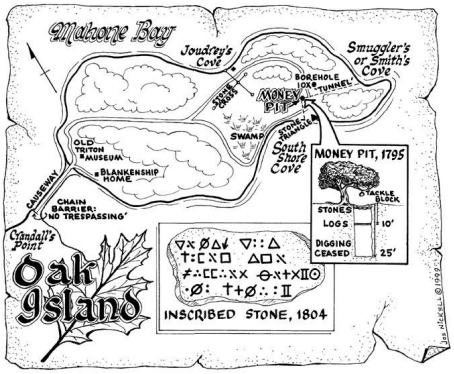
Return to top.

Special Feature

Common Factors in Unsolved Mysteries

by George Anderson

This month, we are going to sponsor a joint AIAA/INCOSE event that will revisit the salient facts accrued during the 73-year search for Amelia Earhart. This enduring subject has spawned a plethora of books, movies and dedicated explorers, who, using various theories, have attempted to find some clue that would lead to a conclusive identification of her aircraft and its final resting place. If this discovery were to occur and be made public it would likely cause a news sensation reminiscent of what occurred when the Titanic was found.



We can imagine that if the Earhart Lockheed 10E is found, analysts would then discard all the inoperative theories that accrued over the years and select the most likely explanation of the last hour of the fatal flight. How will that play out? Will there be a new story created? Will one of the theories be borne out at least in part? We cannot say, but it is informative and thought provoking to compare the Earhart loss with several other enduring mysteries. I have selected three that have reasonably good documentation including an alleged treasure and two fatal air crashes.

Interested? Read More.

Return to top..

Keep up with the latest news and events. Find out about our new Board of Directors. Explore our extensive library of previous lectures from our Monthly Dinner Meetings. Learn of the Benefits of Joining INCOSE. Check out Systems Engineering education in the local area. All this and more awaits you at our INCOSE Chesapeake Chapter Website.

For any comments or suggestions about this newsletter please e-mail our President, George Anderson or our Communications Officer, Paul Martin. We value your feedback.