An Intelligence Civil War: "HUMINT"" vs. "TECHINT"

Matthew Crosston and Frank Valli

Since 9/11, intelligence has evolved within a changing atmosphere of modern tactics and techniques for information collection. This atmosphere, coupled with massive leaps in technological advancement such as social media, mobile communications, processing analytics, large-form solid-state data storage, novel computational hardware, and software equipment, has thrust intelligence communities around the world into a strange new world of multi-dimensional intelligence. While science and technology and human capability both remain valuable facets of the same overlapping intelligence construct, there is an emerging trend of diametrically opposed camps pushing for one method over the other. This article explains how in terms of field application and intelligence information processing and analysis, both HUMINT and TECHINT could be maximized by the elimination of forced rivalry and by the encouragement of mutual cooperation that is currently lacking.

Keywords: cyber, intelligence, TECHINT, HUMINT, science and technology, national security

An earlier version of this paper was published by Frank Valli as "'HumInt' vs. 'TechInt': A Forced Intelligence Dichotomy," *The Security and Intelligence Studies Journal* 1, no. 3 (Summer 2014). Parts of this paper were also published in Matthew Crosston, "American UAV Apartheid and the 'Blowback' of New Drone Armies," *New Eastern Outlook* (April 3, 2015).

Dr. Matthew Crosston, professor of political science, is the director of the International Security and Intelligence Studies (ISIS) program at Bellevue University. Frank Valli earned a Master of Science degree in the International Security and Intelligence Studies program at Bellevue University.

Introduction

Since 9/11, intelligence has evolved within a changing atmosphere of modern tactics and techniques for information collection. This atmosphere, coupled with massive leaps in technological advancement—such as social media, mobile communications, processing analytics, large-form solid-state data storage, novel computational hardware, and software equipment—has thrust intelligence communities around the world into a strange new world of multi-dimensional intelligence. With the implementation of new technologies and their expansion into the public arena, intelligence collection methods—once reserved specifically for governments or major conglomerations—have increased far beyond traditional human intelligence capability. Countering this, however, and setting the stage for the examined tension, is the admission that humans must not be "devolved" from the field of intelligence. No matter how technologically advanced war may become, human assets will remain paramount in some form or other. "Human Intelligence" (HUMINT) should thus always be considered first among equals.

All these advances have been utilized extensively by the intelligence community in the past and now find themselves freely available for public use. Moreover, the more recent controversial revelations involving metadata usage for threat assessment and identification—in short, the entire Snowden affair—can also be included in this encroachment of the technological into the HUMINT sphere. Techniques taught nowadays to university students for conducting rigorous quantitative research (such as mixed-methods software, automatic computer coding, content analysis, text mining, and bootstrapping), in the previous generation would have been hard-to-access technology found almost exclusively within government circles. The incorporation of science and technology into the loosely termed "Technical Intelligence" (TECHINT) has become a major contributor to both data and strategy.[1] While science and technology and human capability remain valuable facets of the same overlapping intelligence construct, an emerging trend sees diametrically opposed camps pushing for one method over the other. This article explains how in terms of field application and intelligence information processing and analysis, both HUMINT and TECHINT are maximized by mutual cooperation that is currently lacking; their forced rivalry must, in our opinion, be eliminated. Most importantly, the failure of developed countries to focus on the TECHINT/HUMINT fusion will create future national security

problems far more complicated and challenging than presently anticipated, especially as other countries around the world seem to be more motivated and accepting of this need for fusion.

A Snapshot of the TECHINT and HUMINT Relationship

As can be seen in modern theater tactics, human intelligence collection techniques are still readily employed in intelligence operations. The professional adaptation to newer scientific techniques of collecting information has indeed been challenging. Though advantageous for seasoned and novice collectors alike, there remains a highly-opinionated bias against "purely" scientific methods of information collection. This bias is most pronounced at the operational and field levels where priority is still placed on the value of spontaneous decision-making, which is supposedly unique to human collectors. On the other hand, critics ask whether it is worth risking a combatant when similar information may be collected through the technological advancements so prevalent in today's modern society: drones, listening devices, sensors, imagery, intranet infiltration, email tracking, and remote computer commandeering. The rivalry fed by these mutual biases runs deep and prevents a much-needed cohesion between the two facets of intelligence gathering.

Perhaps the best way to highlight this tension is the example often praised as the model for TECHINT/HUMINT collaboration: drone usage. While it is true that the validated drone targets were always meant to be established initially by the effective use of human assets on the ground in the target area, the enthusiastic success of the drone program over the years has led to a relaxing of this process. Today, there are numerous TECHINT-validated drone operations on the ground ahead of time. Some parties within the intelligence community have argued that the possible occasional mistaken target is worthy collateral damage in comparison to risking human assets in the field. What is often unsaid is that part of this change in mindset is also an issue of immediacy and convenience: the need for formal HUMINT validation of targets on the ground slows down and limits drone capabilities and usage.[2] Over time, the tendency to maximize TECHINT in such cases has reduced the value placed on HUMINT and lessened the importance of proper TECHINT/HUMINT fusion.

When discussing this rivalry, a so-called knowledge inferiority complex should also be mentioned; any shift away from classic HUMINT toward TECHINT would suddenly place many intelligence professionals on the outside looking in. Worse perhaps, the requirement to upgrade one's skills from a more traditional HUMINT operative to a TECHINT specialist is likely beyond the learning curve of many seasoned veterans. This aspect of the rivalry is little discussed, possibly seen as the elephant in the room. The "science-phobia" that afflicts many universities in the West (according to which students shy away from highly technical, hard science majors[3]) has been long lamented in terms of its impact on the ability of countries like the United States to stay competitive in the global economy. But this reality also has a deep impact on the technological preparedness of young new cadres of the intelligence community. It is a two-level problem: on the one hand, there is not enough new blood capable of utilizing the tools available for intelligence collection; on the other hand, and perhaps more importantly, there do not seem to be any efforts invested in constructing a connective bridge between these two bodies of intelligence, aiming to intensify their reach and maximize talent capability.

Human Intelligence: Collection and Information

The human factor in intelligence collection is as old as war itself. In the field, it is the most readily utilizable and adaptable method for rapidly obtaining, processing, and acting on targets and objectives. The bias in favor of human information collection techniques is most evident among upper-echelon policy generators, but also among veteran field analysts and warfighters. As described in many accounts, soldiers, as "boots on the ground" for informing human intelligence, are vital to winning war.[4] According to Patrick Murphy, former chief engineer for the Defense Advanced Research Projects Agency's PM Unit of Action Technologies, "we talk a lot about technologies. In the urban warfare setting, you can't get away from the human. You can't fight urban without human."[5] This is especially applicable in the modern warfare theater that intelligence collectors face. The bias favoring HUMINT thus has a great impact on the mindset of those reading the intelligence—the recipients—especially as the intelligence is processed up the information chain to those who enact policy decisions. If there is reticence in relying too heavily on the purely technical capabilities of those who are employed by

the intelligence community, traditional policymakers and government actors (often far older than the intelligence operations agents in the field) might be even more skeptical of over-reliance on information obtained remotely from a machine rather than from a person on the ground.

Collection is only one facet of human intelligence. The information deduced from the intelligence collected is important, as it is responsible not only for formulating policy, but also for altering and developing operational capacities in the field. Human intelligence information often proves crucial for locating and neutralizing adversaries and for allowing expeditious action and reaction in the attainment of national security goals. For example, a 2013 National Public Radio broadcast on women in combat emphasized that many successful night raids in Afghanistan were the result of US servicewomen's prowess in collecting human intelligence information from Afghani women.[6] Those within the intelligence community who still favor the HUMINT bias would be justified in arguing that this would not have been possible if the command had been more focused on TECHINT capabilities and less ready to engage human operatives in sensitive and dangerous situations.

While some element of the HUMINT bias is undoubtedly based on professional self-preservation, there are still important real-war aspects in modern conflict that heighten the relevance of HUMINT capabilities. The emergence of non-state actors that blend into civilian societies, their integration, and the subsequent confusion around managing to discreetly and explicitly identify combatants and target areas have made the exclusive use of TECHINT without HUMINT messy and chaotic.[7] Advances in drone technology also illustrate this; they are not yet so sophisticated as to allow drones to fly unencumbered and unnoticed into heavily populated civilian areas and to identify and then eliminate individual targets. Hollywood movies may have gone in this direction, much to global entertainment delight, but real-world military capability is not yet there. Paradoxically, HUMINT can therefore be used to make the execution of mission objectives *less* messy and chaotic. In other words, contemporary modern warfare seems to have some aspects that ultimately make the exclusive use of TECHINT more chaotic and inefficient; the injection of HUMINT into this arena would, in fact, intensify TECHINT success ratios.

Science and Technology: Collection and Information

The employment of purely technological means for intelligence gathering is relatively new. In modern warfare, multiple high-tech devices have been added to the tools of conventional intelligence collection. Whether through email tracing, cyber collection tactics, satellite imagery analysis, or location techniques employed by drones, science and technology have provided a pivotal new capability in modern warfare with obvious technological-scientific benefits for intelligence information.[8] The assessment of the technological capabilities of terrorist groups—for example, whether they can develop and deploy "dirty bombs" or other IEDs—is a task whereby the information is analyzed most efficiently in a rigorously scientific and technological manner. Another of the most valuable benefits of TECHINT is the ability to keep operatives and warfighters out of harm's way. This benefit, however, also has its critics:

> This change from HUMINT oriented activities to a more technological approach through SIGINT fueled criticism immediately following 9/11. A number of commentators, pundits, and national security specialists argued that there was a degradation of CIA human intelligence capabilities over the past few years.[9]

Fears remain that, without human assessment of intelligence collection, subtle nuances in the data could be missed, thus leading to faulty analysis. This always is quickly countered by the idea that TECHINT can come close to being infallible because of its ease of production and the sheer quantity of data it creates. These competing narratives in assessment techniques by end users further exacerbate the antagonism between the two camps and obstruct the much-needed TECHINT and HUMINT synthesis. If this synthesis cannot take place by finding and training people to be adept in both versions of intelligence collection, then efforts should be invested in policies that encourage intelligence agencies to combine their respective emphases more coherently and effectively. Unfortunately, this encouragement has not, to date, been very strong or compelling.

TECHINT vs. HUMINT: The Policy Angle

In the past twenty years, the spawning of the digital age has created an entirely new dimension for intelligence—both in collection and information—further accelerated by 9/11, after which newly-felt American national insecurity

advanced to fever pitch. With the progression of the digital age, however, technology once reserved for agents with top-secret clearance is now available to the masses with simpler, but still powerful versions available for purchase at any computer store—be it encryption, coding, data-mining, the orgy of advanced apps free on any smartphone, or the incalculable amount of dangerous information accessible online at the mere press of a button.

Technology proliferation and transparency have created the means for massive data collection from open sources (OSINT), causing some to argue for limiting the application of HUMINT. Devastatingly for HUMINT proponents, this argument is founded on the dual hits of mission success and asset safety: if TECHINT can get the job done efficiently without human injection, why bother keeping HUMINT operation space so wide and broad?[10] The policies that previously governed intelligence collection were far from prepared to handle this new technological OSINT avalanche. The so-called graybeards of classic human intelligence techniques were confronted with a new capability for collecting quantities of information, never experienced before, while managing that onslaught effectively through traditional methods proved problematic. Forming policy in this new atmosphere and with these new capabilities has been a struggle for everyone.

Policy originating in the American intelligence community took advantage of this new scientific and technological power by exceeding the bounds of US civil liberty traditions. With the implementation of bills like the Patriot Act in 2001 and the revelations leaked by Edward Snowden in 2013, it seems that the opportunity to maximize the technical means of surveillance and information gathering is apparently too large a temptation to pass up.[11] While it is beyond the scope of this article to examine these decisions either ethically or morally, the important yet underemphasized point in society today is how these new collection capabilities have eaten away at what used to be the exclusive jurisdiction of HUMINT operatives and have intensified the bias against allegedly overpromising and underdelivering TECHINT tools. It cannot be denied that modern and advancing technology allows for greater ease of intrusion into areas and locations that were previously challenging for human agents. In addition, these same technologies aid in the development of constant and long-term surveillance and intelligence gathering. Creating such continuity with exclusively human intelligence agents was previously rather cumbersome, dangerous, and, at times, impossible.

Nobody's Happy: The Fiscal Dilemma between HUMINT and TECHINT

There has always been an economic element to this debate that is perhaps more important than most participants let on. From a fiscal standpoint for those on the HUMINT side, funding the acquisition and training of a human agent for utilization in the intelligence community can be far more beneficial. For this camp, the multipurpose utility of human agents with their analytical ingenuity and flexibility creates an appealing logic for greater investment than a cold machine that serves only one utility. This basic funding dilemma often breaks down in budgetary discussions, with one side lamenting the lack of funding to support its new "toys," while the other camp feels disenfranchised from the financial support necessary to keep its core of cadres refreshed, recruited, and reinvigorated. It can indeed be an odd dilemma, as each side is basically arguing that it does not get enough funding while claiming the other side is wasting valuable monies on less efficient practices.

This, of course, flies in the face of the fact that the annual US intelligence budget has consistently increased over the last ten years due, in great part, to the high demand for successful and relevant intelligence and the necessity for resources, ***both*** human and technological, to satisfy that demand. However, as technological development is already a large proportion of intelligence expenditure and comes with the risk of obsolescence and inadequacy in relatively short periods of time, there is a bureaucratic drive to compensate for this by focusing on "pliable" resources in the HUMINT realm. The intelligence community's long-held reputation for operating at the cutting edge of technological research and development results paradoxically in what is, at times, perceived as a massive budgetary imbalance resolved only by abandoning traditional budget alignments. As a result, TECHINT has been gaining unfair financial attention and prioritization compared to investment and support in HUMINT.

This is, however, a greatly flawed approach; budgetary priorities should be balanced effectively so that technological capabilities can benefit fundamental HUMINT techniques and tactics. This might result in reduced risk in terms of human assets being placed in harm's way while also allowing for far greater fidelity in the intelligence collected and the accuracy of subsequent analysis. Budgetary alignment for TECHINT needs to be established in a way that seeks to further advance and activate the funding given to HUMINT.

The technological battlefield that has been forecast as the war front of the future is both virtual *and* physical, whether that be with field level operatives utilizing drone capabilities or cyber analysts tracking down an electronic trail; therefore, TECHINT at its maximum efficiency and greatest relevance should be regarded as a crucial advantage for both operations and analysis. To continue the contemporary tendency to prioritize source funding in which technical capabilities are competing against human talent is to hinder intelligence capabilities and further exacerbate an unnecessary rivalry. Funding should focus on research, development, and operational efforts that fuse TECHINT and HUMINT.

Bridging the Gap

In field applications, the end goal of obtaining adequate, accurate, and actionable information is best attained when HUMINT and TECHINT capabilities are combined. Bridging this gap is no easy task as there are few collectors who operate freely within both fields, and analysts and policymakers tend to have their own preferential bias as to which intelligence capability produces the best and most reliable information and thus receives their preferential treatment, whether procedurally, bureaucratically, or financially. With the battlefield ever expanding into cyberspace and technical collection techniques, a fusion of traditional HUMINT techniques with science and technology seems inevitable.[12] This fusion should not occupy the forefront of future intelligence collection, but it should most certainly form the foundation for future recruiting techniques in terms of talent acquisition for the next generation of intelligence personnel. Eliminating prior stigmas and moving beyond dogmas of fear, be they against HUMINT or TECHINT, will be of paramount importance.

First in this effort must be the recognition that humans will never be fully eliminated from the field of intelligence. No matter how technological and scientifically advanced future warfare becomes, it will still rely on human capital in some form.[13] But the employment of scientific tools and technological capabilities to prevent threats to soldiers, increase capabilities, and present field operators with the means necessary to achieve mission goals should be considered an essential accessory to the human agent. Fortunately, the bias keeping these two INTs apart is the result of personal perspectives within the field of intelligence rather than any unsurmountable

innate dichotomy. This personal bias is founded heavily on the inadequacy that veteran operatives, skilled in traditional HUMINT techniques, attribute to the emerging importance of technology. As mentioned earlier, the fear of not being able to acquire the necessary technical skills is not based simply on their desire for job preservation, but rather on a deep philosophical and professional disagreement with how effectively and to what extent TECHINT can replace the unique advantages of human assets in the field. This is yet another reason proper fusion between the two techniques is essential. The key for short- and medium-term progress is obviously not to discard those who do not have or cannot acquire technological talent, but rather to focus on ways in which each becomes competent in the language, approaches, and objectives of the other. In this way, TECHINT and HUMINT will understand how to interact effectively, thus improving the impact of the intelligence produced and best serving national security.

The Fusion Dilemma around the World – A Brief Overview

While, for now, it is largely true that technologically-advanced states experience this self-imposed rivalry to a higher degree, the dilemma between TECHINT and HUMINT is not destined to be limited to highly-developed nations. This is a problem that will undoubtedly evolve further as intelligence practices and cooperation continue to become more of a global norm.[14] With financial and technical resource shortfalls, many less-developed countries are somewhat forced to favor HUMINT in both collection and assessment over the newer methods generated by science and technology.

Countries such as Britain, Australia, Russia, China, and Israel have begun to emphasize TECHINT over HUMINT, as can be seen by using modern intelligence staples such as drones, aerial and satellite surveillance imagery, and other MASINT, SIGINT, and IMINT tools. The same rivalry seen in the United States is likely to be seen in these countries as well, if not already evident. Countries that have progressed technologically tend to create their own internal HUMINT dilemmas within their intelligence communities, simply because scientific innovation will always outpace the ability of its people to keep up. By not finding the necessary synthesis and fusion, a country endangers its own national security, especially when many lesser-advantaged countries are willing to de facto achieve that fusion

through unscrupulous means. A brief examination of UAV (unmanned aerial vehicles) proliferation is a perfect example of this phenomenon.

De Facto Fusion in the Middle East

In 2013 the Israel Defense Forces (IDF) succeeded in destroying a drone that it tracked flying over sensitive military installations and approaching the Dimona nuclear reactor. The drone was unarmed, but operated by agents elsewhere and attempted to relay images back to a home base. The Israelis did not disclose whether the enemy objective had been successful, but they were certain that the drone was not American, Chinese, or Russian, claiming instead that it was an Iranian drone assembled in Lebanon and flown by Hezbollah.[15] We have referred to this elsewhere as the world's first "Islamic Crescent drone," and it signals the transnational nature of drone technology proliferation already in existence.[16]

In 2013, Iran claimed to have developed both Epic, a drone supposedly designed for both combat and reconnaissance, and Throne, a long-range combat UAV with alleged stealth capabilities. Iran certainly is not shy in its public relations efforts to claim regional dominance in TECHINT.[17] This should be treated with some skepticism given the Israeli factor; it is doubtful Iran can compete with the technical prowess of the Israeli military and its technical arsenal and thus some of these press releases are probably more for effect rather than actually being effective. Indeed, the general global reaction beyond Israel has been overwhelmingly skeptical. Having said that, there are still important things to consider; it is likely prudent for those who are not in favor of an assertive Iran to ascertain the veracity of its claim that its drones have dual capability—both combat and surveillance/reconnaissance.[18] Iran also has made bold claims about how it has developed the human capital to competently utilize the technology. This also needs to be verified. Not coincidentally, after these so-called Iranian "achievements," both Egypt and Saudi Arabia became far more interested in acquiring drones for their militaries and sought the necessary technical and financial investment for developing their own programs and recruiting the right amount of human capital.

The initial pursuit of tactical drones by other countries has up to now been focused much more on strategic global positioning and the projection of power in foreign policy, or at least the possible capacity of that automated

projection. Turkey, however, has a distinctly domestic aspect for its drone pursuits that could provide an extremely dangerous precedent moving forward. While it makes claims about the positive use of drones domestically in order to keep peace and resolve conflict, it seems the more immediate violent use of drones within Turkey is going to be predicated upon the continued destruction of the Kurdish Workers Party (PKK). The Turkish Army has, of course, totally avoided mentioning the PKK by name in connection to its drone policy. It instead has focused more on how effective UAVs can be with border security, urban warfare, and other operational missions. On the surface, there is very little to protest. But when one considers that these issues for years have been code words for PKK unrest, it becomes rather transparent that the deployment of armed drones within the sovereign territory of Turkey is going to be for PKK destruction. This subtle distinction shows how the need to develop human talent alongside technological acquisition is becoming ever more important as drones acquire more uses inside of territorial borders. Simple commercial-military deals like the ones Turkey and Israel had in the past are becoming more layered and spurring the acquiring countries to engage in domestic development for purely domestic security needs. It will be interesting to see how this future develops; we have seen already that there seems to be little in the way of international norms and laws to prevent global operations with armed UAVs when used by major powers like the United States. Will there be even less oversight and global community reaction when smaller powers use weaponized drones for issues taking place within their own borders? If yes, then it means the armed UAV arena moving forward is only getting deadlier with the acquisitions of countries like Turkey.

De Facto Fusion in Greater Asia

If Turkey provides a potential new precedent for armed UAVs in terms of violent domestic uses, then Singapore might also be setting a precedent as well in that it has been surprisingly explicit and direct in its long-term objectives and goals. It has openly declared the simple purchase and acquisition of UAVs from major sellers like Israel as the necessary first step in a long-range strategic plan that demands native-born and domestically-trained personnel to operate drone fleets. This is considered equally crucial, if not the more crucial strategic piece to its national plan.[19] If the Singapore

model, for lack of a better term, becomes more embraced, then the day is drawing near when more countries will be utilizing drone purchases not as the foundation of domestic fleets, but rather as the instigators to develop and evolve native industries and home-grown operators. In other words, Singapore is the country that is the most adamant in declaring its right to achieve expansive drone independence—from construction to militarization to operation capacities. If successful this will signal, if not the end, then certainly a mitigating challenge to the so-called American expertise and technological dominance.

In fact, a possibility exists that other countries within the greater Asia Pacific region will follow the Singapore model and thus create what could end up being the second largest UAV market in the world. (This fact, however, can be argued as statistical trickery: the greater Asia Pacific region *as a whole* could overtake Israel for second place. But this is conflating all national acquisitions into one whole sum. When Israel is compared to the acquisitions of individual nations of greater Asia, it maintains its solid hold in second place).[20] India, South Korea, North Korea, Malaysia, and Australia are all major actors in the greater Asian UAV market, in addition to the stalwarts of China and Singapore. Perhaps most importantly, every single one of these states have expressed the desire to not just purchase UAVs from other countries, but also to train their own agent cadres and to develop new human capital for militarized drones. These countries are pursuing the TECHINT/HUMINT fusion with greater aggression and ambition and do not feel it necessary to align their national interests to the strategic interests of the United States. Thus, it might not be wise to automatically assume that the United States need only worry about non-allies developing domestic UAV industries; even allies, pursuing their own national interests, could find themselves at odds with American objectives and policies.

This is an important distinction to make which at present is being underemphasized within UAV proliferation debates and discussions: the ability to fuse the power of TECHINT with the agility of HUMINT provides new power projection to countries that were previously limited. The United States and Israel have in the past justifiably maintained supreme confidence in their ability to outpace and outrace any other state's acquisition and development. But this logic may have been too absolutist: it is not necessary for a lesser rival to perfectly match the technical and human capabilities of

the United States or Israel in order to present real challenges and dangers to their interests. The fusion attempts described above within the drone arena show just how much potential for disaster lies in a relative increase in capability. Absolute equalization is not necessary for damage to be done.

Changing of the Guard

Retaining policy focus on the needs and requirements of the soldier, operator, and analyst will result in effective and sustainable evolutionary policy—embracing the growth of the technical field as well as the development of modern human agents—and will advance national security interests on the battlefield and in the intelligence arena. To recognize this need and adapt accordingly are the steps required for the intelligence community of the next generation.

Often the best trained, knowledgeable, and experienced personnel do not move up the rungs of the bureaucratic ladder to become effective policymakers. This lack of realistic field experience in the policymaking arena equates to a lack of successful intelligence prioritization and future innovation. As "purists" continue to dominate policy and budgetary discussions, when it comes to the TECHINT/HUMINT divide, the unnecessary and false division between these two crucially important INTs likely will continue. How do intelligence communities from countries like the United States and Israel develop beyond this? First, they should prioritize the promotion and elevation of those who see the need to integrate TECHINT and HUMINT seamlessly in both operations and policy. The only way to enact substantive change is to let people see that new approaches are being genuinely rewarded. The false dilemma over TECHINT/HUMINT can be overcome if the United States and Israel begin to promote those who see the potential of an integrated approach and produce people who are adept in the relevant tools and methodologies.

Second, the United States and Israel should begin developing their own training and educating organizations in order to produce new specialists who can walk and talk in the language and techniques of both INTs. As embarrassing as it may be to admit, there are numerous examples of this process already taking place around the world with the most obvious rivals being China and the Russian Federation. In this case, following the lead of the "enemy" may not be such a bad idea. Transitional training programs could enable and facilitate present generation intel specialists to follow and

understand the need for this fusion. There is no expectation for non-technically oriented employees to become computer scientists or technical specialists to suddenly become adroit "super spies" in the field. Rather, efforts need to be made to properly enhance and engage communication between the two communities so that they can talk and collaborate, even if each remains relatively non-proficient in the specialization of the other; it is more about facilitating competence than demanding expertise. Surprisingly, the benefit of these approaches so far has been largely overlooked. Not taking seriously the fusion between TECHINT and HUMINT as the future of intelligence means an unspoken and crippling civil war continues forward; what should become an alliance unfortunately and dangerously will remain a rivalry.

Notes

1 Intelligence Science Board, *The Intelligence Community and Science and Technology: The Challenge of the New S&T Landscape* (Washington, DC: Office of the Directorate of National Intelligence, 2010), https://fas.org/irp/dni/isb/landscape.pdf.

2 Ashley J. Tellis, *Pakistan—Conflicted Ally in the War on Terrorism* (Washington, DC: Carnegie Endowment for International Peace, 2007), http://carnegieendowment.org/files/pb56_tellis_pakistan_final.pdf.

3 Katherine Beard, "Behind America's Decline in Math, Science, and Technology," *US News & World Report*, November 13, 2013, http://www.usnews.com/news/articles/2013/11/13/behind-americas-decline-in-math-science-and-technology.

4 Andy Savoie, "Boots on the Ground: HUMINT Needed for Urban Warfare," *Aerospace Daily & Defense Report*, December 8, 2004, http://aviationweek.com/awin/official-boots-ground-humint-needed-urban-warfare.

5 Ibid.

6 "Women in Combat, and the Price They Pay," "Morning Edition," *NPR*, March 18, 2013, http://www.npr.org/2013/03/18/174444738/women-in-combat-and-the-price-they-pay.

7 WMD Commission, *Final Report of The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington, DC.: Library of Congress, 2005), https://fas.org/irp/offdocs/wmdcomm.html.

8 Kevin M. O'Connell, "The Role of Science and Technology in Transforming American Intelligence," in *The Future of American Intelligence*, ed. Peter Berkowitz (Stanford: Hoover Institution Press, 2005), pp. 139–174, http://media.hoover.org/sites/default/files/documents/0817946624_139.pdf.

9 Rand C. Lewis, "Espionage and the War on Terrorism: Investigating U.S. Efforts," *Brown Journal of World Affairs* 11, no. 1 (2004):175–182.

10 Ishmael Jones, *The Human Factor: Inside the CIA's Dysfunctional Intelligence Culture* (New York: Encounter Books, 2008).
11 Public Law Pub.L. 109-177, *USA PATRIOT Improvement And Reauthorization Act of 2005* (Washington, DC: Congressional Publications, March 9, 2006).
12 Denis O'Connor, *HMRC Handling of Human Intelligence Sources.* (London: Inspectorate of HM Revenue and Customs, 2006), https://www.justiceinspectorates.gov.uk/hmic/media/hmrc-the-handling-of-human-intelligence-sources-20070325.pdf.
13 Robert K. Ackerman, "Defense HUMINT Needs Technology, Too," *Signal*, October 2006, http://www.afcea.org/content/?q=defense-humint-needs-technology-too.
14 Paul Todd & Jonathan Bloch, *Global Intelligence: The World's Secret Service Today* (New York: Zed Books, 2003).
15 Kristin Roberts, "When the Whole World has Drones," *National Journal*, March 21, 2013.
16 Matthew Crosston, "American UAV Apartheid and the 'Blowback' of New Drone Armies," *New Eastern Outlook*, April 3, 2015, http://journal-neo.org/2015/04/03/american-uav-apartheid-and-the-blowback-of-new-drone-armies/.
17 East West Services, "Iran Announces New 'Epic' Combat UAV with Stealth Capability," *Geo-Strategy Direct,* May 22, 2013.
18 Crosston, "American UAV Apartheid and the 'Blowback' of New Drone Armies."
19 East West Services, "Singapore First East Asian Military to Deploy Israeli Strategic UAV," *Geo-Strategy Direct,* June 6, 2012.
20 "Asia UAV Acquisitions," *Defence Review Asia* 3*,* no.7 (2009): 20.