EXHIBIT 122

MAINE ASSOCIATION of FORMER INTELLIGENCE OFFICERS

Serving the Intelligence Community

October 20 Meeting The Truth behind the CIA's Detention and Interrogation Program

Posted on August 28, 2012 by kr4678

Maine AFIO Chapter Meeting

October 20, 2012

Brick Store Museum Program Center

2 Dane Street, Kennebunk, ME

2:30 p.m. (note change from usual time)

AFIO/ME

Michael Severance, President
P.O. Box D
Kennebunkport, ME
04046

~~~~~~~~~~~~~~

AFIO –National Chapter website

James Cotsana Featured Speaker on

CIA's Detention and Interrogation Program

October 20, 2012

"THE TRUTH BEHIND CIA'S DETENTION AND INTERROGATION PROGAM" is the subject of the

Recent Posts

- March Meeting
- June 17th Meeting
- February 2017 Meeting
- April 2017 Meeting
- January 2017 Meeting
- November Meeting

Next Meeting
March 18, 2017

Meeting Location

Varies. Please review the events or current posts tab above for location

Brickstore Museum's Program Center
2 Dane Street
Kennebunk, ME 04043

Kennebunk High School Auditorium
Fletcher Street (Rt 35)
Kennebunk, ME 04043

Community House,
8 Temple Street,
Kennebunkport, ME 04046

2:00 p.m.

AFIO Publications

AFIO Publications
~~~~~~~~~~~~~~

October meeting of the Maine Chapter of the Association for Intelligence Officers.

With his twenty-six years of experience in CIA's Directorate of Operations and Directorate of Science and Technology, James Cotsana is well qualified to speak on the issue. As a department chief at the Counterintelligence Center he established and oversaw a highly successful program focused on identifying and disrupting terrorist plans and plots while identifying methods of operation.

Jim has served in senior positions with CIA in Europe, Africa, the Middle East, and Southeast Asia. He served as an infantry officer in Vietnam.

Now fully retired, he volunteers with Hospice House in Concord, N.H. and the Concord-Merrimack SPCA.

The meeting will be held Saturday, October 20, 2012 at 2:30 p.m.(Please note change in meeting time) at the Brick Store Museum Program Center, 2 Dane Street, Kennebunk, ME. and is open to the public. For information call: 207-967-4298.

September 15th Meeting Meeting Cancelled ›

Posted in Uncategorized

AFIO National Organization

AFIO National

Meta

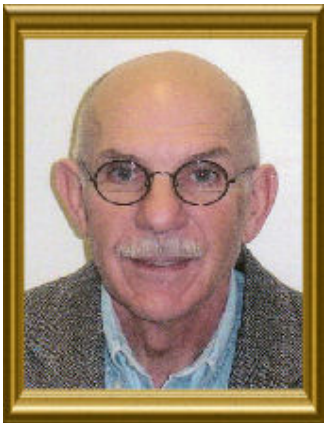
- Log in
- Entries RSS
- Comments RSS
- WordPress.org

↑

Artemus Consulting Group

Artemus

James Cotsana, Jr.



Served twenty-three years experience as an Operations Officer and Senior Manager with the Central Intelligence Agency's Directorate of Operations and Directorate of Science and Technology. As Department Chief of CIA Counterterrorist Center, Mr. Cotsana directed the Department's mission to identify and disrupt terrorist plans, methods of operation and plots. He managed the Agency's covert communications operations and coordinated counterintelligence programs to protect personnel and facilities. Mr. Cotsana, a member of the CIA's Senior Intelligence Service, retired in 2005.

His personal blog is at **http://thedarksideinc.wordpress.com**

Artemus Consulting Group

FACEBOOK TO CRACK DOWN ON SURVEILLANCE

source: wired.com

AS SOCIAL NETWORKS continue to mature, they increasingly take on roles they may not have anticipated. Moderating graphic imagery and hate speech, working to address trolling and harassment, and dealing with dissemination of fake news puts companies like Facebook and Twitter in powerful societal positions. Now, Facebook has acknowledged yet another challenge: Keeping your data safe from surveillance.

That's harder than it may sound. When you post something publicly on a social network, anyone can view it—including law enforcement or federal agencies. Those types of groups, particularly local police, have increasingly capitalized on social media as an investigatory resource. And those one-off cases hardly register compared to the mass surveillance tools that software companies can create by using a social network's API—the set of tools that allow outside parties to develop interoperable software for a company's product. In the case of a company like Facebook, those tools can surveil and collect data about millions of people. These products are then sold to police, advertisers, or anyone else willing to pay. Or at least, they could until this week.

"We are adding language to our Facebook and Instagram platform policies to more clearly explain that developers cannot 'use data obtained from us to provide tools that are used for surveillance,'" Facebook said in a **statement**. "Over the past several months we have taken enforcement action against developers who created and marketed tools meant for surveillance, in violation of our existing policies."

Private Lives

Facebook worked with the American Civil Liberties Union of California, Center for Media Justice, and Color of Change to implement the policy, prompted in part by ACLU **research** from September that demonstrated how law enforcement used third-party tools to track activists, particularly those from the Black Lives Matter movement.

“The clear public policy is important because it sends a very clear message to developers and to businesses about what is not allowed on Facebook,” says Nicole Ozer, the Technology and Civil Liberties Policy Director at the ACLU of California. “And if their business model is based on building tools for surveillance they need to get a new business model.”

Read more: FACEBOOK TO CRACK DOWN ON SURVEILLANCE

ETHICAL HACKING -

source: darkreading.com

If your company doesn't have an ethical hacker on the security team, it's playing a one-sided game of defense against attackers.

Great power comes with great responsibility, and all heroes face the decision of using their powers for good or evil. These heroes I speak of are called white hat hackers, legal hackers, or, most commonly, ethical hackers. All these labels mean the same thing: A hacker who helps organizations uncover security issues with the goal of preventing those security flaws from being exploited. If companies don't have an ethical hacker working for them, they're in a one-sided game, only playing defense against attackers.

Meet the Hackers

Companies house both developer and security teams to build out codes, but unfortunately, there often is little communication between the two teams until code is in its final stages. DevSecOps — developer and security teams — incorporates both sides throughout all of the coding process to

catch vulnerabilities early on, as opposed to at the end, when making updates becomes harder for developers.

Although secure coding practices and code analysis should be automated- and a standard step in the development process - hackers will always try to leverage other techniques if they can't find code vulnerabilities. Ethical hackers, as part of the DevSecOps team, enhance the secure coding practices of the developers because of the knowledge sharing and testing for vulnerabilities that can be easily taken advantage of by someone outside the company.

Take, for example, Jared Demott. Microsoft hosts the BlueHat competition for ethical hackers to find bugs in its coding, and Demott found a way to **bypass all of the company's security measures**. Let that sink in for a moment — he found a way to bypass *all* of Microsoft's security measures. Can you imagine the repercussions if that flaw had been discovered by a malicious hacker?

Let the Hackers Hack

Security solutions (such as application security testing and intrusion detection and prevention systems) are a company's first line of defense because they're important for automatically cleaning out most risks, leaving the more unique attack techniques for the ethical hackers to expose. These could include things such as social engineering or logical flaws that expose a risk. Mature application security programs will use ethical hackers to ensure continuous security throughout the organization and its applications. Many organizations also use them to ensure compliance with regulatory standards such as PCI-DSS and HIPAA, alongside defensive techniques, including static application security testing.

You may be thinking, "What about security audits? Wouldn't they do the trick?" No, not fully. Ethical hacking is used to build real-world potential attacks on an application or the organization as a whole, as opposed to the more analytical and risk-based analysis achieved through security audits. As an ethical hacker, the goal is to find as many vulnerabilities as possible, no matter the risk level, and report them back to the organization.

Another advantage is that once hackers detect a risk, vendors can add the detection capability to their products, thus enhancing detection quality in the long run. For example, David Sopas, security research team leader for Checkmarx, discovered a potentially malicious hack within a **LinkedIn reflected filename download**. This hack could have had a number of potential outcomes, including a full-blown hijacking of a victims' computers if they had run the file. It's probably safe to say that just the audit wouldn't have identified this hidden flaw.

Read more: ETHICAL HACKING -

TECH-SAVVY GMAIL USERS: THERE'S A PHISHING TECHNIQUE THAT CAN BEAT EVEN YOU!

source: technewsworld.com

Gmail users in recent months have been targeted by a sophisticated series of phishing attacks that use emails from a known contact whose account has been compromised. The emails contain an image of an attachment that appears to be legitimate, according to Wordfence.

The sophisticated attack displays "accounts.gmail.com" in the browser's location bar and leads users to what appears to be a legitimate Google sign-in page where they are prompted to supply their credentials, which then become compromised.

The technique works so well that many experienced technical users have fallen prey to the scam, noted Mark Maunder, CEO of Wordfence. Many have shared warnings on Facebook to alert family and friends, given that the technique has exploited otherwise trusted contacts so successfully.

Google's Reply

Google has been aware of the issue at least since mid-January, based on comments from Google Communications' Aaron Stein, which WordPress characterized as an "official statement" from the company.

Google was continuing to strengthen its defenses, Stein said, adding that it was using machine learning-based detection of phishing messages, safe browsing warnings of dangerous links in emails, and taking steps to prevent suspicious sign-ins.

Users could take advantage of two-factor authentication to further protect their accounts, he suggested.

Wordfence last month noted that Google Chrome released 56.0.2924, which changes the behavior of the browser's location bar. The change results in the display of not secure messages when users see a data URL.

Google last month announced additional steps to protect G Suite customers against phishing, using Security Key enforcement. The technique helps administrators protect their employees using only security keys as the second factor.

Bluetooth low energy Security Key support, which works on Android and iOS mobile devices, is another user option.

Realistic View

Recent changes in Chrome and Firefox browsers have mitigated some of these types of attacks, observed Patrick Wheeler, director of threat intelligence at Proofpoint.

However, a variety of techniques are used to target users, he pointed out.

Read more: TECH-SAVVY GMAIL USERS: THERE'S A PHISHING TECHNIQUE THAT CAN BEAT EVEN YOU!

PENTAGON ADVISERS: "WE NEED MORE CYBER TIGER-TEAMS"

source: defenseone.com

Pentagon advisers: We need more infrastructure cybersecurity. Congress: We want more election-hacking security.

U.S. critical infrastructure and military responsiveness is at such high risk to Chinese and Russian hacking that Pentagon advisors **are recommending** a special task force, or “an offensive cyber capability tiger team,” to help the military acquire new weapons of cyberwar. But the real worry for senators on the Armed Services Committee, who heard from Defense Science Board members Thursday, was not how to respond to Russia shutting off the lights but how to respond to an attack like the DNC hack and John Podesta hack — attacks on sovereignty that are not necessarily **an act of war**.

While the group came to warn Congress about attacks to things like the U.S. electric grid and other “vital U.S. interests,” Senators John McCain, R-Ariz., and Elizabeth Warren, D-Mass., quickly brought the discussion to the intelligence community’s assessment that Russia was using spearphishing campaigns to destabilize elections, both in the U.S. and abroad. “If an enemy or an

adversary is capable of changing the outcome of an election, that's a blow at the fundamentals of that country's ability to govern," said McCain. "The election is a system of democracy… if you destroy it then you have basically dealt an incredible blow to the country, which is far more severe than shutting down an electrical grid."

"Describe the range of options the U.S. has for deterrence," against that sort of thing, demanded Warren.

Jim Miller, a member of the Defense Science Board and a former under secretary of defense for policy, squirmed a bit at the question. "One thing we want to do is deny the benefits" of that sort of operation, he said. "Getting that information out earlier would have been very helpful."

The board is a group of civilian experts who advise the Department of Defense on technical matters. On Thursday they presented a new **report** on cyber deterrence.

Read more: PENTAGON ADVISERS: "WE NEED MORE CYBER TIGER-TEAMS"

1. THE CLOUDBLEED BUG: WHAT IT IS...WHAT YOU CAN DO
2. SPY SITES OF WASHINGTON: PRESS COVERAGE
3. HP, DELL, LEXMARK PRINTERS: VULNERABILITIES EXPOSED
4. AT LEAST 76 IOS APPS ARE VULNERABLE

Our Writers

Jim Cotsana

My day job for 26 years was as an operations officer and senior manager with the Central Intelligence Agency's Directorate of Operations and the Directorate of Science and Technology. A Vietnam veteran, I served from 1970-74 as a 1st Lieutenant U.S.M.C. infantry officer. I have an MA in philosophy and am a PhD. candidate while pursing my post-retirement interests in outdoor activities, and U.S. government issues.

Jim Cotsana

JIM'S ARTICLES

HEALTH

- It's Not Easy, But I'm A Believer! (August 2014)
- Quit Whining and See a Chiropractor! (September 2013)

HUMOR

- Everybody Needs a Grumpy Old Uncle (July 2012)

NOSTALGIA

- Cause I Said So!!! (July 2013)

OPINION

- Bring Back Civics Classes! (July 2015)
- Hire a Philosopher! (June 2015)
- I Like My Old Flip-Phone! (May 2014)
- No More Dodgeball? Tell Me It's Not So! (June 2013)
- I Love Women, But... (March 2013)

REFLECTIONS

- Boy, Was I Wrong! (November 2016)
- What Do You Want to Do When You Grow Up? (August 2016)
- My Obit! (April 2016)

Paul Erland - *Farewells*
Wendell Fowler - *Eat Right Now*
Lynn Walker Gendusa - *Just Sayin'*
Tharon Giddens - *Further Review*
Jerry Ginther - *As I Recall...*
CJ Golden - *Golden Ponderings*
Bobbie Green - *Triptalk'en*
Arlen Grossman - *Quotation Quotient*
Leslie Handler - *Leslie Goes Boom*
Frances Hansen
Denton Harris
Ann Hattes - *Food Ventures*
Marti Healy
Peggy Henderson - *"60 & Beyond"*
Quintessential Finishing School
Don Johnson
Edward A. Joseph - *Senior Moments*
Akaisha Kaderli - *Passport Perspectives*
Billy Kaderli - *Passport Perspectives*
Sharon M. Kennedy - *Musings of an Undefeated Matriarch*
Amy Laundrie - *Slice of Life*
Geno Lawrenzi
Jody Lebel - *Gray Matter*
Noah LeVia - *My Thoughts Today*
Bill Levine - *Levine's Levity*
John C. Liburdi

- All Happy Together! (December 2014)
- In the Refrigerator? (June 2014)
- The Chapters of Our Lives (April 2014)
- We All Have a 'Bucket List' (January 2014)
- Leave No One Behind! (October 2013)
- My Personal Best What? (November 2012)
- It's Blond, Not White (April 2012)
- Move, It's an Old Guy! (April 2012)

back to top

Jacqueline T. Lynch - *Silver Screen, Golden Years*
Elaine Marze - *Vintage Vibes*
Bonnie McCune - *Tunnel Visions*
Carrie McWhorter
Millie Moss - *Jottings*
Mike Murphy - *Social Insecurity*
Barbara Newell
Miss Nora - *Ask Miss Nora*
Fritz Penning - *Fritz on Photography*
Mark Pilarski - *Deal Me In*
Patsy Pipkin - *Moving On*
Lynn Pribus - *Health, Wellness & the Good Life*
Cappy Hall Rearick - *Puttin' on the Gritz*
Dusty Reed - *Life Now*
Raymond Reid
Donald Rizzo - *The Grumpy Old Man*
Lori Rose - *The Midnight Gardener*
Sy Rosen
Anna Russell
Alan M. Schlein - *Washington Watch*
Sandra Scott - *Compulsive Traveler*
Elise Seyfried - *Everyday Matters*
Rick Sheridan - *Amazing Peak Experiences*
B. Elwin Sherman - *Strictly Humor*
Bill Siuru
Allen Smith - *Circling the Drain*

Fern Smith-Brown - *As I See It*
Allison St. Claire - *Rainbow Kitchen*
John Stinger - *Picture This*
Mary Stobie - *Wit and Grit*
Eda Suzanne
Karen Telleen-Lawton - *Financial Fortitude*
Tait Trussell - *Aid for Age*
Rose A. Valenta - *Skinny Dipping*
Bill Vossler - *One More Story...*
Karen White-Walker - *Agelessly Yours*
Melanie Wiseman
Ernie Witham - *Ernie's World*
Dick Wolfsie
Paul Wynn
V. Neil Wyrick - *Life Is for Living*