From AFIO's *Intelligencer* Journal, Vol. 21, No. 3, Fall/Winter 2015. www.afio.com ©2015

The Changing Shape of HUMINT

by John Sano

Although often described as the world's second oldest profession, spying – and specifically human intelligence (HUMINT) – continues to evolve. While the basic tenets of human espionage remain constant, there are a variety of factors, which over time have impacted both the tenets and the parameters of spying. It is not just the "how" of HUMINT, but also the motivations and the methodologies employed. Demographics, technology and cultural expectations all play a role in the shaping of a clandestine service officer.

Demographics

The majority of officers serving today in America's Intelligence Community (IC), be it the National Clandestine Service (NCS) of the Central Intelligence Agency (CIA), or in any of the other 16 organizations that comprises our IC, have joined post- 9/11. Despite the attendant controversies that have plagued the IC over the years prior to, and especially after, the traumatic events of September 11, 2001, today's IC member remains highly motivated, patriotic and professional. One significant difference, however, is their "career expectancy." Officers in the Clandestine Service, in years past, often joined with the general expectation that they would serve 20 or more years. This was reflective of the general trend at the time – and not just in the intelligence world – of the "cradle to grave" syndrome, where an employee could expect to spend an entire career in one company or organization. Today's employees – be it in the public or private sector –expect to have several careers over the course of their employable lifespan. Some perhaps view a stint in the Intelligence Community as a stepping-stone to something else, others perhaps as a culmination of a career progression; although given the age restrictions for entry into the IC, this is less likely. This presents a challenge to management as how to utilize their talents – for whatever period of time they serve.

As former National Security Agency (NSA) and CIA director General Michael Hayden, USAF (Ret.), when asked about attrition and the retention of highly trained officers, remarked "... managers need to motivate their workforce as best as possible, keep them challenged, but don't hide from them the pros and cons of working in the Intelligence Community and above all, when they do leave, make sure they leave with your best wishes. They may come back, and/or recommend the organization to others."[1]

Managing this younger, more technically astute, workforce can be problematic for a number of reasons – not the least of which is the dramatic generational difference when it comes to learning. Today's workforce thinks and processes information significantly differently from its predecessors. As Dr. Bruce Perry of Baylor College of Medicine has stated, "Different kinds of experiences lead to different brain structures."[2] As such, today's workforce receives information much faster than their predecessors. And while reception does not always equal comprehension, it does present an issue for managers as well as for IC instructors. Education within the world of HUMINT is in large measure "anecdotally based," with instruction incorporating legacy-based scenarios, or "tribal memories" to emphasize key points. While useful, it is often a technique that many younger practitioners of espionage find unfamiliar, even ineffective.

Growing up on a regular diet of technology-driven information, today's clandestine officer is better connected and more adept at multi-tasking and networking than previous generations. Adjusting to this significant divide is often difficult, for most instructors view education in much the same way as they themselves were taught – via lectures, step-by-step logic and "tell-test" instruction. Today's officers are more comfortable with procedures that they grew up with – TV, Internet, video cams, cell phones and all the other accoutrements associated with the digital age.

What does this mean? Aside from the way today's officers want to learn, it also impacts expectations. Today's clandestine service officer expects to access any information, anytime, anywhere, and on any device. Aside from the obvious security aspects, there

[1] Private conversation between the author and Gen. Michael Hayden in July 1999, reprinted with the General's permission.

[2] Bruce Perry. *The Memories of States: How the Brain Stores and Retrieves Traumatic Experience*, Baylor College Press, July 1997.

is also the problem of managing these expectations – attempting to inculcate the proper balance of security vs. expediency, not to mention patience within an increasingly impatient workforce – is no easy task, but nonetheless a critical aspect of any clandestine activity.

In essence, this "digital divide" differentiates the current generation of officers from their predecessors, the former being "digital natives," while the latter are relegated to the status of "digital immigrants." This is not merely a semantic distinction – today's college graduate has spent more time watching TV and in front of a computer screen than reading books or attending lectures. As such, the thinking patterns they use to learn are markedly different from those of their predecessors. They learn, *inter alia*, via networking, random access (e.g. hypertext), and preferring video game scenarios to regimented lectures, and all forms of social media (e.g., blogs) over repetitive and often outdated texts.

This digital divide extends to HUMINT operations in terms of both the officers engaged and their targets. If, for the sake of argument, we restrict our discussion to traditional espionage — i.e., the spotting, assessing, developing and eventual recruiting of human targets – then targets and targeteers (i.e., the HUMINT operations officer) can often be at variance. Avenues of approach can prove problematic. If the target is, like the targeteer, a digital native, then access and eventual development is often symbiotic. If, however, the target is a digital immigrant the differences can create difficulties; not insurmountable, but which have to be addressed as part of the recruitment cycle.

HUMINT Defined

Human Intelligence encapsulates a wide range of skills – from traditional diplomatic dialogue, to manipulation, to deceit. At its core is the ability to recruit an individual to conduct espionage, to "spy." Ancillary skill sets include counterintelligence, surveillance, liaison exploitation, the use of "cover" – either commercial, or more likely official – and false flag operations (the ability to pose as a representative of a country other than the United States).

The acquisition of an individual(s) to spy at our behest is commonly referred to as the **recruitment cycle**, which includes – in sequential order:

- **Spot** - the ability to identify an individual who has access to information that we want;
- **Assess** – identifying the individual's vulnerabilities and determining whether he/she may be susceptible to a recruitment "pitch;"
- **Develop** – manipulating the individual's vulnerabilities with the intent of making them more amenable to agreeing to your proposal, which is defined as the
- **Recruitment** – the formality of securing an individual's cooperation to steal secrets.

HUMINT complements, and can be bolstered by, other "INTs" – predominantly Signals Intelligence (SIGINT), Geographical-Spatial Intelligence (GEOINT), Measurement and Signature Intelligence (MASINT), and increasingly Open Source Intelligence (OSINT) – a fairly recent development as an INT – but one which generates a near overwhelming amount of information that can be used for myriad intelligence efforts. As but one example, the bulk of SIGINT operations are often HUMINT enabled, i.e., a human source initiates the penetration of a system, either through the provision of technical information then further exploited by NSA, or via the introduction of technical devices (switches, or other electronic mechanisms) into foreign databases or electronic infrastructures.

As the country's national HUMINT manager – the CIA, and specifically the National Clandestine Service, also engages in cooperative relationships with other intelligence as well as law enforcement entities – both domestic and especially foreign intelligence and security organizations. The CIA, by statute, is also tasked with undertaking covert action (CA) which is "…an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that **the role of the United States Government will not be apparent or acknowledged publicly…**" All CA activity is conducted by HUMINT operatives.

Technology

Today's clandestine service officers have grown up in a world of digital expediency, if not dependency, and while schooled in the nuances of conducting traditional espionage, rely increasingly on technical assistance in the application of their tradecraft. This is a good thing, as technology has increased efficiency and in many instances shortened timelines. Yet with improvements in efficiency and speed comes vulnerabilities as well – vulnerabilities that often cannot be foreseen readily or assessed accurately.

The digital revolution has made our day-to-day lives easier, albeit for digital immigrants perhaps a bit more confusing and frustrating at times. What is equally true is that with these efficiencies have come additional responsibilities and risks for the tradecraft of espionage. Learning about potential targets or adversaries and crafting an approach via technical means – whether it is via e-mail or a social blog, or through more elaborate and esoteric mechanisms such as avatars, or similar methods – might well be expeditious, but highly insecure. Further, communicating via these mechanisms further complicates matters for the same security issues. While the longstanding (and clearly "digital immigrant") modus operandi of "chance encounters," cryptic telephonic codes, and clandestine meetings in a safehouse or rolling car may appear antiquated, they have proven generally more reliable from a security perspective, but certainly more time consuming. This is not to say that technology does not play an important role in approaches and maintaining contact with an agent, but only when used in – for lack of a better term – "moderation." Too often espionage operations are over-reliant on the "ease" of utilizing technical means to communicate, which is vulnerable to hostile counterintelligence activities.

Aside from the security issues attendant in the over-reliance on technology, there are also the cultural changes that have accrued over time. In the not-so-distant past, communicating with headquarters was not nearly as quick as today's near-instantaneous speeds nor offering as many alternatives. In today's world, the previous time lag in Headquarters' responses to the field have diminished from days, to hours or minutes. While coordination has become more efficient and timely, it has resulted in the transfer of greater decision-making responsibility to headquarters, vice the field. Given the dearth of experience of many field operatives – a byproduct of the 1990s "peace dividend,"[3] and while not risk averse, it has promoted a penchant to defer operational decisions to managers who are perceived as having more experience.

Cultural Expectations

During the Cold War intelligence targets were clearly defined – the Soviet Union being the primary (if not almost exclusive) focus. In today's post-9/11 environment the targets are more diverse and elusive. Non-state terrorist targets pose unique and unprecedented challenges. While today's operations officers face many of the same ethical and moral challenges their predecessors did when working against more traditional targets, the continuing political controversies over whether US (specifically CIA and military) actions during the continuing war on terrorism have further complicated the situation. Whether combating terrorism on legal and moral grounds was and is justified calls into question whether such activities warrant continuing in any form. Espionage has always faced moral quandaries, yet in years past HUMINT operations were often rationalized in terms of the "end justifying the means." In most cases this was the containment, if not disruption of the aggressive Russian intelligence services, the KGB (now the SVR) and GRU.[4] While one could make the same case for the terrorist target, the fundamental difference between these targets (e.g. KGB vs. Al-Qaeda, or other affiliated groups) is that the former was politically based while the latter is more religiously focused. Today's operations officers may be less inclined to adopt an "end justifies the means" mentality than their predecessors.

The Future

The Intelligence Community will continue to undergo change, influenced as much by domestic politics as developments beyond our borders. Despite technological advances, HUMINT will continue to occupy a critical role in providing intelligence to U.S. policymakers. Discerning plans and intentions can only come from the recruitment of human sources. Even information stored digitally often requires human access; and even with data that is extracted electronically, there is still the requirement to interpret those documents and how they fit into the larger context. Human beings are essential to all processes and operations – whether they are public or private based. As such they are the first and last line of security. They are also the first and last entry points into the intelligence arena.

As we continue to advance technologically, in essence making our world smaller, the potential threats posed by these advancements will make both protecting and exploiting real secrets exponentially more difficult. In addition, as these challenges continue to grow, those tasked with addressing them will need to adjust at a much more rapid rate. This applies both to field operatives as well as to their managers.

[3] Through budget cuts, Congress severely restricted hiring of Intelligence Community personnel during much of the 1990s. The political rationale was that the US should enjoy a "peace dividend" from the dissolution of the Soviet Union, the newly independent Eastern European nations, and the end of the Cold War. The consequence was that few were hired during this period resulting in a paucity of experienced middle managers over the ensuing two decades.

[4] For a brief history of Soviet/Russian intelligence services see Robert W. Pringle, "Guide to Soviet and Russian Intelligence Services," The Intelligencer, Vol. 18, No. 2, Winter/Spring 2011.

As described above, the differences in experience and cultural expectations will continue to exacerbate the relationship, but only temporarily as the "old guard," or "digital immigrants" gradually gives way to the "new guard," or "digital natives." Traditional approaches to espionage – while forming the bedrock for HUMINT – will have to be further augmented. The next generation of operatives and their managers will need to be more familiar with, if not adept at, technological augmentation. Augmentation, not replacement. While the tendency to rely increasingly on technology to make HUMINT collection more efficient is commendable, adherence to the core principals will ensure that human operations remain as secure as possible.

Constrained budgets, while often cyclical in nature, will likely remain flat, if not decreased, over the next several years or longer. The Intelligence Community, for many years immune to the exigencies of financial debate within Congress – particularly during times of crises – is no longer exempt. While the old adage, "there will always be money for good operations" will remain fairly constant, what constitutes "good operations" may likely shift – dependent upon the prevailing political winds and the prioritization of competing requirements (both operational and structural/administrative). In addition, hiring and promotions within the IC are contingent to a significant degree on the availability of funds. While both will continue – hiring dependent on attrition rates and promotions on performance metrics – the availability of both will be diminished.

The impact on the future generation of officers cannot be underestimated. With a workforce that can be expected to remain, on average 7 years, any limitations on advancement could have a deleterious effect on morale as well as retention. Today's IC officers are however, exceptionally adaptive, and resilient. Though they may stay for a shorter period of time than their predecessors, their accomplishments and dedication to the mission are of equal measure and will serve the Intelligence Community well in the years ahead.

Readings for Instructors

Mark Lowenthal. *Intelligence. From Secrets to Policy*, 4th edition. Washington, DC: CQ Press, 2009.

Jennifer Sims and Burton Gerber. *Transforming U.S. Intelligence*, Washington, DC: Georgetown University Press, 2005.

Loch Johnson. *National Security Intelligence*. Cambridge, UK: Polity Press, 2012.

Jeffrey Richelson. *The U.S. Intelligence Community*, 5th edition. Boulder, CO: Westview Press, 2008.

James Olson. *Fair Play*. Sterling, VA: Potomac Books, 2006.

Allen Dulles. *The Craft of Intelligence*. Guilford, CT: The Lyons Press, 2006

Loch Johnson. *Secret Agencies, U.S. Intelligence in a Hostile World*. New Haven, CT: Yale University Press, 1996.

John Sano is currently Vice-President of AFIO. He was formerly the Deputy Director of the CIA's National Clandestine Service from 2005-2007. He holds a B.A. in Political Science and an M.A. in Asian Studies from St. John's University in N.Y. and a Masters in International Affairs from Columbia University, NY.