AMERICAN INTELLIGENCE JOURNAL

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Counterintelligence, Operations Security, and Information Assurance

NMIA

Vol. 29, No. 2, 2011

American Intelligence Journal

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Vol. 29, No. 2 *2011* ISSN 0883-072X

The *American Intelligence Journal* (*AIJ*) is published by the National Military Intelligence Association (NMIA), a non-profit, non-political, professional association supporting American intelligence professionals and the U.S. Intelligence Community, primarily through educational means. The Board of Directors is headed by Lieutenant General James A. Williams (USA, Ret), and the president of NMIA is Colonel Joe Keefe (USAF, Ret). NMIA membership includes active duty, former military, and civil service intelligence personnel and U.S. citizens in industry, academia, or other civil pursuits who are interested in being informed on aspects of intelligence. For a membership application, see the back page of this *Journal*.

Authors interested in submitting an article to the *Journal* are encouraged to send an inquiry – with a short abstract of the text – to the Editor by e-mail at <aijeditor@nmia.org>. Articles and inquiries may also be submitted in hard copy to Editor, c/o NMIA, 256 Morris Creek Road, Cullen, Virginia 23934. Comments, suggestions, and observations on the editorial content of the *Journal* are also welcome. Questions concerning subscriptions, advertising, and distribution should be directed to the Production Manager at <Admin@nmia.org>.

The *American Intelligence Journal* is published semi-annually. Each issue runs 100-200 pages and is distributed to key government officials, members of Congress and their staffs, and university professors and libraries, as well as to NMIA members, *Journal* subscribers, and contributors. Contributors include Intelligence Community leaders and professionals as well as academicians and others with interesting and informative perspectives.

NMIA CORPORATE MEMBERS

Accenture
Advanced Government Solutions, Inc.
Advanced Technical Intelligence Center
American Military University
AMERICAN SYSTEMS
ANSER, Analytic Services Inc.
BAE Systems
CACI
CALNET Inc;
Computer Sciences Corporation
Concurrent Technologies Corporation
DynCorp International
Eagle Ray, Inc.
EKS Group, LLC
General Dynamics Advanced Information Systems
General Dynamics Information Technology
GeoEye
Henley-Putnam University
Institute of World Politics
ITSC Library
JB&A, Inc.
KMS Solutions, LLC
L-3 Communications
Liberty University
Northrop Grumman
MacAulay-Brown, Inc
Parsons Infrastructure & Technology Group, Inc.
Pluribus International Corporation
Riverside Research Institute
Science Applications International Corporation (SA
SOS International, Ltd.
SPARTA Inc. a PARSONS company
Sytera, LLC
TAD PGS
Thermopylae Sciences & Technology
The SI
Zel Technologies, LLC.

AMERICAN INTELLIGENCE JOURNAL

Table of Contents

Table of Contents *(Continued)*

The opinions expressed in these articles are those of the authors alone. They do not reflect the official position of the U.S. government, nor of the National Military Intelligence Association, nor those of the organizations where the authors are employed.

PRESIDENT'S MESSAGE

"Made in the USA: Stolen and Transferred to an Unnamed Country with a Cool Wall, Great Noodles and Countless Cyber Hackers"

This is a line from an economic espionage poster produced by the National Counterintelligence Executive (NCIX). Funny, catchy, but not at all taken seriously, not yet anyway. A prediction: this cyber security theme will soon achieve a place in our lexicon comparable to "Loose Lips Sink Ships" and "Uncle Sam Wants You" – because this is a war, and one just as dangerous and all-consuming.

Last month we had an unprecedented event. The former Director of National Intelligence (VADM Mike McConnell), the former Secretary of the Department of Homeland Security (Michael Chertoff), and a former Deputy Secretary of Defense (William Lynn) discussed in the open "China's Cyber Thievery Is National Policy – And Must be Challenged" (*Wall Street Journal*). Saying their comments would have been classified three months ago, they referred extensively to an October 2011 NCIX Report to Congress: "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace." Chinese cyber espionage has been hugely successful, resulting in the loss of "billions of dollars" and "millions of jobs" for the U.S. with equally large impacts on U.S. national security. "It is much more efficient for the Chinese to steal innovations and intellectual property – the source code of advanced economies – than to incur the cost and time of creating their own. They turn those stolen ideas directly into production, creating products faster and cheaper than the U.S. and others." Unfortunately, since these three distinguished national security leaders made a very public alarm call, the volume of the resulting national dialogue has been disappointedly quiet.

During recent Congressional testimony, FBI Director Robert Mueller said the cyber threat will surpass the threat from terrorists. "In the same way we changed to address terrorism, we have to change to address cybercrime." National Intelligence Director James Clapper commented, "The Cyber Threat is one of the most challenging ones we face"…"We foresee a cyber-environment in which emerging technologies are developed and implemented before security responses can be put in place."

This *AIJ* offers a superb array of articles, focused on counterintelligence, operations security, and information assurance, critical tools in cyber defense. You'll find leading-edge dialogue in plain language from a mixture of scholars and intelligence practitioners.

Two recent and very public examples of cyber terrorism: the WikiLeaks release of sensitive U.S. data and the legal travails of Megaupload had similar characteristics – government secrets or proprietary materials were stolen; they were used other than intended, for substantial gain of those involved in the activities; and the defensive response was overwhelmingly damaging. The WikiLeaks case led to the questioning of the IC "need to share" initiatives. Megaupolad is impacting the free flow of information (PARS/SLARS efforts in Congress), using tactics and achieving objectives common to any terrorist organization.

Stuart Varney (whom I have admired since his early days at CNN) did a recent piece contrasting the Facebook IPO and the bankruptcy of American Airlines. Facebook is the "new entrepreneurial way to success for American Business." Facebook has about 3,000 employees for a $70-$100 billion company. American Airlines is the "old" face: 70,000 employees, 80% union, large pension debt, and losing billions annually. China's new entrepreneurial approach is simpler, cheaper, less risky, and with a much greater return on investment. And it is using every tenet of Sun Tzu's *The Art of War*; including "know your enemy." Ed Giorgio, formerly of NSA, points out the asymmetric advantage for China: "They know us much better than we know them (virtually every one of their combatants reads English and virtually none of ours reads Mandarin)."

NCIX also put out an insightful "Black Market Price List" for obtaining specific elements of your personnel information on the black market. I find these numbers cheap compared to the potential take:

- Your social security number, $3.
- Your mother's maiden name, $6.
- Mag-stripe data from a "secure premium-level credit card," $80.
- Name and password for your online bank account, $1,000.

The cyber threat is so large that its scope is hard to grasp, and the cost for the U.S. to defend and respond is also growing quickly. The list of high-profile computer breaches by China is endless: Google's Gmail, Yahoo, Adobe, Rackspace, Northrop Grumman, Lockheed Martin, The Pentagon, NASA, State and Energy, DoD Labs, The World Bank, NASDAQ, the International Monetary Fund, EMC's RSA, and two Canadian economic ministries. Economic espionage, including cyber, is even more pervasive. Thefts of Valspar paint formulas, as a minor example, are estimated to be worth over $20M in R&D costs. And China is not even the biggest threat; number one is said to be Russia (both state and criminal), number two is Israel, then France, Brazil, and the list goes on. Countering these efforts is costly. The FY2012 Presidential budget request has over $4B easily identifiable for cyber security defense, or over $12B, depending upon how you count. The Air Force has 30,000 personnel that have been transferred from support functions to cyber warfare. Over 90,000 uniformed service personnel engage in cyber warfare. And

things "cyber" in the U.S. government are too numerous to list: Cyber Czar, National Cyber Security Division, Cyber Command, Cyber Genome, etc.

Who among our readers believes they may have access to electronic information which may be of interest to our adversaries? If so, have you read and understood the NCIX report? (http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf). Another important read related to this volume of *AIJ* is the NCIX's most recent National Counterintelligence Strategy of the United States. (http://www.ncix.gov/publications/policy/NatlCIStrategy2009.pdf).

NMIA holds at least two symposia each year. Our NMIA symposium in November, titled "Intelligence Support to Small Unit Operations," received outstanding feedback. It was based on the premise that if you are at the pointy end of the spear you will have different perspectives and resources than if you are a D.C. analyst. We had an outstanding group of speakers and panelists, folks you don't normally get to hear from and engage with.

Our Spring 2012 National Intelligence Symposium provides a Community-wide overview of both substantive and resource developments and challenges impacting the intelligence mission. We are privileged to welcome our Keynote Speaker, the Honorable James R. Clapper, Director of National Intelligence; the heads of the DoD intelligence agencies; and the Service intelligence chiefs addressing how the IC will meet the dynamic demands on intelligence in the face of our country's deficit and budget challenges.

We are in the initial stages of planning for our Fall 2012 Symposium, likely to be held in September, which will be focused on the Defense Attaché world and the Foreign Area Officer (FAO) community. NMIA is also planning two "workshops" for later this year, one on "Intelligence Education" and one on "Counterintelligence Developments." Our annual Intelligence Community Awards Banquet will be on Sunday, May 20. Individuals and organizations can register now at www.nmia.org. This always proves to be a great event with good food, updated venue, a superb networking opportunity, but most importantly a chance to recognize the best and brightest from across the intelligence discipline. Our National Military Intelligence Foundation (NMIF) has completed its annual scholarship awards for students pursuing courses of study in intelligence and related disciplines. This year we had a record number of awardees and record scholarship dollars thanks to the generosity of our sponsors and the success of our programs.

Joe Keefe

From the Editor's Desk…

The theme of this issue of *AIJ* echoes that of an NMIA National Intelligence Symposium held a couple of years ago. That forum featured several panel discussions held at the classified level led by senior officials from DIA's relatively new Defense Counterintelligence and HUMINT Center (DCHC, or "DX," as it is affectionately known by its internal office symbol) and ODNI's National Counterintelligence Executive (NCIX). The Board of Directors thought it would be illuminating to follow up that effort with a *Journal* issue focused on the same concerns, but obviously at the unclassified level so that all AIJ readers can benefit. The result is the enclosed collection of articles, whose principal focus is on the theme "Counterintelligence, Operations Security, and Information Assurance."

An article in the September 28, 2011, edition of *The Washington Post* caught my eye. By Derrick Dortch, it was titled "Counterintelligence: A Quiet but Critical Mission." The author observes, "Every so often we hear about a big espionage case in which someone has been caught spying on the United States. Robert Hanssen, a former FBI agent, and Aldrich Ames, a former CIA employee, both gave secrets to the Russians. Then there were 10 Russian spies caught in 2010. Each time it seems we are still a bit startled. But it goes on more than we know." Here where I work at DIA, employees were bowled over a decade ago when one of their own, long-time Cuba analyst Ana Montes, was arrested in September 2001 while spying for the Cuban government. That case garnered much less attention than Hanssen's or Ames', in part because it hit the news shortly after the terrorist attacks of 9/11 and thus got shoved to the back pages of the paper. American citizens had more immediate worries on their minds at the time. Yet, it was the classical situation of an insider betraying her country, and I must admit I was personally acquainted with the perpetrator from having attended regional warning meetings and National Intelligence Estimate coordination sessions alongside her over twelve years earlier while working for the Army Intelligence Chief in the Pentagon. How is it we fail to see the warning signs until too late? Darlene Holseth explores this problem in her insightful article about insider betrayal.

The *Post* writer goes on to lament the recent loss of a friend who he claimed knew better than most about such issues. That individual was Brian Kelley, a former CIA case officer, Air Force CI officer, and NCIX official. Dortch describes Kelley as "a hero, an honorable man who was awarded the Distinguished Career Intelligence Medal." The writer characterizes the field of CI and one of its noted practitioners this way: "Counterintelligence is what quiet professionals like Brian do every day to protect us. He

sacrificed much during his service, then became an educator at CIA University and the Institute of World Politics. He was passionate about his work and an example for those who are interested in 'spy catcher' careers." Dortch next ticks off a list of agencies for aspiring CI officers to consider: CIA, which has CI analysts and officers; DIA, which absorbed the Counterintelligence Field Activity (CIFA) into the consolidated DCHC; FBI; the Navy's NCIS, which many TV watchers assume just investigates murders, but is also involved in the CI arena; the Army's INSCOM, whose 902nd MI Group focuses on CI, plus the Army's CID; the Air Force's OSI; DoD's Defense Security Service (DSS), whose Director Stan Sims and CI Chief Bill Stephens have contributed an excellent article explaining DSS's role in promoting sound CI practices in cleared industry; the Department of Energy, whose Office of Intelligence and Counterintelligence deals with threats to this country's nuclear energy capacity and other scientific national security matters; and, finally, NCIX, whose mission is to be the unifying agency of the U.S. CI community.

In fact, the just-retired NCIX, Robert "Bear" Bryant (no kin to the legendary Alabama football coach), recently was guest speaker for a luncheon meeting of the Standing Committee on Law and National Security of the American Bar Association (ABA). Bryant spent four decades in the CI business. Since his 2009 appointment as NCIX, he has established a U.S. CI program "that reflects the evolving threats to American interests with a strong focus on insider threats, emerging technical threats, cybersecurity and economic espionage." Prior to his NCIX stint, he served as the Deputy Director of the FBI "where he was involved in the successful investigations and prosecutions of the spies Aldrich Ames, Earl Pitts and Harold Nicholson," according to the ABA announcement.

Closely related to CI are the fields of Operations Security (OPSEC) and Information Assurance (IA). It seemed to make sense to dedicate an issue of *AIJ* to all three, in the hopes that intelligence-focused experts would contribute their thoughts about CI, operations-focused personnel about OPSEC, and information technology specialists about IA. OPSEC is defined in Wikipedia (which NIU academicians are expected to shy away from!) as "a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information."

The IA focus follows up the theme of a 2010 *AIJ* issue, "Cyber Security and Operations." As I said at the time, this is a burgeoning, complicated field for which the definitive policies and organizational relationships are still evolving. From time to time, *AIJ* will feature articles on cyber matters that hopefully will help solidify the significance of this decidedly 21st century threat. In this issue, Tom Ranieri, a repeat performer in our pages, discusses the Internet in terms of ideology and the CI challenges thus posed. In May 2011, DIA held an event called "Cyber Awareness Seminar/IC Focus," sponsored jointly by the DCHC and the Directorate for Technical Collection. It was taught by the DoD Cyber Crime Center's Defense Cyber Investigations Training Academy (DCITA), "the premier defense academic institution for digital forensics and cyber investigations." That same month, White House officials launched an "International Strategy for Cyberspace," which the administration touted as "unifying U.S. engagement with international partners on a range of cyber issues for the first time." The strategy being a whole-of-government effort, participants at the launch included Secretary of State Hillary Clinton, Homeland Security Secretary Janet Napolitano, Commerce Secretary Gary Locke, Attorney General Eric Holder, then-Deputy Defense Secretary Bill Lynn, and Deputy National Security Advisor for Homeland Security and Counterterrorism John Brennan. One of the CI-related goals of the new strategy is to "protect U.S. networks from terrorists, cyber criminals

and states, and will respond to hostile acts in cyberspace as it would to any other threat to the country."

A huge concern of the U.S. federal government is how to capitalize on the benefits of the sweeping trend toward use of social media without endangering national security. According to one contract firm engaged with the government in this arena, "The use of social networks is now allowed in the federal agency enterprise for public engagement, interagency collaboration, and federated communication. Hundreds of thousands of users have access to read and write on Facebook, Twitter, Skype, LinkedIn, wikis, blogs, etc. But today there is little to no information assurance, data leakage prevention, eDiscovery content moderation, logging or social network application controls." Several of the articles in this issue of the *Journal* cite the growing use of social media and its consequences for CI and IA.

Such developments greatly worry government officials at all levels, as several of our authors in this issue of *AIJ* will attest. Federal agencies are frantically trying to educate their workers about the rapidly expanding threat picture. For instance, in the department in which I work, DoD Directive 5240.06, dated May 17, 2011, mandates annual refresher training in Counterintelligence Awareness and Reporting via a briefing given at the SECRET/NOFORN level. In October 2011, new DIA employees began to receive this training as part of their TOUCHSTONE classes required for all newcomers. I am certain other departments and agencies have taken similar steps. The increasing attention and interest in CI is reflected by the fact that NIU now has an approved certificate program in the subject, which has proven to be quite popular with students. This program is laid out in the pages that follow by one of its designers, retired LTC Joe O'Neill.

This issue of the *Journal* leads off with an article by an Australian colleague, Hank Prunckun, on the need for CI to be grounded in theory, which is important because most articles tend to focus on practice instead. Aden McGee discusses CI in irregular warfare and the need for it to be treated as a "joint" commodity. One of our veteran authors, R.J. Godlewski, looks at the financial aspects of CI and explains how money contributes to asymmetrical warfare. Continuing our emphasis on China, which we intend to do with every issue of the *Journal*, we offer a wealth of viewpoints on that behemoth and daunting CI challenge, by such experts as Stéphane Lefebvre of Canada; John Dotson, who teaches in NIU's Reserve Program; and Maj Dave Berkland, who works on the Air Staff in the Pentagon. Bill Streifer digs back into history to examine what the OSS was up to in China, and specifically Manchuria, in the final years of World War II. As usual, we also can count on another historian, Ken Campbell, to profile an international intelligence stalwart of the World War II era, this time examining the career of a Swiss intelligence official, Hans Hausamann. Moving back into the present, LT Mike Cantilo surveys the overall CI threat in the post-Cold War period, while Col Eric Gartner of OSI examines CI and security in the context of Clausewitzian theory, based on research he conducted while at the National War College.

Although not directly related to our CI theme, MAJ Mike Adamski evaluates ODNI analytic standards. Dr. Gordon Middleton of Patrick Henry College's Strategic Intelligence Program suggests ways of overcoming information overload, and DIA librarian Bianna Ine explains how Open Source Intelligence (OSINT) can benefit the IC, which apparently ODNI has figured out based on the establishment of its widely utilized Open Source Center. An NMIA award-winning paper at the Air Command and Staff College is presented in this issue of *AIJ*, as Maj Colby Kuhns, a veteran U-2 pilot, advocates for the potential utility of airborne intelligence, surveillance, and reconnaissance (ISR) assets in stability operations and explains why these get short shrift in the heat of battle when priorities seem to point in a different direction. A little less operationally focused, yet filling the bill in terms of our goal of having *Journal* articles bridge the divide between theory and practice, is part two in a series of articles about critical thinking and sensemaking by David

Moore and Robert Hoffman, this time offering what they call the "Data-Frame Theory" of sensemaking as a model intelligence types should follow.

Finally, as a precursor for the Spring 2012 issue of *AIJ*, the overall theme of which will be "Cultural Intelligence and Regional Issues," COL Laurie Hummel and Peter Siska of the Department of Geography and Environmental Engineering at West Point expound on their concept of a regional knowledge system. COL Hummel, currently deployed to Afghanistan assisting a counterpart service academy in Kabul, is working on another article with some remote colleagues in her spare time that will tie in nicely with some other regional pieces in the works to provide us with an intriguing next issue. If any of you *Journal* readers, regional experts or not, culturally attuned or not, would like to contribute to that issue, please contact either myself or Kel McClanahan, my associate editor and book review overseer, and let us know what's on your mind and/or ready to come off the point of your pen. My new e-mail address for *AIJ* business is aijeditor@nmia.org, which feeds directly into the account that many of you have been using, William.Spracher@dodiis.mil; phone number is (202) 231-8462. Kel can be reached at aij.associate.editor@gmail.com. The suspense date for getting manuscripts in to us is April 30, 2012. Remember, not all articles in a given issue have to fit the announced theme, but we would like a solid core of 6-8 of them to do so. If a manuscript relates to the theme, it has a better chance of passing muster with this editorial team and with the Board of Directors, which has the final say in what gets published. For a taste of "coming attractions," the Fall 2012 issue of the *Journal* will explore "Information Warfare" and the Spring 2013 issue will follow up the theme of the Fall 2011 National Intelligence Symposium and highlight "Intelligence/Information Support to Small Unit Operations." We look forward to hearing from our readers and aspiring authors!

Bill Spracher

Operation Cardinal:
"...So You Must be a Spy"

by Bill Streifer

John W. Brunner was a member of the Office of Strategic Services (OSS) during World War II, in charge of the cryptography section of the Communications Center at OSS HQ in Kunming, China. The following is a brief history of the OSS:

> Early in World War II, President Roosevelt realized that the existing intelligence agencies were not providing him with the information he needed, so he asked World War I hero, prominent international lawyer and, incidentally, his Columbia University classmate William "Wild Bill" Donovan to go to Europe to find out what was happening there. Donovan's report was so impressive that Roosevelt asked him in 1941 to head an organization called the Office of the Coordinator of Information (COI). When the U.S. was drawn into the war, this organization was renamed the Office of Strategic Services (OSS) and given broad new powers and independence. The OSS not only provided most of the usable intelligence in all theaters of operations but also conducted propaganda operations and provided large scale support to resistance/guerrilla operations in all theaters.
>
> When the war ended, J. Edgar Hoover, who wanted to take control of all of the OSS international operations, asked President Truman to discontinue the OSS, which Truman ordered done. By mid-September, however, he realized that this would leave him without a reliable intelligence service, so on September 20, 1945 he ordered that the Research and Analysis and Photographic branches of OSS be transferred to the State Department, the guerrilla branches discontinued, the field intelligence operations transferred to the War Department and that the independent status of OSS be terminated as of October 1. The field intelligence operations assumed the name of Strategic Services Unit of the War Department (SSU). They quickly resumed responsibility for Research and Analysis as well. On October 1, the OSS effectively ceased to exist, but only on paper.
>
> The only thing that changed when OSS morphed into SSU was that guerrilla operations were no longer necessary. In a short time, the name changed again (in China) to External Survey Detachment of the Navy (ESD). On January 22, 1946 the SSU was renamed the Central Intelligence Group. By 1947, this had changed to the Central Intelligence Agency (CIA) in which final form it still exists and even resumes guerrilla operations when needed.
>
> John W. Brunner
> Former OSS

During World War II, President Truman was eager for the Soviet Union to end its neutrality in the war against Japan. Major General John R. Deane, who headed the U.S. military mission in Moscow, was certain that U.S. armed forces could not defeat the Japanese Kwantung Army in northern Korea and Manchuria "with anything like the facility with which the task could be accomplished by the Red Army already facing it." It therefore was "extremely important," Deane said, that "Russia be induced to accept this as her mission." Then, on August 8, 1945, at a hurriedly summoned news conference, the President made a brief, yet extremely important, announcement. With a broad grin, Truman said, "Russia has just declared war on Japan. That is all." The following day, he addressed the nation. "The military arrangements made at [the Potsdam Conference] were of course secret," the President said. "One of those secrets was revealed yesterday when the Soviet Union declared war on Japan."

According to London's *Sunday Observer*, the Soviet invasion of Manchuria and northern Korea was part of a five-point secret agreement between Roosevelt and Stalin prior to Yalta. Although the *New York Times* called the report "highly speculative," Secretary of State Byrnes later acknowledged that U.S. military leaders were aware of the agreement but secrecy was imposed for "sound reasons," saying its disclosure would "tip-off to Japan that the Soviet Union was planning to enter the war in the Pacific." The agreement called for Manchuria to become an independent republic temporarily within the Soviet zone of occupation. American military historians refer to the Soviet invasion of

OSS Map Reflecting the Soviet-U.S. Demarcation Line of Responsibility for Northern Korea and Manchuria.

Manchuria as "August Storm," while Russian historians simply call it the "Manchurian Strategic Offensive."

During the Potsdam Conference on July 26, 1945, U.S. and Soviet Chiefs of Staff met to discuss the line of demarcation between the American and Soviet zones of operation in Korea and in Manchuria, if and when the Soviet Union declared war on Japan. General Marshall, Soviet General Antonov, and Air Marshall Fallalev agreed upon a line which ran from Cape Boltina on Korea's northeastern coast, through a number of cities in China, and "thence along the southern boundary of Inner Mongolia." U.S. aviation would operate south of the line—including the cities of Mukden, Manchuria, and Konan, Korea—and Soviet aviation would operate north of the line. U.S. and Soviet commanders also agreed that the line applied both to reconnaissance as well as combat missions; that U.S. air operations north of this line and Soviet air operations south of this line must be coordinated; and that the line was subject to change. Since the United States had no intention of sending ground troops into China, only aviation and naval operations were discussed.

On August 9, the Soviet invasion of Manchuria and Korea began. The following day, Colonel Charles Bonesteel III and Colonel Dean Rusk drew a new line along Korea's 38th parallel "to halt the marching Russian army." And that same day, the U.S. Ambassador to the Soviet Union sent a telegram to President Truman and Secretary of State Byrnes which read, "Considering the way Stalin is behaving in increasing his demands on [T.V.] Soong [Chang Kai-shek's emissary to the United States]…I cannot see that we are under any obligation to the Soviets to respect any zone of Soviet military operation." General Deane concurred.

MUKDEN, MANCHURIA, AND KONAN, KOREA

In anticipation of a sudden collapse or Japanese surrender, General Marshall issued a basic outline plan, designated "BLACKLIST," which called for the "progressive and orderly" U.S. occupation of Japan and Korea as well as the "care and evacuation" of Allied POWs and civilian internees at the "earliest possible date." After Japan surrendered, General Albert Wedemeyer, the commander of U.S. forces in China, requested that the OSS organize POW rescue missions behind Japanese lines. The missions drew OSS personnel from Special Operations (SO) and Secret Intelligence (SI) with skills in clandestine operations, communications, medicine, and language training in Japanese, Chinese, and Russian. Each team was assigned an area, and each was named after a bird. Operation Cardinal's area of operations included the Hoten POW camp in Mukden, Manchuria, and two smaller camps where General Wainwright and Governor General Arthur E. Percival were being held prisoner by the Japanese. The Cardinal team was comprised of Major James T. Hennessy (Special Ops team leader), Major Robert F. Lamar (physician), Technician Edward A. Starz (radio operator), Staff Sergeant Harold "Hal" B. Leith (Russian and Chinese linguist), and Sergeant Fumio Kido (a *Nisei*—second-generation—Japanese interpreter). Cheng Shih-wu, a Chinese national, accompanied the OSS team as interpreter.

On August 16 at 4:30 in the afternoon, a B-24 with extra fuel tanks departed Hsian, China, for Mukden, the former capital of Manchuria. Six hours later, with Soviet troops 120 miles away and Japanese aircraft in the area, six men and 17 cargo parachutes were deployed along with 1,300

pounds of rations and a half ton of equipment: weapons, ammunition, two radios, and batteries. Despite a 20- mph wind, the decision was made to jump. "Our first priority was to rescue the POWs," Leith said. As the B-24 left the area, a *kamikaze* pilot headed his "Zero" straight for the aircraft. Fortunately, Lieutenant Paul Hallberg, the B-24 pilot, pulled back on the controls and the Zero passed underneath, avoiding a collision.

Hundreds of Chinese descended on the drop zone; one offered to lead four members of the Cardinal team down a dirt road toward the Hoten POW camp. After walking a half mile, they were confronted by a platoon of Japanese troops. When the Chinese guide saw the Japanese approaching, he ran away, and Major Hennessy waved a white handkerchief to signal their peaceful intentions. A Japanese sergeant ordered the team to "halt and squat down" while Japanese soldiers "aimed their rifles at us and clicked their bolts," Hennessy said. While in the squatting position, the team was ordered to throw their weapons on the ground while Hennessy attempted to explain that the war was over and they were only there to establish contact with the POWs. The Japanese sergeant, who remained "suspicious and unconvinced," responded that he had heard that the war with the United States was over, but that the Japanese were still fighting the Soviet Union.

The Japanese were officially notified of the armistice 45 minutes after the Cardinal team set foot in Mukden. It was only by "sheer tact and presence of mind," and utilizing the services of a Japanese interpreter, that Major Hennessy was able to convince the Japanese commander that the war was indeed over. The following morning, the Cardinal team was driven to Japanese secret police (*Kempeitai*) headquarters where they met a *Kempeitai* colonel who bowed deeply and informed the Americans that he was surrendering. With hand gestures, he declared his intention to commit *hara-kiri* in full view of the Cardinal team. They declined the offer.

Accompanied by an escort of Japanese soldiers, members of the Cardinal team were taken to the Hoten POW camp where 1,600 British, Australian, Dutch, and American prisoners—malnourished and emaciated—survived nearly 3½ years of internment. When it was discovered that General Wainwright was not among the prisoners, an attempt was made to contact OSS headquarters in China. When that failed, Major General George M. Parker, the highest-ranking American POW, and Colonel Matsuda, the commandant of the camp, informed the Cardinal team that General Wainwright and other high-ranking officers were in Sian, about 100 miles northwest of the Hoten POW Camp. The next morning, Leith and Lamar, accompanied by a Lieutenant Hijikata, a guard, and an interpreter boarded a train for Sian. After long delays and a change of trains, they arrived at the camp at 3:00 the following morning.

After a brief rest, the OSS team met Generals King and Moore, Governor Tjarda Von Starkenbergh, General Wainwright, and Arthur E. Percival, Governor General during the fall of Singapore, a defeat which Churchill described as the "biggest humiliation in British military history." Leith recalls that Wainwright looked thin and his hearing was failing. "He had experienced a brutal captivity," Leith later wrote. General MacArthur described seeing Wainwright for the first time:

> I rose and started for the lobby, but before I could reach it, the door swung open and there was Wainwright. He was haggard and aged… He walked with difficulty and with the help of a cane. His eyes were sunken and there were pits in his cheeks. His hair was snow white and his skin looked like old shoe leather. He made a brave effort to smile as I took him in my arms, but his voice wouldn't come. For three years he had imagined himself in disgrace for having surrendered Corregidor. He believed he would never again be given an active command. This shocked me. "Why, Jim," I said, "your old corps is yours when you want it."

General MacArthur Embracing General Wainwright upon the Latter's Liberation from Japanese POW Camp.

When the Soviet Army began occupying Mukden on or about August 21, it issued passes to the Cardinal team which allowed the members to move freely about. However, since vehicles were in short supply, none was supplied to the Americans. That evening, a Soviet Army mission of four officers and an interpreter arrived at Hoten. They took control of the camp from the Japanese and announced that the POWs were liberated. The prisoners, now armed with Japanese weapons, patrolled the camp. According to Colonel Victor Gavrilov, Institute of War History at the Russian Defense Ministry, the POWs had been "starved and tortured by the Japanese guards; they could have hardly made good warriors."

After a brevet promotion to Major, Leith accompanied Wainwright and the other VIPs to PeiLing airport, north of the city, where a C-47 and a B-24 awaited their arrival. Days later, the 19-man POW Recovery Team No. 1, under the command of Lieutenant Colonel James F. Donovan, arrived in Mukden to "reinforce and assist" the initial OSS contact team. After the Cardinal team was relieved, Hal Leith, who spoke Russian and Chinese fluently, remained behind to "keep an eye on the Russians and the Communist Chinese 8th Route Army." However, the problem of repatriating the officers and men from the Hoten POW camp remained.

"Without informing the Soviet side," Gavrilov said, "the U.S. command started sending one plane after another to Mukden in order to transfer its men, and supply them with essentials." At first, the Soviet command detained the crews of these planes to "clarify the situation." Later, however, the headquarters of the Baikal Front ordered its forces to assist U.S. aviation in the delivery of goods to the POWs at Hoten.

Between August 27 and September 20, over 1,000 B-29s began flying POW supply missions to 157 camps throughout the Far East. Each aircraft carried 10,000 pounds of much-needed food and medical supplies. However, the planned altitude of 500 to 1,000 feet for parachute drops proved too low for efficient operation of the cargo parachutes, and reports began to pour in of barrels plummeting to earth, resulting in damage, injury, and, in some instances, the death of civilians and military personnel. As Leith noted in his diary, "The B-29 air drops have improved the food situation 200%. I am really glad." Meanwhile, OSS headquarters received a message from the Cardinal team which read, "Unless dropping can be improved, recommend it cease as it has done more harm than good."

In northern Korea on August 29, an aberrant parachute drop nearly caused an international incident when parachutes failed to open properly and a barrel crashed to the ground nearly injuring a Soviet colonel. Later that afternoon, when another B-29, called the "Hog Wild," appeared over the Konan POW Camp and refused to obey instructions by Soviet fighter pilots to land immediately, Soviet Major Savchenko, the commander of the 14th Fighter Bomber Regiment, convened a "war council" to determine how best to respond. According to Savchenko's vice commander, Ivan Tsapov, "Being in charge of the zone, we demanded that our rules be obeyed. Even Russian transport and bomber plane pilots kept order. They gave notice on flights in our zone a day earlier. Americans did not want to do so." When Lieutenant Joseph Queen, the B-29's airplane commander, continued to ignore demands to land and instead flew out to sea, Yak fighters fired on the American bomber, causing one of the B-29's four engines to burst into flames. Queen then crash-landed his B-29 on a Soviet airdrome after six members of the crew parachuted into the cold and turbulent Sea of Japan. As the B-29 came to a stop, the crew jumped to safety while Russians threw dirt on the engine to extinguish the fire. Staff Sergeant Arthur Strilky, the Hog Wild's radio operator, later stated, "The chances of living through that crash are so remote that I still feel that Joe saved all of us."

When General MacArthur learned of the incident, he fired off an angry cable to General Antonov, Chief of General Staff, Soviet Armed Forces, and a member of the Soviet Supreme High Command, which read, "The American plane was plainly marked and its mission could not fail to have been identified as purely benevolent." In response, Antonov sent a cable to MacArthur which read, "I feel, Dear General, that you will agree that in the action of the Soviet fliers in this incident, there were manifested only measures of self-defense against an unknown plane, and that there were no other intended acts." Later, the Soviet front received an order from Antonov to arrange transportation of the prisoners from Mukden to Dalian by rail instead of by air. "Apparently, this was done to rule out unauthorized landings," Gavrilov said, and to prevent another "willful act," like that which the commander of the Hog Wild had committed. "Besides, by rail was also safer." And on September 10, 750 Mukden POWs left by train for Dalian; the remaining prisoners departed the following day. Victor Gavrilov credits Soviet forces with the release of the POWs at Mukden. Hal Leith, a member of Operation Cardinal, credits the OSS.

"The camp is deserted," Leith said, and Operation Cardinal's primary mission was accomplished. Camp Hoten once again assumed its role as a prison, this time for 5,000 Japanese soldiers who had been captured by the Russians. Cardinal turned out to be the "most challenging and difficult" of the OSS "mercy missions" due to "the large number of POWs to contend with" and the distance from home base. Although some OSS team members

survived the encounter "relatively unscathed," others were forced to suffer various forms of indignity including being stripped naked and having their faces slapped by the Japanese. Later, increased Soviet hostilities prompted Donovan to request that American personnel withdraw from the area immediately. On October 5, Major-General Kovtun Stankevich, garrison commander of Soviet forces in northern Manchuria, accused Leith of spying. "You are fluent in Russian but you don't have a Russian name so you must be a spy," Stankevich said. Leith and the others were offered two choices: "Leave immediately or get a free trip to Siberia."

OSS Officer Hal Leith Flanked by Soviet Counterparts.

After denying the accusation "to no avail," Leith's party, along with Charles Renner, the French Consul General and his family, departed Mukden for Beijing on a C-46 transport plane the following day. "At the airport, we put sugar in the tank of our jeep," Leith said. "We didn't want to leave anything useful for the Russians, any more than we already had." Months later, after Soviet forces left Manchuria, Leith returned to Mukden.

[Editor's Note: The above article was based in part on an earlier article, cited below, which appeared in the Summer/ Fall 2010 issue of *The OSS Society Journal*. Permission was obtained by the author.]

Notes:

"Operation Cardinal: '… So You Must be a Spy'" is based on conversations with Ivan Tsapov, Arthur Strilky, Hal Leith, and John W. Brunner, plus information from the following sources:

Foreign Relations of the United States (FRUS), U.S. State Department, diplomatic papers, Potsdam Conference, July 26, 1945.
University of Wisconsin Digital Collections.
BLACKLIST, third edition, August 8, 1945.
Cables between General Douglas MacArthur and Army General A.E. Antonov.

Newspaper Articles:

Calgary Herald (AP), "Washington Sees Early End to War in the Pacific," August 8, 1945, p. 1.
New York Times, "The American Mood on the Eve of Victory," August 13, 1945, p. 18.
Schenectady Gazette (AP), "Secret Agreement on Russian Claim to Kuriles Known to Military Leaders," January 29, 1946, p. 1.

Journal Articles:

Clemens, Peter. "Operation Cardinal: The OSS in Manchuria, August 1945," *Intelligence and National Security*, 13, no. 4, 1998, pp. 71-106.
Gavrilov, Viktor. "Saving General Wainwright," *Ria Novosti*, May 9, 2005
http://en.rian.ru/analysis/20050905/41306298.html.
Streifer, Bill. "OSS in Manchuria: Operation Cardinal," *The OSS Society Journal*, Summer/Fall 2010, pp. 22-25.

Books:

Deane, John R. *A Strange Alliance*. Bloomington: Indiana University Press, 1973.
Leith, Harold. *POWs of Japanese Rescued*. Victoria, BC, Canada: Trafford, 2003.
MacArthur, Douglas. *Reminiscences*. New York: McGraw-Hill Book Co., 1964.
Tsapov, Ivan. *Life in the Sky and on the Land. Moscow:* Delta NB, 2004 (in Russian).
Yu, Maochun. *OSS in China: Prelude to Cold War*. New Haven, CT: Yale University Press, 1996.

Bill Streifer, BA, MBA, is the author of fiction and non-fiction on military and intelligence topics during World War II and the Cold War. His current book project, The Flight of the Hog Wild*, by Bill Streifer and Irek Sabitov with an introduction by Dr. Benjamin C. Garrett, Senior Scientist at the FBI's forensic WMD laboratory, concerns a possible intelligence/aerial reconnaissance mission over Soviet-held northern Korea. On August 29, 1945, an American B-29 Superfortress on a POW supply mission was shot down by Soviet fighters, an incident which some believe may have been the first military encounter of the Cold War.*