From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 22 • NUMBER 1 • $15 SINGLE COPY PRICE Spring 2016 ©2016, AFIO

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
Web: **www.afio.com**, E-mail: **afio@afio.com**

GUIDE TO THE STUDY OF INTELLIGENCE

Educating the Next Generation of Intelligence Professionals

by Jan P. Herring

Introduction: The Educational Challenge

The "future" that intelligence professionals will have to understand and work in will differ significantly from that of today. Educating and preparing students for that challenge requires intelligence educators both to be aware of how that future is likely to evolve and to begin developing new educational material and methods today.

The intelligence environment of 2020 and beyond will be shaped by many of the same issues we face today, i.e., geo-political differences, increasingly sophisticated military technology and weapons, international trade and monetary issues, a growing concern for the protection of critical infrastructure, and terrorism in all its multi-faceted forms; and, a host of new and emerging national policy issues that heretofore have mainly been the concern of the private sector, i.e., intellectual property (IP) protection, supply chain integrity, public health, and climate change. Preparing intelligence students to cope with both types of issues in an insightful and professional manner is a part of the challenge. Preparing them to work in either or both private-sector intelligence and government organizations is a new and emerging challenge for most educational institutions. We are probably better prepared to handle the former, but have much work to do to prepare today's students for intelligence work in the private-sector or to address private-sector issues within government intelligence organizations.

It is the private-sector challenge that we need to highlight. For the most part, both government and academic educational entities are well positioned to begin preparing government intelligence personnel for policy-related issues stemming from the private sector. Identifying the appropriate subject matter experts and bringing them into the current government and academic educational systems seems a rather straightforward approach to this challenge. And, possibly, enhancing such educational efforts through the assignment of government intelligence personnel in private-sector exchanges or hiring experienced business intelligence personnel for specific government intelligence work.

The private-sector intelligence situation is not so tractable. With the exception of a few universities and private-sector educational academies specializing in intelligence training, there is no formal or organized educational system producing intelligence professionals for the business community. As a result, both the quality and quantity of well-trained business intelligence professionals is woefully inadequate. For the most part, corporations either pay to have their employees trained for intelligence work or they are left to learn the "trade" on their own.

Some private-sector entities have hired former government intelligence officers for certain specialized needs such as communications security and counterintelligence work. But few government intelligence analysts or field collectors have been successful in finding equivalent jobs in the private sector. Their subject-matter expertise and associated skill sets are just not a good match for most business intelligence assignments. The few that have made a successful transition have either gone back to school to acquire appropriate business knowledge and occupational skills, or gone through some industry specific and/or business intelligence training. However, such occupational training is not easy to find and provides no guarantee of employment. Furthermore, most universities and other types of higher education have not seen this area of professional development as a part of their institutional responsibilities.

There is one additional problem that further complicates this educational challenge. The two intelligence "communities," public and private sector, currently have no formal way of communicating or working with each other on problems or issues of common concern. This is particularly true of contemporary issues such as cyber security or global supply

chain protection. And while private-sector intelligence training is available to government employees, the reverse is not true. However, both communities are welcomed to participate in academically based education and training. So if universities and accredited private-sector training organizations were to develop appropriate "next generation" intelligence courses and materials, they could be the logical provider of such education services for both future public and private-sector intelligence professionals.

Two major forces-of-change appear to be shaping the future intelligence environment that both public and private sector intelligence professionals will be confronted with, and equally important, will be working in. The better we understand both, the better we as educators will be able to prepare today's students for their future assignments.

The Privatization of Intelligence

First is an on-going trend, known as the Privatization of Intelligence. The concept of "privatizing intelligence" was defined by two former OSS officers and friends, Bill Colby and Stevan Dedijer.[1] Colby, a long-time CIA officer and one time Director of the CIA, and Dedijer, a Yugoslav that volunteered to serve in the US military during WWII, subsequently becoming a university educator and the "godfather" of today's business intelligence discipline, were directly involved in the movement of professional intelligence operations from government auspices to private-sector entities such as corporations and financial institutions. This public to private sector migration during the 1970s and '80s, resembled that taking place in several countries where governments were divesting themselves of government-owned transportation, mining and other business enterprises. This governmental action was called "privatization." Thus, the creation and operation of organized intelligence functions by private sector entities was labeled the Privatization of Intelligence.

It began in the 1970s as business competition became more heated and international. Several multinational corporations and their leaders recognized that they – like governments – would need formal, organized intelligence programs to compete successfully...and possibly survive. In that vanguard were firms such as Motorola, Kodak, IBM, and corporate leaders in the chemical, communications, and pharmaceutical sectors.[2]

By the mid-1980s, the international business intelligence (BI) profession had grown to the size that it spawned its own professional society, i.e. the Society of Competitive Intelligence Professionals (SCIP, which was renamed Strategic and Competitive Intelligence Professionals).[3] Today, SCIP has members and chapters in some 50 countries. Its membership has varied over the years, from about 7,000 in the 1990s to around 3,000 today. An estimate of the total number of BI practitioners worldwide would probably be 10 to 100 times that number, which would include part-time as well as full-time employees. Furthermore, it has been estimated that up to 85% of all multinational corporations have some form of business or competitive intelligence function.[4] This growth in private-sector intelligence operations is worldwide. In some countries, their governments have encouraged and assisted them, China and France being prime examples. In most, however, it has been a business-driven phenomenon.

The Merger of Private and Public Concerns

The second major force shaping the future of intelligence are governments worldwide focusing more on business or private-sector issues such as supply chain security, IP protection, and even climate change. Although this trend is rather late to the scene, it is clearly moving national intelligence communities into areas and disciplines that require government intelligence professionals to understand more about private-sector organizations and their operations. For the most part, government intelligence education and training has not yet begun to address these types of private-sector issues. And, except for a few universities, such as Mercyhurst, most academic educational institutions are not yet aware of these new government intelligence initiatives – and even fewer are currently capable of addressing them.

These two major forces-of-change will cause government intelligence professionals and private-sector intelligence practitioners to increasingly focus on

1. See Jon Sigurdson and Yael Tâgerud (eds.). *The Intelligent Corporation-The Privatization of Intelligence* (Taylor Graham, 1992).

2. See Jenny Fisher, "Competitive Intelligence: A Case Study of Motorola's Corporate Competitive Intelligence Group, 1983-2009" in the *Guide to the Study of Intelligence*, *http://www.afio.com/publications/FISHER_BusIntel_CaseStudy_Motorola_FINAL_2014July14.pdf*. See also John J. McGonagle's article, "Competitive Intelligence" in the *Guide* at *http://www.afio.com/publications/MCGONAGLE%20Competitive%20Intel%202014Aug27%20DRAFT.pdf*.

3. www.scip.org.

4. Jan Herring, "Create an Intelligence Programs for Current and Future Business Needs," *Competitive Intelligence Magazine* 8 (5), September-October 2005.

similar issues and challenges. Both will use the same "open sources" of intelligence (OSINT) for collection and similar analytical methodologies – but will produce results for different types of customers with their specific public or private sector applications. Consequently, this future "intelligence world" will be both similar and different with new and unexpected intelligence challenges – of a different and increasingly complex nature. And, most likely, we will see an entirely new and disparate "Intelligence Community" – one including both government and business intelligence professionals.

What about this new "evolving" public/private-sector "Intelligence Community?" *It is unlikely to be* a formally combined public-private intelligence organization – for the most part, each sector will continue to operate separately, responding to its own priorities.

Both communities will work increasingly on similar problems, e.g., threats to company's IP and supply chains, cyber and financial security issues, threats to public health, including pharmaceutical production and supply chain integrity, and given the government's growing concerns about its security, the national infrastructure – which, for the most part, is owned by the private sector. These are just a few of the types of new security issues finding their way into national intelligence requirements in the US and worldwide.

Furthermore, as it becomes more and more evident that a country's national security in today's global marketplace is a combination of its military security and its economic well-being, the two intelligence communities' responsibilities will begin to converge. How and when is unsure. But they will – possibly sooner than expected. It would be in the best interest of all for the two communities to work together on some aspects of these intelligence topics.

For intelligence professionals, it behooves us to begin thinking more constructively about that future intelligence environment. For educators, it is not too soon to begin considering how we will train future intelligence officers to work in that new intelligence world with overlapping concerns and interdependent responsibilities.

"That Future" Intelligence Environment

Let me describe a possible scenario for "That Future" intelligence environment, at least one that seems reasonable for planning purposes in the near term:

- For the most part, governments will still view the world as made up of major geo-political blocs – North and South America; Europe, both separately and the EU; Russia, old and new; the Middle East – both friendly and threatening; Southeast Asia, Northeast Asia, and China; and, a new and challenging Africa. Military and political affairs will continue to dominate their concerns – though energy and monetary issues will not be far behind. Global trade and commercial competition will become a national priority. International terrorism will continue to be a major national security concern – both domestically and abroad.
- The business world will increasingly be made up of "true" multi-national corporations (MNC's) including state-owned-enterprises (SOE's) … all competing on a global basis … with growing levels of government involvement and BI assistance. Such companies realize that to be successful, they will have to better understand the geo-political world they operate in … and cope with the regional as well as global competitors they face in each chosen market … which in some cases, includes the local governments. They will need better BI and security capabilities than most currently possess if they are to survive and succeed.
- Both private sector and government entities will have growing interests in both geo-political and geo-economic affairs. MNC concerns about government activities affecting trade and monetary affairs have grown with their global operations – and will continue to do so. Joint interests in the new and emerging intelligence topics of cyber security, IP threats, and supply chain viability will grow internationally. And both communities will share a mutual concern for the threats posed by international terrorism … and climate change related disasters and implications.

Preparing intelligence professionals for such a future world – with better skills, greater real world experience, and the ability to work together in public-private partnerships will be the challenge for both government and private-sector intelligence educators.

Preparing Professionals for "That Future"

What types of intelligence professionals will be needed to address this future intelligence world … and what training they will need?

- **Analysts** – Both communities will require analysts. But each with new and different types of skills. Government analysts with business skills, enhanced by real world experience ... and, BI analysts with a greater understanding of international and geo-political affairs.
- **Open Source Intelligence (OSINT) and Information Services Professionals.** These are the new types of modern day librarians that are necessary to fully exploit the growing number of international databases and syndicated information services. These professionals are a combination of library science and information services experts. Some of the best have come from the ranks of the Special Library Association (SLA) membership. But they too require "intelligence" training before they can become BI practitioners.
- **Knowledge Technologists.** Peter Drucker's "blue collar" workers of the knowledge-worker age. The tech-savvy, computer science experts that both Intelligence Communities will need to fully exploit the internet world and apply all the advanced collection and analytical software that will be available. They will be needed for both intelligence production and counterintelligence purposes. Cyber security will be one of their specialties.
- **Human Source Intelligence (HUMINT) Collectors.** This profession will continue to play its critical role in government intelligence operations – and, will increase in importance in business intelligence, where it has played only a limited role up to now.[5] The private sector needs to increase substantially its professional development in the HUMINT collection field.
- **Counterintelligence Professionals.** This group of intelligence officers will play an increasingly important role in both the government and business worlds. As a country's national security becomes more dependent upon its economic well-being, the protection of both industrial and financial resources from foreign government intelligence and criminal threats will become national intelligence priorities. Government counterintelligence officers are better prepared for this new challenge, but will need education about the private sector's current capabilities and limitations to better assist corporations protect their IP including trade secrets. And, although business professionals are fairly good at traditional security and patent protection tasks, few have the counterintelligence training necessary to protect their IP and key personnel from sophisticated hackers or hostile intelligence services.
- **Intelligence Managers.** Management training for intelligence professionals is an area that has largely been overlooked. Promotion to management in government primarily has been governed by the "Peter Principle" – promoted to your level of incompetence. There have been some leadership courses and senior-level seminars provided as one rose in rank, and possibly an academic sabbatical. Recently, both government and one or two academic institutions have begun to address this shortcoming; however, much more is needed. The University of Maryland University College (UMUC) is the only institution to offer a graduate degree in intelligence management.[6] The BI community has very little to offer as far as formal intelligence management training. Corporations would benefit greatly from such education.
- **The Intelligence Customers.** Lastly, the users of intelligence – both government officials and business executives – need formal intelligence education, basically "what it is – and how to use it." The private sector probably needs it more because there are fewer good role models or experienced users around to learn from. For the business community, it is pretty much what they can learn from spy novels and movies. Intelligence is not taught as a management discipline in any of the leading business schools.

The education and training of these intelligence professionals – both business and government – will be a challenge. Preparing them for "that future" world described, along with our current, traditional educational offerings, will require thinking more creatively, new materials, and innovative methods to educate:

- *Government intelligence officers* how to address those new and emerging policy subjects stemming from private-sector activities;
- *Business intelligence professionals* how to handle both the geopolitical challenges confronting MNC's and the threats posed by foreign intelligence services; and,
- *Both communities, jointly* how to deal more effectively with intelligence issues affecting both our economic and national security.

It is not too early to start thinking and preparing for this challenging educational task.

5. A CI Foundation survey in 2006 revealed that less than 3% of BI professionals work in this field full time. "State of the Art: Competitive Intelligence," A Competitive Intelligence Foundation Research Report 2005-2006.

6. *http://www.umuc.edu/academic-programs/masters-degrees/management-with-intelligence-management-specialization.cfm*.

Jan P. Herring, a well-recognized expert in the business intelligence field, is a charter member of the Society of Competitive Intelligence Professionals, a SCIP Fellow, and 1993 recipient of the Society's Meritorious Award. His professional experience includes developing Motorola's highly acclaimed intelligence program, co-founding the Academy of Competitive Intelligence, and setting up the US Government's first business intelligence program. Before his BI career, Mr. Herring served 20 years with the CIA as an analyst, field collector, and a manager. His assignments covered a wide range of intelligence activities, including: weapons systems and threat analysis for the national reconnaissance program; managing the IC's National Technical Assessment program for the Defense Department; and leading IC efforts in a wide variety of international affairs, including strategic arms limitation negotiations; export control implementation; and the opening of US-China trade relations. During his government career, he served as chairman of the Director of Central Intelligence's Scientific & Technical Intelligence Committee and as the first chairman of the Inter-Agency Technology Transfer Intelligence Committee. Mr. Herring's last government assignment was as the first national intelligence officer (NIO) for science & technology. Upon leaving CIA, he was awarded the Agency's highest honor, the Medal of Distinction, and received letters of commendation from President Ronald Reagan, Attorney General William F. Smith, and FBI Director William H. Webster, for his contributions to national security and federal law enforcement. He is the author of numerous articles and several book chapters on intelligence in the private-sector and co-edited a two-volume series entitled *The Art and Science of Business Intelligence Analysis* (Greenwich, CT: JAI Press, 1996.) Mr. Herring has a bachelor's degree in physics from the University of Missouri.

This article was based on a keynote presentation given by the author at the 10th annual conference of the International Association for Intelligence Education (IAFIE) at Mercyhurst University in Erie, Pennsylvania, July 14, 2014.

"Am I surrounded by dolts?
Why have I never been told
that we have no spies in England?"

— Kaiser Wilhelm on learning
that his First Army was surprised
by British troops at Mons, August 1914

"If you do not think about the
future, you cannot have one."

— John Galsworthy, English novelist and
Nobel Prize winner, *Swan Song* (1928).