CyberPro

Volume 1, Edition 5
July 17, 2008

Keeping Cyber Professionals Informed

This newsletter is intended to keep subscribers who are involved in the development of Cyber-related concepts and initiatives informed on items of common interest. The newsletter and the information contained therein shall not be used to provide a competitive advantage for any commercial firm. Any misuse or unauthorized use of the newsletter and its contents will result in removal from the distribution list and other appropriate administrative, civil, and/or criminal action.

The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or National Security Cyberspace Institute.

To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.

Table of Contents

CyberPro

Volume 1, Edition 5
July 17, 2008

Keeping Cyber Professionals Informed

** CYBER-RELATED CONFERENCES **

Note: Dates and events change often. Please visit web site for details.

Please provide additions/updates/suggestions for the CYBER calendar of events here.

14-17 July 2008	**Annual International Test & Evaluation Association Technology Review**, Crowne Plaza Hotel, Colorado Springs CO, www.itea.org
15 – 17 July 2008	**Air Force Symposium 2008 – Cyberspace**, Maxwell AFB (Montgomery) AL www.maxwell.af.mil/au/awc/cyberspace
2 – 7 Aug 08	**Black Hat USA 2008 Briefings & Training**, Caesars Palace, Las Vegas, NV, http://www.blackhat.com/
19-21 Aug 2008	**LandWarNet: Providing & Enabling Joint Generating/Operating Force Network Capabilities,** Broward County Convention Center, Ft. Lauderdale, FL, http://events.jspargo.com/lwn08/public/enter.aspx
15-17 Sept 2008	**24th Annual Air & Space Conference and Technology Exposition**, Washington D.C., http://www.afa.org
18-19 Sept 2008	**Current and Future Military Data Links**, Washington D.C., http://www.asdevents..com/event.asp?ID=257
25-26 Sept 2008	**Electronic Warfare Operations and Systems 2008**, London UK, http://www.asdevents.com/event.asp?ID=241
29-30 Sept 2008	**Airbone Networks Conference,** Washington D.C., http://www.asdevents.com/event.asp?ID=267
30 Sept – 2 Oct 2008	**National Security 2008**, Brussels, Belgium, http://www.asdevents.com/event.asp?ID=265
6-8 Oct 2008	**Strategic Space & Defense**, Qwest Center Omaha Convention Center and Arena, Omaha, NE, http://www.stratspace.org/
7-9 Oct 2008	**2008 Cyber Awareness Summit**, Bossier City-Shreveport, LA, http://www.cyberinnovationcenter.org/
16-17 Oct 2008	**8th Annual C4ISR Integration Conference** , Defense News Media Group, Arlington, Virginia, http://www.dnmgconferences.com/07c4isr/index.php?content=home
3-5 Nov 2008	**Global MilSatCom 2008 Conference & Exhibition,** Millennium Conference Centre, London, UK, www.smi-online.co.uk/08globalmilsatcom20.asp

*** OPEN-SOURCE MATERIAL ***

Innovations Shape LandWarNet

BY: ROBERT ACKERMAN, SIGNAL MAGAZINE
07/15/2008

Application and system advancements have been introduced for the Army's LandWarNet program in order to reach the program's goal of full connectivity from command levels to the individual soldier. Lt. Gen. Jeffrey A. Sorenson explains how LandWarNet will be the Army's way of communicating in the future, with a mission to improve situational awareness. There are a number of problems that the Army will address as part of the updates, including consolidating its data systems and developing a structure for the Army network's aerial layer.
http://www.afcea.org/signal/articles/templates/signal_connections.asp?articleid=1658&zoneid=220

Study: Reform copyright law to save digital works

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
07/14/2008

According to a study by the Library of Congress, digital works are at risk of disappearing unless better preservation methods are developed. The library's National Digital Information and Infrastructure Preservation Program is pushing for reform of copyright laws to allow digital works to be preserved like traditional authorship. New forms of authorship include websites, blog and 'user generated content', and are vulnerable to hacking, over-writing and deletion. The article also outlines recommendations for better preservation methods for digital work.
http://www.gcn.com/online/vol1_no1/46644-1.html

Cybereye | Privacy matters

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
07/14/2008

Information Technology and Innovation Foundation President Robert Atkinson spoke at a forum on digital privacy hosted by Congressional Quarterly. Atkinson spoke about how to pass the cost of information protection down to consumers, and how to define privacy and appropriate uses of personal information.
http://www.gcn.com/online/vol1_no1/46642-1.html

Symantec: Microsoft Access ActiveX attacks will intensify

BY: JEREMY KIRK, NETWORKWORLD
07/14/2008

According to vendor Symantec, the Neosploit toolkit is now available which can be used by less-technical hackers to exploit vulnerability in Microsoft software, which means that attacks on the software could intensify. Microsoft has just released a patch for the vulnerability on July 8, and the bug is especially dangerous because the infected ActiveX control is digitally signed by Microsoft, meaning it could be run automatically for many users. Microsoft released a number of suggestions in a security advisory to avoid attacks until a patch is available.
http://www.networkworld.com/news/2008/071408-symantec-microsoft-access-activex-attacks.html

Mercenaries Gone Wild

STRATEGY PAGE
07/10/2008

Cyber war waged by non-government groups is becoming increasingly more popular, as seen recently in Lithuania, where 300 websites were defaced by, apparently, pro-Soviet Russian hackers. In many cases, when highly classified personal data is stolen, it is thought that foreign governments are paying individual hackers to avoid retaliation. This is especially dangerous as the government usually has little or no control over the hacker groups, often not even having consistent contact with the hackers.
http://www.strategypage.com/htmw/htiw/articles/20080710.aspx

Cold War 2.0 heating up on multiple fronts

BY: CHARLIE COON, STARS AND STRIPES
07/11/2008

Air Force Gen. Kevin Chilton states that he worries about "asymmetric vulnerabilities" in space and cyberspace capabilities. In an interview with Stars and Stripes, Chilton talks about the need for an advanced missile-defense system, as well as aligning the United States cyber warfare policies with NATO policies. The interview details current capabilities and necessary improvements for space surveillance and defending against missiles.
http://www.stripes.com/article.asp?section=104&article=63337&archive=true

Trojan Attacks Multimedia Files Stored on Hard Drives

BY: KELLY JACKSON HIGGINS, DARK READING
07/10/2008

Christopher Alme of Secure Computing, announces that an aggressive and sophisticated Trojan is affecting many user's multimedia files that come originally from a Warez site, but can be shared through peer-to-peer file swapping. The Trojan preys on the ASF file feature in MP3 and WMA music files, although many users may not even know their files are being infected. Secure Computing states that the main purpose of the Trojan is to spread a password stealer.
http://www.darkreading.com/document.asp?doc_id=158672&WT.svl=news1_2

DoD Dives Into Cloud Services

BY: JAMES ROGERS, BYTE AND SWITCH
07/11/2008

HP has signed a deal with the Department of Defense to build an ambitious cloud infrastructure, working with the Defense Information Systems Agency. DISA CIO John Garing called cloud computing as a "top priority" as it would offer users a faster, cheaper way to run network applications. Officials have identified the new approach as a way to avoid costs for hardware and software, as well as a system for enabling armed forces to access servers on the DISA network, which oversees the U.S. military's command and control systems.
http://www.byteandswitch.com/document.asp?doc_id=158663&WT.svl=news1_1

Agencies make headway in reducing Internet gateways

BY: MARY MOSQUERA, GOVERNMENT COMPUTER WEEK
07/10/2008

Federal agencies have reduced internet gateways to only 79, and will have until the latter part of 2009 to being operating the 79 gateways under the Trusted Internet Connection (TIC). The

government is hoping to improve information security and provide an easier system of monitoring data traffic by reducing the amount of internet gateways. Agencies have already cut their amount of external connections nearly in half, from 4300 in January to 2758 in May. Agencies plan to eventually install Einstein technology to continuously monitor the traffic at the trusted Internet gateways.
http://www.gcn.com/online/vol1_no1/46634-1.html

Hacker Sentenced to 2 Years for MySpace Cyberstalking

BY:KEVIN POULSEN, WIRED BLOG NETWORK
07/10/2008
Jeffrey Robert Weinberg has been sentenced to 2 years in prison for hacking into victim Amor Hilton's Myspace account, disconnecting her cell phone service, and then placing harassing phone calls to the victim. Hilton recorded a phone call from the hacker, and reported the harassment to the police. The Southern Californian man has already served time in prison for hacking into the Lexis-Nexis consumer database.
http://blog.wired.com/27bstroke6/2008/07/accused-myspace.html

Defense 2.0 a work in progress

BY: WYATT KASH, GOVERNMENT COMPUTER NEWS
07/10/2008
Defense 2.0 refers to new era of adapting "next-generation Internet technologies" as businesses increasingly embrace social networking applications and rely more heavily on the internet to operate. "Web 2.0" has brought a lot of information security issues, including developing a process for engineering safeguards on new systems, and the lack of a security model like Web 1.0. Michael R. Nelson, a professor from Georgetown University's Communication, Culture and Technology Program states that based on recent studies, Internet use will double between 2007 and 2011, and that businesses will have to adapt to secure not only their own servers, but also access to other servers.
http://www.gcn.com/online/vol1_no1/46629-1.html

Iraq Embarks on Technology Path

BY: MARYANN LAWLOR, SIGNAL ONLINE
07/2008
The Iraq Communications Coordination Element (ICCE) is working to help Iraq build infrastructure, services, and government structure in order to improve Iraqi information technology conditions. Gen. Spano has determined that a lack of leadership and coherent processing were the most pressing issues keeping Iraq from planning and executing policy, services and infrastructure initiatives. Gen. Spano has framed a four-part plan to continue the work of Gen. Hawkins in laying the plan for creating a Joint Theater Network Control Center, and building an integrated knowledge management system.
http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1642&zoneid=236

Q&A with Lt. Gen. Michael Peterson

BY: ROXANA TIRON, THE HILL
07/10/2008

Air Force Lt. Gen. Michael Peterson answers questions on cyber security, radars and satellites and his position as the Chief of Warfighting Integration and Chief Information Officer. Peterson emphasizes the importance of the Internet in modern warfare, and how cyber attacks are becoming more sophisticated. Peterson also answers questions about the location of the AF Cyber Command headquarters, and how the Air Force is working to stay ahead of new technology and emerging vulnerabilities.
http://thehill.com/the-executive/qa-with-lt.-gen.-michael-peterson-2008-07-09.html

Massive patch coming for DNS vulnerability

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
07/08/2008

Dan Kaminsky, of IOActive, Inc., discovered a vulnerability in the Domain Name System about six months ago, which has led to major vendors of DNS releasing a patch which will stop cache poisoning and misdirection of web requests. DNS is a system that translates written names into OP addresses, which means that DNS is essential to almost all uses of the Internet. A group of 16 researchers met on Microsoft's campus in March, and agreed to release a patch in July, followed by details of the vulnerability.
http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn_daily&story.id=46623

U.S. Army challenges USAF on network warfare

BY: CARL JONGSMA, COMPUTERWORLD
07/07/2008

The Army has introduced the Network Warfare Battalion, which will compete with the U.S. Air Force's Cyber Command. The Network Warfare Battalion will centralize the Army's existing computer network operations, and will provide support to the Department of Defense. Although the Air Force has historically been responsible for intelligence and networked operations, some argue that the NSA or the FBI may be better suited for defending the electronic frontier.
http://www.networkworld.com/news/2008/070708-us-army-challenges-usaf-on.html?page=1

Lawmaker: Improve emergency systems

BY: BEN BAIN, FEDERAL COMPUTER WEEK
07/09/2008

Rep. Henry Cuellar gave a speech that emphasizes the need for improving emergency response communications and interoperability. Cueller and his subcommittee have been working with DHS to form a national emergency communications plan. Cueller emphasizes the importance of elevating the importance of the emergency communications of DHS, as well as the importance of appointing an assistant secretary to manage the Homeland Security Department's Office of Emergency Communications.
http://www.fcw.com/online/news/153088-1.html

Cyber realities setting in

BY: MICHAEL BRUNO, AVIATION WEEK
07/09/2008

Because the final basing decision for the new Air Force Cyber Command, the headquarters will be spread out among nine locations, in an effort to meet the 45 percent-manning requirements needed for initial operations in October. Maj. Gen. William Lord announced that the command will initially operate in a virtual environment, and that about 240 positions will be filled during the summer months to declare initial operations capability on Oct. 1. The article also contains a detailed report of each location, including the number of manned positions and major duties of each.

Report advocates better training for wireless Internet users

BY: ALYSSA ROSENBERG, GOVERNMENT EXECUTIVE
07/08/2008

A report released by Telework Exchange and Sprint Nextel found that federal agencies could provide more training on information security, especially for federal employees that use wireless Internet when they telework. The report surveyed teleworkers and business executives on their knowledge of information security procedures. The report also surveyed executives about their company's compliance with Department of Defense Mandate 8100.2, which requires data to be encrypted to be transmitted over wireless networks, and suggests that there needs to be a similar set of requirements for civilian companies.
http://www.govexec.com/story_page.cfm?articleid=40413&dcn=e_gvet

Microsoft confirms active Word attacks

BY: GREGG KEIZER, COMPUTER WORLD
07/08/2008

The Microsoft Security Response Center issued a security advisory stating that attackers were exploiting a flaw in Word 2002. Microsoft explains that there are only limited, targeted attacks currently, and that it could be triggered by rigged word documents that the user opens. Microsoft recommends using Word 2003 viewers in place of a patch, as 2002 is the only version that contains the vulnerability.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9107979

Over 10M Bots Active Worldwide in Q2

BY: KELLY JACKSON HIGGINS, DARK READING
07/08/2008

A report from Commtouch Software Ltd. States that Telecom Italia, Brasil Telecom and Verizon are some of the domains hosting the majority of bot infecting computers. The report also found that an average of 77% of all email is virus infected and that pharmaceutical spam made up 46% of all spam. The report states that the bots were evenly distributed geographically, with Turkey having the most at 11%.
http://www.darkreading.com/document.asp?doc_id=158434

CyberPro

Volume 1, Edition 5
July 17, 2008

Keeping Cyber Professionals Informed

Hackers to Face Off in Black Hat 'Iron Chef' Contest

BY: KELLY JACKSON HIGGINS, DARK READING
07/07/2008

Fortify Software is hosting a version of "Iron Chef" which pits two hackers against each other in a competition to find vulnerabilities in mystery code. The contestants bring their own machines and tools, and do not have access to the code until the competition begins. The audience is also able to compete with the hackers, and could win a prize for finding the most vulnerabilities. Fortify is sponsoring another competition in the same week that awards an iPhone to whoever can find the most vulnerabilities in a web application.
http://www.darkreading.com/document.asp?doc_id=158356&WT.svl=news1_1

Russians Organizing 'Political Hack Force'

BY: TIM WILSON, DARK READING
07/07/2008

According to a report in the Washington Post, researchers at iDefense have found hacker groups using internet forums and spam emails to promote "Hackers United Against External Threats to Russia", which calls for hacking into Ukraine, the rest of the Baltic states, and Western nations that support the expansion of NATO. One hacker website, hack-wars.ru, offers training and coordination to hackers in hopes of organizing Russian hackers into an organized political force.
http://www.darkreading.com/document.asp?doc_id=158344

A massive threat to national security may be in your computer

BY: J.J. GREEN, WTOP RADIO
07/08/2008

National Counterintelligence Executive Joel Brenner recently gave an interview on counterintelligence and current U.S. concerns, specifically Russia, China, Iran and Cuba. Brenner explains that a major cause of the problems is industrial espionage, and American dependence on foreign production of sensitive computer components. Rep. Frank Wolf states that the FBI has confirmed that the Chinese government was behind the attacks on U.S. government computers in 2006, but Brenner thinks that Russia is a bigger threat to U.S. cybersecurity. Brenner explains that the Russians have more sophisticated cyber espionage capabilities, and that their human intelligence force is growing inside the United States.
http://www.wtop.com/?nid=251&pid=0&sid=1435773&page=1

Weak server aided Russian cyberattacks

BY: JEREMY KIRK, TECH WORLD
07/07/2008

An official with Lithuania's Computer Emergency Response Team (CERT) announced that the attacks on 300 Lithuanian websites were due to vulnerability in web server software or the Linux operating system, and that the majority of the attacked websites were hosted on one physical server. The attacks are similar to attacks on Estonia in April and May 2007, although the Russian government denied involvement or knowledge of the attacks in Estonia as well. The attacks have been referred to the police, which has a department under the Ministry of the Interior which handles cybercrime.
http://www.techworld.com/security/news/index.cfm?RSS&NewsID=102090

Virtual Connections

BY: GAUTHAM NAGESH, GOVERNMENT EXECUTIVE
07/01/2008

Second Life is a three-dimensional virtual world, created in 2003 by Linden Research Inc., which is a 3D graphic design and network company. In Second Life, users create avatars, which are digital representations of themselves, and are able to interact with other avatars, as well as browse businesses and collect information from organizations. Second Life is part of a federal online movement referred to as Government 2.0, a public sector version of Web 2.0. Don Tapscott, the founder of nGenera, who is currently collaborating with the Office of Management and Budget in Canada to form a report on Government 2.0, states that Government 2.0 is improving government relations with the public and has the potential to improve the quality of government services.
http://www.govexec.com/features/0708-01/0708-01s2.htm

Microsoft warns of new Access attack

BY: ROBERT MCMILLAN, COMPUTER WORLD
07/07/2008

Microsoft announced that cybercriminals are exploiting a bug in software that is used by Microsoft Corp.'s Access database program, although few details are released. A Microsoft spokesman, Bill Sisk, explains that an investigation is underway, and that the attack appears to be targeted, and not widespread. Microsoft advisory has offered multiple work-arounds for the problem, but has not said when the bug will be fixed.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9107219

Call for web to stay open for all

BBC NEWS
07/07/2008

The Web Science Research Initiative (WSRI) and the National Endowment for Science Technology and the Arts (NESTA) has announced a partnership that will look at ways to ensure that the web stays safe and open for use. The WSRI currently studies how the web is growing and how to make the most of its potential. NESTA originally announced support for the program in May 2008 with cash donations, and donations from BT, a telecoms company, will also help to start the projects research program.
http://news.bbc.co.uk/2/hi/technology/7493859.stm

Wake-Up Call To Business: Tighten Up On Information Security

SPACE WAR
07/07/2008

Bruce Hallas, a specialist in information security for the UK, explains how medium size enterprises, who make up almost 60% of the total workforce of the UK, are especially vulnerable to poor information security. These businesses are reluctant to share information or vulnerabilities in fear of losing business to competitors, and are concerned about releasing potentially sensitive information. A new report, "Security Economics and the Internal Market" suggests the EU issues a breach notification law to notify consumers when their personal information has been compromised.

http://www.spacewar.com/reports/Wake_Up_Call_To_Business_Tighten_Up_On_Information_Security_999.html

Cyber Command takes shape

BY: MICHAEL HOFFMAN, AIR FORCE TIMES
07/07/2008

The Air Force Cyber Command has established a new cyberspace operator badge, as well as 17 new enlisted and officer Air Force Specialty Codes, and will soon release a detailed career plan for airmen. The command will include operators, specialists, analysts and developers. Almost all communications and information airmen will make the switch to Cyber Command, and airmen in Communications-Electronics, Information Management and Communications and Computer Systems specialty codes will switch to the new IB (Cyber Operators/Specialists) code.
http://www.airforcetimes.com/news/2008/07/airforce_cyber_career_070308

Nebraska backs Offutt for home of new Air Force Unit

ASSOCIATED PRESS
07/07/2008

Nebraska is hoping to convince the Air Force to locate its new Cyber Command headquarters at Offutt Air Force Base in Omaha. Nebraska Gov. Dave Heineman has submitted letters of support from governors from Kansas, Minnesota, South Dakota and Wyoming. Nebraska officials state that they have access to an extensive network with capacity to grow, readily available facilities including nearby universities with cyber programs, a reliable power supply and an educated workforce.
http://www.kxmb.com/getArticle.asp?ArticleId=254161

Analysis: NSA Spying Judge Defends Rule of Law, Congress Set to Strip His Power

BY: RYAN SINGEL, WIRED BLOG NETWORK
07/03/2008

U.S. District Chief Judge Vaughn Walker issued a ruling which found that Congress had clearly set out rules for wiretapping in 1978 and that the legal justification for President Bush's warrantless wiretapping program has no legal merit. The vote is scheduled for July 8, and questions whether or not the nation's highest elected officials are above the previously set wiretapping laws.
http://blog.wired.com/27bstroke6/2008/07/analysis-nsa-sp.html

Toward New Horizons: The Birth of Huffman Prairie in Cyberspace

BY: ANDREW STRICKER, MAXWELL.AF.MIL
07/05/2008

Huffman Prairie , which includes virtual learning laboratories, simulation design and production studios, classrooms, auditoriums and conference spaces, is currently developing new educational technologies, such as virtual iPod education stations, cyberspace-delivered simulations and challenges, data mashups, and many others. Huffman Prairie's Second Life virtual region was developed to provide simulation and educational experiences as well as working with the university/research community to better understand how to prepare and educate Airmen for cyber combat.

http://www.maxwell.af.mil/au/aunews/archive/0312/Articles/Huffman-Prairie-Stricker2.doc

Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites

BY: DANIEL MCLAUGHLIN, SECURITY NEWS PORTAL
07/02/2008
Lithuania suspects that Belarus or Russia is responsible for hacking into hundreds of Lithuanian websites, replacing the website's content with images of the Soviet hammer and sickle and five-pointed red star. Lithuania has had tense relations with both Belarus and Russia lately, after banning the use of communist symbols. Estonian president Toomas Hendrik Ilves walked out of a recent meeting with Dmitry Medvedev after a Moscow politician criticized Estonia's treatment of Russians.
http://www.snpx.com/cgi-bin/news55.cgi?target=www.newsnow.co.uk/A/285043700?-18613

Army activates network warfare unit

ARMY.MIL
07/02/2008
The Army Network Warfare Battalion, which will support the Army and the DoD through strategic and tactical support, was activated at Fort George G. Meade, MD on July 2. Maj. Gen. David Lacquement, commander of U.S. Army Intelligence and Security Command, explains how the battalion will provide faster, more efficient support to forces and will lead the Army in developing network warfare capabilities.
http://www.army.mil/-newsreleases/2008/07/02/10569-army-activates-network-warfare-unit/

Cyber security is essential to national security

BY: REP JOE PITTS, THE MERCURY
07/01/2008
Recent cyber attacks on Rep. Frank Wolf and Rep. Chris Smith's office computers are one of many events that point to China as a source for many cyber attacks. China is also blamed for power blackouts in the U.S. in 2003 and for a company's compromised computers following a visit to China. Rep. Joe Pitts explains how America must control the electromagnetic spectrum in order to maintain its military edge.
http://www.pottstownmercury.com/site/news.cfm?newsid=19818939&BRD=1674&PAG=461&dept_id=635485&rfi=6

DHS financial systems' security questioned

BY: BEN BAIN, FEDERAL COMPUTER WEEK
07/02/2008
The Department of Homeland Security recently hired the consulting firm KPMG to test security weaknesses in the DHL financial management systems. KPMG recommends that DHL identify the weaknesses in the system, determine a plan of action assuring that fundamental causes of IT problems are addressed, and implement the processes to fix the problems. DHS has agreed to implement the audit's recommendations as well as correcting software coding issues and re-examining the financial systems consolidation project.
http://www.fcw.com/online/news/153038-1.html

Analysis: Feds use cell phones to track us

BY: SHAUN WATERMAN, GPS DAILY
07/02/2008

The American Civil Liberties Union is suing the Department of Justice in order to obtain information on federal authority's cell phone monitoring. ACLU attorney Catherine Crump explains that the searching may violate fourth amendment rights, by using administrative subpoenas rather than a warrant based on probable cause to obtain information from phone companies. Crump also explains that the lack of public information on administrative policy regarding the cell phone monitoring makes it difficult to estimate how widespread the practice is.
http://www.gpsdaily.com/reports/Analysis_Feds_use_cell_phones_to_track_us_999.html

CyberPro Content/Distribution

This newsletter is intended to serve as a snapshot of Cyber-related events and issues, and is distributed every two to three weeks. Feel free to forward this newsletter to other interested individuals. If you have information you think should be included, or if you would like to be added or removed from distribution, please e-mail *CyberPro News Subscription*.

The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or the National Security Cyberspace Institute.