PUBLISHED BY THE INTERAGENCY OPSEC SUPPORT STAFF

THE OPSEC INDICATOR

Volume XI

Winter 2000

"Meeting The Challenges of a Changing World"

IOSS Hosts National Threat Symposium

by Tom Harig, IOSS Staff

The bucolic campus of the Johns Hopkins University's Applied Physics Laboratory (APL) in Laurel, MD. was the setting in October 1999 for the 11th annual IOSS-sponsored National Threat Symposium.

Approximately 200 guests from government and industry gathered to hear experts from the Intelligence Community discuss the multifaceted threat facing the United States in the 21st century.

This year's symposium focused on how once-anonymous adversaries can suddenly emerge on the world stage with terrifying and lethal consequences by targeting our information systems, developing intelligence denial and deception programs, employing weapons of mass destruction, and engaging in old-fashioned human intelligence collection operations.

Since the 21st century will be one in which information technology will predominate, it was fitting that the symposium opened and closed with presentations made by representatives of the National Security Agency whose mission is to maintain information superiority for the United States.

These presentations covered potential information warfare and terrorism activities associated with Y2K issues as well as a glimpse into the future of signals intelligence operations directed against this country. No longer can we expect this threat only from traditional adversaries. Proliferating technologies are enabling terrorists, criminal enterprises, and other subnational groups to mount effective signals intelligence operations against the United States and its allies with potentially dire consequences for both.

Thanks to advances in electronics, the U.S. technical intelligence collection capability is expanding. However, many countries are adapting that same technology to develop denial and deception programs designed to neutralize our advantage. Dr. Jim Bruce, the Deputy National Intelligence Officer for Science and Technology at CIA's National Intelligence Council described how our adversaries are taking advantage not only of technology to implement their programs, but also to acquire knowledge about our own sources and methods from publicly available sources.

Dr. Bruce warned that we must learn to keep truly secret matters secret, otherwise our intelligence agencies will be in for increased surprises from our adversaries.

The spectre of chemical, biological, and nuclear weapons being wielded by rogue nations or terrorists haunts the world. These weapons of mass destruction are especially appealing to adversaries wishing to confront the United States, but who cannot hope to match its overwhelming

(continued on page 3)

INSIDE THIS ISSUE:

Director's Message..... 2
OPSEC's High Rollers..... 4
OPSEC in World War II..... 8
The "DICE" Man Cometh..... 11

Director's Message

I am writing this article before January 1st, so if you have The OPSEC Indicator *in your hands right now, then I trust that we all made it through Y2K without too many difficulties. So let's get back to business. As we begin the year 2000, the message that IOSS is communicating to its OPSEC customers is, "our business is to ensure that the adversary doesn't know yours."*

This is no easy task, because we are openly and freely sharing more information about ourselves than ever before. We are experiencing the Information Age – it has exploded our capability to produce information at a rate faster than our ability to analyze and protect it. Guarding information with safes and fences is increasingly ineffective because information systems technology has produced vulnerabilities never faced in the past. As a result, OPSEC principles are more important now then ever before.

Over the years, we have marketed OPSEC as simple common sense actions that all good security processes consider when protecting assets. Who were we kidding? If OPSEC is so simple, if it is basic common sense, if it is something we have been doing for years, then why are we still giving away critical information every day? Why is the information needed by our adversaries and competitors to be successful against us so easily exploited? Why is history always repeating itself in this regard? Why are so many not using OPSEC? The answer to these questions is twofold. First, there is no accountability for the establishment of OPSEC programs; it is often easier to accept the risk than try to reduce it. Second, it's more comfortable to buy the post-Cold War "no threat" myth than it is to deal with the more subtle and elusive threats of today. If you can convince yourself there is no threat, then there is no risk, and you don't need OPSEC.

Traditional security programs are still using strategies focused on protection of classified information only. This is because only the compromise of classified information has consequences. Just try punitive action against someone who showed poor judgment by compromising critical (unclassified) information. This applies to government and contractors alike — the Industrial Security Program is based on protection of classified information. Application of OPSEC to contracts is "as needed." While this isn't necessarily wrong, it does assume that those making contractual decisions are well informed on OPSEC and where the process is properly applied. Even when OPSEC ***is*** *required in a contract, the infrastructure supporting the contractor is weak. Program managers must be prepared to identify their program's critical information and provide the threat analysis before the contractor can develop a plan and complete an analysis. Managers decide what information is critical, and then use their resources to provide comprehensive threat information often unavailable to contractors.*

Most security programs are independent, point-to-point processes, that are not integrated to ensure all assets are protected simultaneously. It doesn't do much good to do security halfway, and no one has the means or expertise to know all the answers. OPSEC, security, intelligence, and counterintelligence efforts must work together to provide adequate protection to our secrets. Finally, there is no one process in charge that has responsibility to ensure that all information and assets are being protected. It doesn't matter how secure the front door is, if you've left the back door standing open!

No, we don't need more policy. We simply need existing policy enforced. In 1999, I personally visited and presented the OPSEC message to over 60 groups representing military, civilian, and private industry organizations. What I discovered is that OPSEC is still being given lip service. Many listened to my message, agreed that OPSEC was important and then went about their business with very little changed. I heard statements like, "It's a great idea, but no one is making me do it. If it's not in the contract, I don't get paid." Private industry is waiting for government sponsors to be serious about OPSEC — and require them to do it.

When President Reagan signed National Security Decision Directive (NSDD) 298 in 1988, it was to establish a national OPSEC program to exist within all executive departments and agencies with a national security mission. Since then, much regulatory guidance has been issued. DOD Directive 5205.2 and Joint Chiefs of Staff (JCS) Publication 3-54 establish policy for application of OPSEC to government, military and contractor operations. The Department of Energy, Department of Justice, and Department of Commerce all have OPSEC policies. Even so, the failure of NSDD 298 to have an accountability structure allows it to be a matter of choice and judgment. If leadership is not accountable, if it's not part of their report card, then it is just another one of those things crying for attention and competing for resources and priority.

I will be spending much of my time this year bringing to senior leadership throughout the community the message that OPSEC is not just a good idea, it is vital to the future success of our missions. The world is changing, and it is not a kinder, gentler, safer place. OPSEC must be integrated and formally practiced by security and operations personnel at all levels. It is not something to do once a year to satisfy "check box" requirements.

IOSS is serious about supporting the needs of its customers who must have OPSEC programs within their organizations. This is our charter and we are prepared to respond. We have updated our course curricula and introduced new courses to assist you in the challenges you face. Our website (www.ioss.gov) is now up and ready to provide timely information on training, conferences, symposia, and products.

Our staff has the expertise to help start programs and energize existing programs. Just tell us what you need. The "Year of the Dragon" promises to be a challenging year for us all, so let the "Purple Dragon" make a positive impact on your operational success.

Thomas P. Mauriello

Threat Symposium *(continued from page 1)*

military superiority.

Navy Commander Rick Oswald, Director of the Central MASINT Organization's Weapons of Mass Destruction Non-Proliferation Program explained how Measurements and Signals Intelligence (MASINT) can support policy makers, war fighters, and civil defense, counterterrorist and other security specialists by detecting, identifying, locating, and neutralizing these threats.

Although most of the day was devoted to technical threats to the Nation's security, Ms. Regina Hanson, Senior Intelligence Analyst in the FBI's National Security Division, devoted her presentation to describing the "old-fashioned way" the Chinese collect high-tech information.

With Chinese intelligence operations very much in the news, Hanson's description of the methods used to spot, assess, recruit, and develop human sources was timely and appropriate.

The National Threat Symposium is one of the few events where a cross-section of government and contractor security, OPSEC, and intelligence personnel can come together for networking in a classified environment to learn the latest threat information from experts in the field.

The attendees capitalized on the opportunity to engage the speakers in lively discussions following the presentations and during the breaks.

The consensus among the attendees was that APL was an ideal place to meet. Plans are already being made for next year's symposium at the APL on November 2, 2000.

The IOSS is working with the National Counterintelligence Center (NACIC) to come up with a combined event featuring exhibit booths and speakers.

Be a part of the planning process. The IOSS needs to know your concerns and interests. If you have any ideas for speakers or topics over the coming months, please contact the IOSS.

OPSEC Professionals Hit the Jackpot at Las Vegas Regional Symposium

by Patrick D. Weadon, IOSS Staff

The Interagency OPSEC Support Staff conducted its annual Regional Conference from November 30 to December 2, 1999 in Las Vegas Nevada. The conference was held at the Department of Energy's (DOE) Las Vegas facility and was attended by more than 120 professionals from the intelligence, defense, law enforcement and U.S. Government contractor communities.

The week's events began on November 30 with the presentation of OP 200, a condensed version of the basic OPSEC course, and a seminar on web security. In addition, Mr. Kurt Haase, Director of OPSEC programs for DOE Nevada, along with DOE contractors Mr. Wayne Morris and Ms. JoAnn Archuleta, conducted a day-long seminar on OPSEC Program Management.

Need for OPSEC

The following day, formal conference proceedings began with an inspiring and informative keynote address by Captain Edwin Kanerva, USN, chief of NSA's Operations, Readiness and Assessments division. Captain Kanerva welcomed the participants and focused on the need for OPSEC in the coming century.

Mr. Tom Mauriello, Director of the IOSS, followed Captain Kanerva. Mauriello echoed the remarks made in the keynote address and noted that 2000 was indeed the "year of the dragon." He added that the prodigious use of OPSEC was the answer to the myriad of challenges presented by the Information Age.

Mauriello also noted that the protection of open source, unclassified material would play a major role in protecting national security programs in the 21st century.

Mauriello concluded by advising that the IOSS stands ready to provide expertise and logistical support to agencies, organizations and individuals involved in the protection of national security programs.

Information Wars

Mauriello was followed by Mr. Joseph Ruffini of Systems Technology Associates, Inc, Colorado Springs, CO.

Ruffini, a 25-year veteran of the "information wars" focused on the now-familiar message that the development of the Information Age has brought not only great benefits, but also great risks.

Ruffini outlined many of the legal intelligence tactics and techniques used by Fortune 500 companies and emphasized that the incredible advances in technology have left the public and private sectors exceptionally vulnerable to espionage.

Next on the schedule was Mr. Mark Mooney of the Defense Security Service (DSS). Mooney provided informative insights into the state of technology transfer and suggested ways to recognize and prevent situations that could result in the loss of America's technology.

Mooney's presentation was followed by four classified briefings featuring speakers from the Defense Security Service, the Defense Intelligence Agency, NSA, and Special Agent Del Spry of the Federal Bureau of Investigation. (FBI).

This diverse group provided information on an array of interesting topics to include threats from North Korea and China, joint COMSEC monitoring, and the Aldrich Ames case.

Ames Case Reviewed

Perhaps the most intriguing of the classified sessions was Spry's account of the events leading to the arrest of Aldrich Ames. Spry held the audience spellbound with interesting facts of the events leading up to Ames' arrest, and the incredible level of detail and commitment that was required to gain enough evidence to bring Ames to justice.

Thursday's sessions were also characterized by a series of informative briefings and workshops. Mr. Keith Rhodes, Technical Director in the Accounting and Information Management Division, Office of the Chief Scientist for Computers and Telecommunications, for the

General Accounting Office, began the day with an overview of the Y2K situation.

Like most experts, Rhodes discounted the idea of major problems, however, he cautioned that despite the fact that the world was not headed for Armageddon, there several peripheral security issues that need to be addressed before the curtain can be brought down on this issue.

DOD Efforts

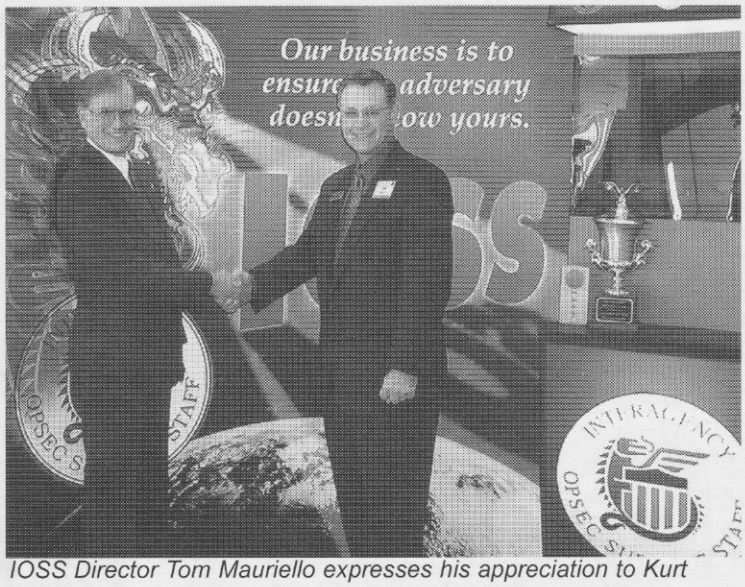
Ms. Linda Brown, a Senior Policy Analyst within the Security Directorate, Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, and Major Jim Lyons USAF, followed Mr. Rhodes' presentation with an overview of the current status of DOD efforts to reduce and or eliminate critical information from DOD web sites.

Brown and Lyons did an effective job relating the challenges facing DOD web masters and suggested several realistic solutions to meet those challenges.

Special Agent John Bellus of the FBI then took the stage to provide an overview of issues facing the National Infrastructure Protection Center (NPIC). Bellus, a 12-year veteran of the bureau, outlined the steps that the NPIC is taking to protect the nation's critical infrastructure and to combat cyberterrorism.

OPSEC Wars

Thursday's events concluded with a compelling presentation by Mr. Lawrence Marino, a 25-year veteran of the "OPSEC wars" on the events surrounding the initial assault at Waco. He also briefed on the Awareness of National Security Issues and Response (ANSIR) program, by Special Agent Kevin Walsh of the FBI.



IOSS Director Tom Mauriello expresses his appreciation to Kurt Haase, DOE, Nevada for hosting the event. The newly designed IOSS exhibition booth is in the background.

Walsh provided a summary of the exciting activities of "the public voice of the FBI for national security issues," and outlined different ways the Bureau uses the resources of the ANSIR to provide unclassified national security threat and warning information to U.S. corporate security directors, law enforcement and other government agencies.

As on Wednesday, the day's events were also supplemented by daylong threat and survey planning workshops.

The entire symposium proved to be a great resource for the OPSEC community.

New Challenges

As stated by IOSS Director Mauriello in his opening address, the challenges to our Nation's security posed by the Cold War may be behind us. However, the uncertainty created by the demise of the bi-polar world combined with the new factors created by the Information Age will require a greater commitment than ever to the use of OPSEC.

The IOSS wishes to thank Mr. Kurt Haase, and the competent, professional, and accommodating staff of DOE's Las Vegas facility for their help in making the regional symposium a great success.

The IOSS is laying the groundwork for the National Conference and Exhibition in June.

New Seminars and Course Offerings

The IOSS is proud to host two exciting new seminars this year. The first is taught by Majors, Capps and Associates, and is entitled "Advanced Analytical Concepts for OPSEC and Counterintelligence Professionals."

The second, taught by Nick Sommese and Tom Kerry of S&K Consulting, is entitled "Practical Application of the OPSEC Process."

Former FBI agents Dave Majors and Rusty Capps are familiar to many IOSS customers, having retired from illustrious careers in intelligence and counterintelligence before establishing their education and training firm.

Their seminar is designed to provide OPSEC practitioners with an insight into HUMINT collections methods and techniques, and the counterintelligence programs designed to protect information from HUMINT collection.

Nick Sommese and Tom Kerry are also well known to OPSECers, having been part of the original OPSEC establishment. They are both veteran speakers at the National OPSEC Conference.

At our request, they have expanded their conference half-day Adversary Strategy workshop into an excellent two-day seminar. The seminar teaches students how to use the Adversary Strategy method of analysis in applying the five-step OPSEC process to real world risk management problems. Students learn to reduce a complex problem to its component parts to determine what is truly important to ensure mission effectiveness.

Both seminars are extremely valuable to anyone developing expertise in OPSEC, so we are offering each seminar four times this year at no charge to students.

The classes are fast moving, requiring student participation and feedback. Classes are taught at the IOSS in Greenbelt, MD, and each is limited to 25 students. The Counterintelligence Seminar requires a U.S. Secret clearance; no clearance is required for the Practical Applications Seminar does not require a clearance. Contact the IOSS for a calendar and registration information, and plan to register early.

IOSS Training Schedule — February through April 2000

For classes offered at the National Cryptologic School (NCS), call the registrar at (410) 854-6417. For all other classes contact the IOSS.

February 10-11 — OP-300, OPSEC Fundamentals, NCS

February 14-16 — Web Content Vulnerabilities Seminar, IOSS

February 28-March 1 — Counterintelligence Seminar, IOSS

March 16-17 — OP-300, OPSEC Fundamentals, NCS

March 29-24 — OP-380, OPSEC Program Manager's Course, NCS

April 5-6 — Practical Application of the OPSEC Process IOSS

April 27-28 — OP-300, OPSEC Fundamentals, NCS

The OPSEC Indicator

Published Quarterly by

The Interagency OPSEC Support Staff

6411 Ivy lane
Greenbelt, Maryland
20770-1405

Thomas P. Mauriello
Director

Lynne M. Yates
Editor

Telephone
(301) 982-0323
FAX
(301) 982-2913

This is a U.S. Government Publication

Contents are not necessarily the views of, or endorsed by, any government agency.

DRAGONTALK

New People on the IOSS Team

The IOSS has recently hired a cadre of uniquely qualified employees and detailees. Join the IOSS in welcoming them into the OPSEC community.

Jim Aycock is a detailee from the Commerce Department at the National Institute of Standards and Technology, Gaithersburg, MD. Jim began his career as a police officer at the University of Maryland. From there, Jim joined NSA as an investigator before moving to Commerce, where he conducted administrative, personnel security and criminal investigations. He also conducted annual "good citizenship" reviews of candidates for the Malcolm Baldrige National Quality Award.

Jim has 27 years of experience in law enforcement and security disciplines and holds a master's degree in public and business administration. He will be the Web administrator and teach classes for IOSS.

Ronald Burley is a telecommunications specialist on a detail from the General Services Administration (GSA). Ron began his career in the Air Force as a security specialist and cryptologic technician.

Later, Ron left the Air Force and worked as a contractor for the Department of State. There he supervised the engineering and installation of nonsecure communication systems for American embassies worldwide.

Ron joined GSA in 1994. Ron was a project manager assigned to GSA's Office of Information Security. He has also worked as a systems administrator for the Department of Energy and the Pentagon's Single Agency Management Division.

Ron has a degree in criminology and is certified as a network administrator, network engineer, and a contracting officer.

Gary Manning joins the IOSS as an intelligence analyst and will be involved in many IOSS programs and projects. Gary brings more than 20 years of OPSEC experience to the staff.

He has provided intelligence analysis support to OPSEC for more than 13 years, and has more than 5 years of specific program management experience with integrating government and private industry security programs and requirements.

Gary's 22-year Federal career has included various security and intelligence positions with the U.S. Army and the Defense Security Service (DSS).

His career began with the U.S. Army and his civil service experience includes counterintelligence support to technology protection, personnel security, industrial security and the detection and deterrence of espionage.

Gary's most recent assignments include positions such as Senior Intelligence Officer at the Defense Intelligence Agency and Chief of Counterintelligence for the DSS. He has an MBA and a bachelor's degree in criminal justice. Gary is an accomplished public speaker and instructor.

Rick Townsley comes to the IOSS with a diverse background and a master's degree in public administration. He was the first systems administrator for a new DOD E-911 emergency phone system—the first of its kind in the U.S. government.

Rick is a certified Information Systems Security analyst and has earned National Cryptologic School adjunct faculty certification. Prior to joining the IOSS, Rick worked as a DOD systems threat analyst.

Rick also served for 12 years as the director of a crime laboratory in Anniston, AL. Rick is a visiting professor at Bowie State University, where he teaches criminalistics.

Lynne Yates is the new Editor of the OPSEC Indicator. She has more than 20 years of related experience. Most recently, Lynne was the Editor of a monthly DOD publication.

Previously, Lynne spent several years as a DOD counterintelligence Special Agent conducting background and special investigations. For more than four years, she provided security and counterintelligence awareness briefings for government employees and contractors.

Lynne has also held several posts in the human resources field. Prior to joining the government, she worked as a defense contractor. Lynne has a degree in journalism and will perform OPSEC awareness training and and contribute to other IOSS publications.

The Battle of the Bulge

How Hitler's OPSEC Resulted in Massive Allied Casualties

by Patrick D. Weadon, IOSS Staff

For many, the winter season is a time to take stock and reflect on the events of the past. For this author, dark winter days sometimes serve as a reminder of the Battle of the Bulge. This horrific battle, which lasted from December 16, 1944 to January 28, 1945, was one of the largest land battles of World War II. The cost in lives was devastating.

America has always mourned the horrible loss of more than 50,000 lives lost during the long Vietnam conflict. It is shocking to consider that, in a brief span of 44 days, 19,000 American soldiers lost their lives in this battle.

Not Just For Good Guys

Despite the ultimate Allied victory, Hitler was able to deal a devastating blow to the Allied efforts to end the war in early 1945. He was able to throw a monkey wrench into the Allied war effort for many reasons.

For OPSEC professionals, the battle holds many important lessons; not the least of which is never to forget that OPSEC is not some secret weapon that can only be used by the "good guys."

Let's go back to that dark snowy winter of 1944. Imagine you are one of the most effective fighting tools known to man—an American infantryman.

You are safely sequestered in your foxhole in the Ardennes awaiting your orders. You have marched and fought halfway across Europe. You are still alive; many of your buddies that landed with you on the 6th of June are not. You were scared to death the first day your boots first touched the bloody sands of Omaha Beach, and you remained scared to death that you will not live to see another Christmas.

Lately, however, you have reason to be cautiously optimistic. You keep hearing from a buddy at Headquarters that this crazy war just might be coming to a close soon. The word is that the German armies are reeling from one defeat after another.

Many of the senior officers in your command are planning to go on leave to Paris. Some of your buddies have even taken to sledding on the new fallen snow.

You tell yourself to stay cautious and to not assume anything, but every now and then your mind comes back to one wonderful thought, "Maybe this horrible war will be over soon and we can all go home!" Unfortunately, home is the last place you will be going.

Due to Allied hubris, and an outstanding OPSEC plan executed by the German high command, you will soon be retreating from an onslaught of enemy tanks and doing everything in your power to avoid joining your poor dead buddies left behind on Omaha beach. Unknown to you, your Supreme Commander, General Eisenhower, is receiving daily "ULTRA" intelligence intercepts which clearly indicate that German forces are growing steadily weaker and that the German general staff is planning a series of defensive actions to thwart the coming Allied offensive.

From the beginning of the war to the present day, the ULTRA intercepts have been a godsend, enabling Eisenhower and the Supreme Allied Command to know the enemy's intentions.

Many senior officers (including Ike) are concerned about the thinly held lines on certain areas of the Allied front. ULTRA however provides no indication of a German offensive, so no thought is given to addressing the situation.

Surprise Attack

What you and General Eisenhower do not know is, like Frederick the Great, Adolf Hitler plans to conduct a massive winter attack against enemy lines. He will attempt to streak across Belgium and France to capture the vital port of Antwerp.

This move (which the German general staff considers unlikely to succeed), has the potential to split the Allied armies in two and destroy the vital supply line that emanates from Antwerp. Far worse, the plan, even if partially successful, could prolong the war by months and increase the already strained relations between American and British commands.

The ULTRA information is not

totally inaccurate. Hitler's armies *are* in trouble—they are short of vital supplies, most importantly, fuel.

Morale is still high, but it becomes more evident every day that it is only a matter of time before the Allied armies cross the Rhine. Hitler, in an effort to overcome these factors, decides to fall back on an effective technique used by armies throughout history—a surprise attack.

This will not be easy, as the Allies have shown a strange talent for being in the right place at the right time. In order for the attack to succeed Hitler must use something familiar to all of us in his planning—OPSEC.

Hitler's Intricate OPSEC Strategy

The following is a list of operational steps taken by the German high command as listed in Chapter 16, "*A Rather Ambitious Attack*" of the *West Point History of the Second World War*.

•Hitler selected the moniker "Watch on the Rhine" for the operation. This was done to encourage the Allied belief that the Third Reich planned to stay on the defensive. He also ordered the flooding of the airways with detailed messages on phony defensive operations.

•Only a handful of senior officers were notified of the plan. Those that were given information on the attack were told that any breach of security concerning the attack on their part would result in their death.

•No one with any knowledge of the planned attack was allowed to fly west of the Rhine.

•Camouflage discipline was maintained and radio blackout was vigorously enforced.

•Rather than assign a letter or number to the date for the launching of the attack, the designator "0" was given to the operation—a simple but striking departure from past designators. Hitler surmised that even if documents concerning the attack were captured, the 0 designator would prevent the Allies from drawing any conclusions.

The above steps, along with other tactical moves in the northern sectors near the Roer River, led to the following. On December 15, German intelligence staff nervously checked the American sector to try to determine if the buildup had been discovered. They could find no such sign. Intelligence reported no U. S. reinforcements moving to the Ardennes area.

The plan seemed to have worked—that night as the units moved to the line of departure, German troops first learned of the plan to attack the American sector at 5:30 a.m., on December 16, 1944. In short, through the carefully applied use of OPSEC, the German Army was able to achieve complete surprise. As the German divisions smashed through the American lines, all hell broke loose. Many units simply cut and ran; others managed somehow to hang on and fight back.

Indicators

To this day, historians still ponder how this could have happened. As was the case with the surprise attack at Pearl Harbor, there were many indicators that could have led analysts to a different conclusion regarding German intentions. For example:

•On December 14, a woman who crossed over from the German lines told the commanding general of the 28th Infantry that the woods near Bitburg were filled with German equipment. Her accounts were so credible that she was sent to First Army headquarters for further interrogation. She arrived on December 16.

Year of The Dragon

According to the Chinese Zodiac, those born in the "Year of the Dragon" are full of vitality and enthusiasm, intelligent, gifted and perfectionists — but these qualities make them unduly demanding to others.

In this Year of the Dragon, 2000, let's enthusiastically and painstakingly apply the OPSEC 5-step process to all we do – and demand that everyone with a national security mission do the same – to ensure critical information is completely protected.

- Aerial reconnaissance from December 8-15 picked up sizeable movements of equipment and troops both east and west of the Rhine.

- Several nights before the attack, both the 106th and the 28th Infantry Divisions reported more vehicle noise than usual. The reports of the 106th were dismissed because they were considered "too green." The 28th Division, having spent a great deal of time on the line, concluded that the increased noise was due to various units being relieved.

- Several recently captured German POWs and deserters advised that an attack would be made before Christmas. Their claims were dismissed for various reasons.

Hugh M. Cole, the author of the U.S. Army's official history of the Ardennes offensive, perhaps said it best. "The Americans and British looked in a mirror for the enemy and saw... only the reflections of their own intentions."

False Allied assumptions about enemy capabilities and intentions had brought disaster. The supreme irony perhaps is that Hitler would ultimately fall prey to his own faulty assumption, namely that the American Army would be no match for his well-trained infantry and tank divisions.

Hitler was able to deny the American command the critical information it needed to ascertain his intentions.

Fortunately for the Allies, he did not gain enough critical information about the allied counterattack to allow his armies to reach Antwerp. In the end, the brilliant use of operation security by the German Command was not enough to overcome the Allied will to fight back.

A Lesson in OPSEC

The major lessons then for OPSEC professionals are quite simple.

Classified information will always be a major factor in discerning the intentions of the adversary, but to get the complete picture everything must be considered. Basing analysis only on classified information (as Eisenhower did with ULTRA) runs the risk of ignoring the obvious.

OPSEC, properly applied, can supply the needed edge to obtain the element of surprise. (It was the Germans in this case who were able to put this theory to good use.)

Always be ready to question your assumptions about what you know about your adversaries and, more importantly, what they know about you.

As we enter the new century, the intelligence and defense communities will continue to benefit from advanced technology and the many tools produced by the Information Age.

We must never forget, however, that battles are often lost and won, not by who has the best hardware or supplies but by those that have the ability to use critical information to their advantage.

Midway, the Battle of San Jacinto and the destruction of the Spanish Armada are further examples of this. Luckily, the Allies prevailed in the Battle of the Bulge; nevertheless the events of December 16 to January 28, 1944 in the cold dark forests of the Ardennes are a stark example of just how valuable OPSEC can be in overcoming a superior force.

QUARTERLY QUOTE

What concerns me is not the way things are, but rather the way people think things are.

—Epictetus

Ray Semko, the "DICE" Man, Joins the IOSS

Ray Semko, known to many in the OPSEC and defense communities as the the "DICE Man" joined the IOSS on January 18.

Ray brings more than 30 years of military and government security and counterespionage experience, but he is most closely associated with his Defensive Information to Counter Espionage (DICE) briefings. He has been presenting these around the world since he initially created them for Defense Intelligence Agency (DIA) employees in 1988.

Ray will be traveling for the IOSS to raise awareness of the threats to U.S. security and the value of OPSEC in neutralizing these threats.

Ray, a native of Pittsburgh, PA, joined the U.S. Army at 18 and served in Viet Nam. He retired from the Army after 21 years—17 spent as a counterintelligence agent.

He joined the DIA in 1988 and was the first DIA representative to the IOSS in 1989. He was also a regular speaker at the national OPSEC conferences.

In addition to his counterintelligence duties, Ray has performed OPSEC assessments for the Army, Pentagon and Joint Chiefs of Staff, among others.

Prior to joining the IOSS team, Ray worked as a Counterintelligence Officer for the Department of Energy(DOE) since 1992.

At DOE, his DICE briefings were so highly requested that, had his schedule permitted, he could have given one every day of the year. Ray revamps the immensely popular DICE briefing yearly to keep it fresh—and the threat information viable.

When not briefing, Ray spends time with his family in rural PA. Ray has officiated almost every sport and was once the coach of the Italian National Football team. Ray also works as a deejay in his few moments of spare time.

IOSS Unveils New INTERNET Web Page

by Jim Aycock, IOSS Staff

The newest IOSS customer service is now online! The INTERNET website went up December 1, 1999 and it is the best way to be up-to-date on IOSS programs, courses, and products. When you log on to the web-site at:

www . ioss . gov

you will see the IOSS symbol spinning toward you, a reminder of the dragonlike nature of our adversaries and the vigilance that must be maintained.

The first section, **About Us** provides an overview of the IOSS and National Security Decision Directive 298 that established our program. The next section is dedicated to **Products and Services**, offered to customers upon request including *The OPSEC Indicator.* Other publications include the *Glossary of OPSEC Terms; Applying OPSEC to US Government Contracts; The Dice Man's X Files; and the Intelligence Threat Handbook*. Videos to order include: *OPSEC: Protecting our Edge / Protecting Tomorrow's Technology Today; OPSEC & Counternarcotics; and OPSEC: The Art of Working Together*.

Multimedia presentations include *OPSEC Fundamentals: Computer Based Training Series* and others.

The third section is dedicated to the **Calendar of Events**. Upcoming courses, conferences and symposia are scheduled months in advance. To facilitate participation, this section is frequently updated.

The fourth section of the website explains the National OPSEC Awards Program. These prestigious awards recognize three classifications of OPSEC efforts: organizational achievement, individual achievement, and multimedia program development.

The newly designed website also contains links to other Federal agencies for effective research and coordination in the OPSEC arena including links to the Department of Justice, the General Services Administration, and the Department of Energy.

Interagency OPSEC Support Staff
6411 Ivy Lane
Greenbelt, MD 20770-1405

First Class Mail
Postage and Fees Paid
National Security Agency
Ft. Meade, MD
Permit No. G-712

Mark Your Calendar

2000 National OPSEC Conference & Exhibition

June 6 - 9, 2000
Hyatt Regency Monterey
Naval Postgraduate School
Monterey, California
Preconference Seminars - June 5, 2000
Join us in Monterey for a week of outstanding briefings, workshops, and exhibits.

For more information contact:
McNeil Technologies, Inc.
Phone: 410-553-6465
Fax: 410-553-9275
Email: opsecconf@
mcneiltechmd.com