'The More Things Change': HUMINT in the Cyber Age

David V. Gioe

From targeting to recruitment, clandestine handling to intelligence collection and processing, no aspect of Human Intelligence (HUMINT) operations remains unaffected by the profound impact of technological development, particularly in cyberspace. Rapid innovation in this domain has both enabled and encumbered the gathering of intelligence via human sources, and in some respects even altered the established human agent acquisition cycle itself. Although perhaps some aspects of twenty-first century HUMINT techniques would be unfamiliar to John Le Carre's Cold Warrior, George Smiley, he would surely maintain that personal interaction remains the heart of HUMINT, and no amount of cyber-interaction can replace the close bond between an intelligence officer and his or her agent.

Despite rapid advances in other intelligence collection types, including Signals Intelligence (SIGINT), overhead imagery intelligence (IMINT), and Electronic Intelligence (ELINT), HUMINT operations will remain a core staple of intelligence collection for the foreseeable future, supplemented, not replaced, by cyber developments. Given the necessity and timelessness of interpersonal interaction, how much HUMINT can actually be accomplished (or defeated) in cyberspace is a challenging question to consider. One thing, however, is certain: 'Technology has turbocharged espionage' (Campbell, 2013: 62).

This chapter explores five primary lines of inquiry with respect to the impact of digital and cyber developments in HUMINT. First, this chapter will consider if HUMINT is even still required in an age of unprecedented publicly available information resulting in open source intelligence (OSINT) and accessible big data. Second, if HUMINT operations remain a core function of intelligence, this chapter will further explore both the offensive human

D.V. Gioe (✉)
New York, US
e-mail: dvgioe@gmail.com

R. Dover et al. (eds.), *The Palgrave Handbook of Security, Risk and Intelligence*, DOI 10.1057/978-1-137-53675-4_12

recruitment targeting that results from social media exploitation as well as cyber espionage. Third, the flip side of this targeting boon is increased counter-intelligence challenges for any intelligence or security agency, from phishing to cyber hacks that have infiltrated and exposed a great deal of sensitive information about on-going intelligence capabilities and operations and the personally identifiable information (PII) of those employees of the US intelligence community. Fourth, the advances in technology as well as networked communications have raised concerns about the challenges of working undercover as an intelligence officer. In particular, this chapter will consider the impact of data mining and the proliferation of biometric data that is collected and often shared internationally. Finally, perhaps the most underappreciated development is the role of mass intelligence leaks on the recruitment of new human sources, also referred to as 'agents'. This chapter concludes that cyber capabilities and considerations will not fundamentally alter the nature of HUMINT operations, but they will force change to the process in which HUMINT operations are conducted. Although HUMINT operations will have to evolve, intelligence officers should embrace the potential of technologically empowered HUMINT operations while at the same time recognizing and mitigating the considerable concomitant challenges.

The Impending Decline of HUMINT?

There is a popular – and pernicious – myth that holds that after the al-Qa'ida attacks of September 11, 2001, the Central Intelligence Agency acknowledged that its traditional methods of espionage would not work against radical Islamist terrorist groups. Further, because CIA operations officers (or 'case officers') under traditional covers would not penetrate groups like al-Qa'ida, the CIA needed to reinvent itself for the coming struggle. In any case, groups like al-Qa'ida were cellular in nature and based on a high degree of trust and personal verification. The efflux of this analysis was HUMINT methods could not be effective against such groups in any case and technology would replace traditional methods. While this was allegedly happening, technological capabilities at the National Security Agency exploded, rendering an over-reliance on SIGINT to provide early warning as well as actionable intelligence.

According to Charles Cummings, 'The CIA effectively gave up on HUMINT in the wake of 9/11, relying increasingly on blanket electronic surveillance – of phone calls and emails, conversations in chat rooms, of banking records and travel plans' (Cummings, 2015). Cummings suggests that SIGINT (which is done by the NSA not the CIA, as Cummings seems to imply) has eclipsed HUMINT as the lead collection type against terrorism. This betrays a deep misunderstanding of the CIA's role and efforts in HUMINT and illustrates a misconception in popular understanding of the craft, especially in the digital age. Not only are HUMINT and SIGINT not mutually exclusive, most counterterrorism (and other) operational successes after 9/11 relied on a synergistic relationship between the various 'INTs'. But

if HUMINT is not eclipsed by SIGINT, might it be made redundant by open source intelligence (OSINT) and the tantalizing promises of 'big data'? Noted one CIA officer, 'Mouse clicks and online dictionaries today often prove more useful than stylish cloaks and shiny daggers in gathering intelligence' (Mercado, 2004: 45). Does this relegate the HUMINT collector to the status of relic, or street tradecraft as anachronistic?

With the prolific annual increase in information available online and the corresponding emphasis in publicly available intelligence, some authors have argued that OSINT collection and analysis (including 'big data') will overcome clandestine sources in the near term. According to former senior US intelligence officer John Gannon, 'Open source has expanded well beyond [the] "frosting" and comprises a large part of the cake itself. It has become indispensable to the production of authoritative analysis' (Gannon, 2001: 67). Further, as one CIA officer wrote, 'Collecting intelligence these days is at times less a matter of stealing through dark alleys in a foreign land to meet some secret agent than one of surfing the Internet under the fluorescent lights of an office cubicle' (Mercado, 2004: 45). These officials seem to suggest that HUMINT is of a time gone by, perhaps considered even quaint, and that stealing the adversary's plans and intentions can be done almost exclusively over fiber-optic cables. While there is no denying that OSINT is a valuable tool, it cannot replace traditional HUMINT when it comes to collection of national security information in its formative stages, that is, before it appears on the internet at some point.

It is a timeless debate whether information is worth stealing because a government or other entity has attempted to keep it concealed. The Soviet KGB, for instance, historically placed a higher degree of confidence in classified information that was collected via HUMINT means, even if there was publicly available open source information that was more reliable. However, information believed to be secret is not necessarily more valuable than that collected by a human agent. Still, not all intelligence officers would agree that non-secret intelligence is intelligence at all, but that pendulum seems to be shifting in favor of OSINT, particularly as the analytical tools improve and budget watchers see real value. Indeed, OSINT is appealing because it is politically acceptable to adversaries (no foreign official is suborned or betrays his country), involves almost no risk of diplomatic incidents, and is relatively inexpensive. A subcategory of OSINT, Social Media intelligence (SOCMINT), also may yield valuable insights into the political and cultural dynamics of a country, particularly if it is a 'hard target' or closed country. A former Director of GCHQ, Sir David Omand, has argued persuasively that SOCMINT be considered a key intelligence collection type alongside SIGINT, IMINT, etc. (Omand et al, 2012: 1–23). But can SOCMINT become first among equals?

Technological sources provide vast volumes of intelligence, but HUMINT remains fundamental for truly understanding adversaries' capabilities and intentions. Properly vetted and methodically corroborated, open source information (to include social media) can tell the intelligence analyst or defense

planner a great deal about what is happening in the present time, but it cannot reveal much about the plans and intentions of foreign adversaries, particularly the handful of senior leaders who call the tune in most adversarial regimes. That remains primarily the realm of HUMINT. In fact, the wealth of intelligence collected by skillful Internet browsing can help focus HUMINT collectors on the so-called 'unknown unknowns' and ensure that these intelligence officers are focused on the very highest priorities. During the Cold War, for instance, Soviet newspapers and other 'gray literature'[1] needed to be collected by CIA officers because they were not available via other means. Freed from such collection duties by digital technology, today's operations officers can hunt higher priority quarry. And, as explained below, they can use SOCMINT and OSINT in their efforts as a force-multiplier.

Biometrics: The Double-Edged Sword

Since the post-9/11 invasions of Iraq and Afghanistan, military intelligence in particular has relied heavily upon biometrics to identify hostile actors in a guerilla or counterinsurgency environment. It is common for even small units to take fingerprints or retinal scans of suspected insurgents for upload into a massive biometric database (Clark, 2014). The advances in high-speed data transfer have made local intelligence actionable in ways before thought impossible. The role of such interconnected technology on the battlefield and improved real-time situational awareness has been revolutionary for military personnel, but networked computer systems carrying massive amounts of information can also pose a threat to intelligence officers. Former CIA Director John Brennan noted, 'Digital footprints may enable us to track down a suspected terrorist, but they may leave our officers vulnerable as well' (Lyngaas, 2015). Brennan may have been referring to the challenge posed by advanced biometrics, which can make developing and maintaining cover identities difficult.

Maintaining and 'defending' one's cover has always been a key requirement for any operational intelligence officer. Intelligence officers travel internationally for a multitude of reasons, and chief among them is meeting with their clandestine agents. Doing so in alias or a disguise can add to the security of the operation. However, technology and the Internet pose direct challenges to this in two main ways. First, biometrics – particularly those employed at international borders – make alias travel more challenging. Limiting a single alias for use in a single country had already truncated the use of alias travel, and as countries share more biometric information, such as those of the European Union, a single identity may now only be used in a group of countries. If an intelligence officer wishes to travel in a personal capacity, such as on vacation in Europe, he or she must think carefully in an attempt to balance professional and personal personas. The most common forms of biometric tracking are retinal scans and fingerprints, but continuously improving facial recognition software can be accurately employed well

beyond border checkpoints and the like. While it may be technologically possible to defeat these measures, the more prudent course of action may be to accept them as the new normal from a counterintelligence perspective and plan operations accordingly.

It is harder to plan around the second form of digital tracking, and that is the prevalence of social media. As noted, SOCMINT can be a powerful tool for intelligence collection or source verification, but it must be considered from a counterintelligence viewpoint as well. Over a billion people now have Facebook (or similar) accounts, not to mention professional profiles in LinkedIn and other social networking sites. These, to use Director Brennan's words, could also be described as 'digital footprints' – the kind that can both validate a persona and withstand some level of scrutiny by a curious acquaintance or a security service. Before the proliferation of social media, and certainly during the Cold War, an intelligence officer only had to back up (or 'defend') his cover in mostly superficial ways. For instance, he could pose as a businessman traveling in search of contracts or clients. He would need a few business cards, perhaps some corporate letterhead, a phone number, and some sort of plausible cover legend to tie it all together.

Today, even if the biometric issue could be solved, the ostensible businessman would need a LinkedIn profile, a web presence, and other digital trappings of a life in pursuit of commerce. If pressed, he could have to describe his office building, his parking garage, his favorite lunch place, or his daily commute in ways that could be easily checked in Google Earth or similar commercially available mapping software.[2] Even if his business were deemed legitimate by an investigator, how could he explain having no personal social media presence? And, if he did have one, how far back does it go? Thanks to a digitally connected world and the necessary footprints in cyber space, the ease with which identities can be checked, and the increased level of scrutiny that alias travel must bear, call into question the efficacy, cost effectiveness, timeliness, and defensibility of such intelligence tradecraft much further into the twenty-first century. Given that the need for operational travel will remain (agents will always need to be met in person at least occasionally), new tradecraft methods will have to be developed that can both utilize technology for defensive purposes such as withstanding scrutiny, as well as harness cyber power for offensive missions.

Cyber Counterintelligence: Phishing, Hacking, and Social Media Exploitation

The cyber age impacts classic conceptions of HUMINT, ranging from how agents are recruited to their handling; including communication procedures, meeting arrangements, and even payment for services. HUMINT agent recruiting has always followed a familiar pattern, commonly referred to as the 'HUMINT recruitment cycle'. Although the words used might vary,

prerequisites to any agent recruitment include the phases of spotting, assessment and development before a formal recruitment is made. Just a generation ago, an intelligence officer would spend much time attempting to meet as many contacts as possible, perhaps by attending various international gatherings or similar functions. He would then sift through these contacts to determine who worked in which agencies or departments – and in what capacity. Once this was determined, the intelligence officer would seek to ascertain more precisely which contacts had access to non-public information sought by his intelligence service or political leadership. This process is called 'determining placement and access' and is extremely time consuming.

However, savvy spies and intelligence services can save massive amounts of time and energy by harnessing the power of social media and online research tools to reduce the amount of time required to 'troll' for contacts and further reduce the sifting required to determine the 'placement and access' of any contact. This is enabled by two key cyber events: First, exploiting social media to find out what people voluntarily reveal about themselves and second, malicious hacking. For instance, via professional networking sites such as LinkedIn, people reveal an astonishing amount of information about their professional positions, detailed duties within those positions, place in a corporate hierarchy, client base, dates of employment, military service, security clearance level, and other information that might take a non-tech enabled intelligence officer weeks or even months of personal meetings to elicit. Combining information on professional sites such as LinkedIn with personal information provided via sites such as Facebook – again, voluntarily – may reveal a startling amount of information on a person, including personal situations such as marital status, travel history, date of birth, children's and siblings names and dates of birth, and even candid comments about frustrations at work, conflict with a professional superior, disagreement with a national policy, disappointment with an election result, and so on.

Even if a person wished to remain off of social media and provided no information voluntarily, this is no longer a sure-fire defense due to the second key cyber consideration: the age of persistent (and often successful) cyber-attacks. While economic espionage and organized crime make up the majority of hacking activity, cyber breaches such as that of the Anthem health insurance company would reveal a trove of sensitive personal data, potentially including one's own medical history, and perhaps more importantly, that of one's family (Reuters, 2015). Even more devastatingly, breaches of US government systems, such as the June 2015 breach of the Office of Personnel Management (OPM), lay bare troves of personal information that would save any intelligence service untold amounts of time in seeking the right approach to recruit the right person, in the right agency, at the right time.

It is not hyperbole to acknowledge that the twin cyber giants of social media and malicious hacking have revolutionized the ways in which intelligence services seek, locate, assess, and vet their quarry. During the Cold War,

intelligence agencies were happy to receive an internal phone book that listed individuals and in which department or directory they worked. Although the internal employee directory was not a highly classified document, it was a basic building block of mapping the adversary, even knowing who was on their team was a place to start. As such, even this rather low-level information was protected. Today, there is no need to steal the proverbial internal phonebook. Many employees of intelligence and security agencies have a social media presence and openly advertise their affiliations (although the majority do in responsible ways). This seemingly innocuous information could be part of a targeting mosaic, carefully woven by a hostile intelligence service. With such an increased counterintelligence threat, it was not long until governments developed training and awareness programs for social media. At present, the US Department of Defense has at least five different such programs (US DoD, 2015). Likewise, in 2011, the British Ministry of Defence launched the 'Think before you share' campaign for service members and MoD civilians who are active on social media sites. The UK Chief of the Defence Staff's Strategic Communications Officer reminded his staff 'to be aware of the risks that sharing too much information may pose', warning, 'You don't always know who else is watching in cyberspace' (UK MoD, 2011).

Before massive leaks and government hacks, both intelligence officers and those with high level clearances were encouraged to minimize or simply not develop a social media presence. It was felt that this type of prudent reduction of one's online presence would aid in the maintenance of clandestine covers as well as retard some advances in biometric technology. Indeed, having a smaller digital footprint would make it harder for any adversary to challenge one's cover as well as complicate any potential recruitment approach. This calculus has been turned on its head by massive breaches of several government as well as private databases that store personally identifiable information as well as personally sensitive data.

A minimized social media presence could be considered best practice because hostile intelligence services would surely use any publicly available information to build a picture of their target. They would look, for instance, for social media posts that may suggest a disagreement with a national political issue or foreign policy approach. This would be considered a potential motivation to betray one's own government. Alongside this search for potential motivations, potential vulnerabilities would also be sought by scouring the Internet. Might the target be having financial problems, or maybe a serious health issue affecting himself or his family? Might the target have a vice that could be exploited? Or maybe she could suffer from a gambling or drinking problem. Keeping these personal beliefs and problems off of social media was part of a robust counterintelligence posture. However, according to US officials, the recent OPM breach has most likely laid bare the potential motivations and vulnerabilities of millions of current and former US government employees, over a million of whom have had access to Top Secret information at some point in their career.

Crucially, the data stolen includes the 'Questionnaire for National Security Positions' (often referred to as the SF-86), filled out by millions of US federal employees seeking some level of security clearances (Takala, 2015). The SF-86 runs over one hundred pages and lists such things as personal finances, assets, personally identifiable information, passport information including dates of travel to foreign countries, and an exhaustive list of former residential addresses, employers, friends, and family members. Perhaps most alarmingly, the OPM hack also gave the perpetrators access to background investigators' notes during security clearance investigations. These notes would likely contain the investigating officer's comments and concerns about the subject's suitability for access to classified information. In hostile hands, these notes, combined with the SF-86 forms themselves could provide a blueprint for a foreign intelligence approach to a vulnerable US government employee. As one author commented, 'United States national security is in deep trouble, perhaps the worst it's been in history'. The same author noted, 'The OPM breach let loose what is probably the most complete national government employee blackmail kit ever to fall into enemy hands' (Gewirtz, 2015).

Additionally, the cyber age has not only altered the assessment process, but it has changed some agent handling techniques as well, including the speed at which time sensitive information can be received by the case officer as well as enhancing the security of the relationship. The cyber age has enabled data to flow securely and rapidly around the world, even in and out of otherwise 'closed' countries. Moreover, the rapid advances in encryption now protect data in ways previously thought impossible, including related developments as The Onion Router (TOR) and other 'dark web' sites. Applied to agent communication, secure links with real time connectivity can be nothing short of a tradecraft revolution. During the Cold War, for example, the CIA and its partner British SIS ran a high-ranking source within Soviet military intelligence (the GRU). Colonel Oleg Penkovsky had advance knowledge that the Berlin wall would be erected in August 1961, but he was in Moscow at the time, and his handlers were unable to meet him personally to debrief this intelligence. In the cyber age, it is likely that Penkovsky would have been issued with some sort of secure communication system to alert his handlers to the impending construction. Had Penkovsky been able to warn the Kennedy administration about the Wall's construction in advance, history may have turned out differently. Indeed, the Cuban Missile Crisis was resolved peacefully thanks to Penkovsky's timely intelligence. Throughout history, meeting recruited agents is almost always the most precarious and dangerous part of any HUMINT operation. Indeed, the very reason intelligence street tradecraft was developed was to make personal meetings as secure as possible. Historically, the deadly serious cat and mouse game between intelligence officers and adversarial security services has incorporated technological developments as quickly as possible. To wit, the history of operational tradecraft would read like a history of innovation with the side that successfully fielded the latest technology first often winning that round.

A Personal or Exclusively Cyber Relationship?

Although it may have a rather glamorous or sensational reputation, many aspects of spying have a great deal in common with its more prosaic cousin: dating. In both cases, technology (for those who avail themselves of it) enables people to meet, consider what they have in common, and get to know each other. But, it is hard to imagine that online dating will turn into an exclusively online or 'virtual' marriage. At some point, the participants will meet face to face. Likewise, even if social media or cyberspace could bridge the gap for a willing intelligence service and its agent, they will meet in person at some point.[3]

Despite the advantages of technology, there is no substitute for the personal interaction between a case officer and his or her agent. Any case officer would want the 'gut-check' of meeting an agent personally in order to make a more comprehensive assessment of his or her suitability. The case officer would want to hear, in person, why his agent decided to take the risk to work for a foreign intelligence service. Even if this answer were already provided via a computer message, the case officer would want to look his agent in the eye during his or her explanation of motivation. Could the agent keep eye contact? What if he kept looking away? Could he sound sincere? Could he recapitulate the intelligence already provided? What if the details did not match what had been provided via electronic means? What if he had trouble restating his motivations for spying in person? It could be that the agent is helplessly shy or perhaps has a bad memory. Or, alternatively, it could signal a looming counterintelligence issue, such as he may be controlled by his service, or, he may not have been the person behind the keyboard typing the messages to the case officer. Like an online love interest that sounds too good to be true, a hostile intelligence service would have a much harder time leading an experienced case officer down the primrose path in person. If an operations officer were to succumb to the convenience of a purely cyber clandestine relationship, he or she would miss the invaluable opportunity to apply human intuition and emotional intelligence (sometimes referred to as 'soft skills') to the case.

Even if there is no disconnect between a 'virtual' and actual persona, the need for interpersonal contact supersedes just the vetting and assessment stages of HUMINT. A good deal of any human communication is done through non-verbal means, and part of HUMINT is interpreting unspoken communication such as mood and body language. It is commonly held that the most successful case officers are highly manipulative, but this undervalues the skills of good listening and empathy. This is why the most talented case officers have a high degree of emotional intelligence. A touch on the arm, or a look in the eye, a calming act of kindness, a well-timed, thoughtful gift, and some reassuring words of encouragement are all necessary parts of running a human agent. Any agent will need direction and tasking, and this can be done via digital means. But, if the case officer and agent are only connected via a fiber optic line or satellite uplink, the case officer may not discern what his agent is thinking or

feeling. Inflection and tone are notoriously difficult to discern over email, yet these are critical insights into an agent who may be despairing or wavering in his stressful double life. Many agents at some point will face a personal crisis, or perhaps a distracting family issue, or have a security scare. At such times, the case officer becomes more than a person that collects intelligence, he becomes a friend to confide in, or a rock when the going gets tough. Thus, although tempting from an efficiency and security standpoint, simply running agents solely via computer or digital interface is not the way to motivate, access, guide, and maintain a productive human agent.

Jeopardizing Future HUMINT via Trusted Insider Leaks

Perhaps the largest hidden cost of mass intelligence disclosures to future HUMINT collection is the crisis of confidence in the minds of those who Western governments most desperately wish to recruit. Recruiting human intelligence sources is already a difficult task, made harder by mass leaks. A representative of an adversary government, a rogue state, or a member of a terrorist network may wish to cooperate with an intelligence service for any number of reasons, provided his safety can be reasonably assured. If he is considering cooperation, he will look for an official who is a discreet professional to provide his information. He may study the officers of his desired agency for a long time in order to make up his mind about a life-changing decision. Indeed, any slip up on the part of the case officer, such as indiscretion or sloppy agent tradecraft, could very well cost the foreign agent his life and potentially even jeopardize the well-being of his family in his home country. This is serious business and a potential foreign agent will weigh carefully the risks and benefits of a clandestine relationship with the beneficiary government. The potential agent must be satisfied that his case officer can assure his safety, and, of course, these assurances must be credible.

Thanks to the actions of Edward Snowden and Chelsea (Bradley) Manning, this challenge may seem, at present, to beset only American intelligence, but the problem affects other countries as well. First, it directly affects those American allies who heavily rely on American HUMINT, passed regularly via liaison channels. Moreover, it may affect other intelligence services who, to date, have not suffered a catastrophic intelligence breach, but it would be wrong to think that mass leaks would happen only in America. For instance, in February 2015 hundreds of intelligence cables belonging to multiple South African intelligence and security agencies were leaked to the media (Smith, 2015). One South African government spokesperson described the mass leak as 'deeply embarrassing', but embarrassment is only the tip of the iceberg in terms of problems for the South African services. More problematically, it may produce a chilling effect on future HUMINT recruitment. Mass leaks and their accompanying crisis of confidence in security is now a primary reason potential human intelligence sources may opt to avoid committing espionage on behalf of any foreign intelligence service.

Recruitment of a foreign source may take many forms. For instance, a potential source may be sought out due to his placement and access (likely enabled by SOCMINT and OSINT), approached by a CIA case officer or FBI Special Agent, his motivations and personality assessed, and perhaps recruited to work in place (on motivations and recruitment, see Burkett, 2013: 7–17). He might walk in to an embassy or consulate abroad and volunteer his services. Perhaps he will need some convincing that the risk is worth the reward and, in any case, the risks will be minimized by clandestine interactions with well-trained professionals.

But how can intelligence services continue to attract these sorts of people whose information is required by policy makers and defense planners? Human agents have a risk calculus that includes money, ideology, ego, revenge, or some combination of these. But in all cases, potential sources must be reassured that hushed words stated in confidence will not endanger them in the next tranche of leaked information. The consequences for diplomats, military officers, security personnel of hostile regimes, or terrorist networks, would be swift and severe. Given this guaranteed punishment, it is understandable that a potential foreign agent may decide against walking into an embassy, seeking out a representative, or accepting a follow-up meeting with a friendly foreign interlocutor. In fact, a strange correlation may be that those who face the harshest retribution if exposed probably have the information most desired by policymakers.

Diplomats might also have additional future trouble engaging foreign interlocutors and one can envision why. Diplomats may meet privately with each other and may say some strikingly undiplomatic things in order to get past public posturing and move forward a bilateral issue of concern. It is the job of the diplomat to honestly relate the information provided by his interlocutor to his capital and he would naturally include the name and position of his interlocutor along with his interlocutor's unvarnished remarks. In the era of mass leaks, foreign government officials might think twice about sharing frank thoughts with their counterparts if they think what they say will be on the Guardian, Al Jazeera, or WikiLeaks tomorrow. For instance, German Free Democrat Party (FDP) member Helmut Metzner was identified in a WikiLeaks cable as providing candid information to the US Embassy in Berlin about German government coalition negotiations in 2009, according to a British press account. Metzner was fired from his senior party position as Chief of Staff to the FDP chairman in light of his efforts to keep US officials apprised of German political developments (Traynor, 2010). Perhaps with the Metzner case in mind, US Former State Department Undersecretary for Management, Patrick Kennedy, characterized Chelsea Manning's disclosures as having a 'chilling effect' on foreign officials (Gosztola, 2013). If the practice of diplomacy requires trust and discretion, how much more difficult is the task for intelligence officers?[4]

The real question for the Manning case, beyond the damage of what information he has revealed, is the potential value to policy makers of the intelligence that will not be collected. It is the discreet conversation with a

potential cooperative source that will not happen that is the intelligence price to be paid. To be sure, Manning did not have access to CIA operational cable traffic[5] (the internal communications of the National Clandestine Service, see Hosenball, 2009), but if she had it, chances are he would have provided it to WikiLeaks (Shane and Lehren, 2010); and the cost in human lives would have been dramatically higher, thus the crisis of confidence in global, and particularly American, human intelligence sources.

CIA takes the protection of source identities extremely seriously (see Kimball, 2007: 63–67) and even in a 'need to share' culture, Manning did not have access to this sort of information.[6] But does a potential future human intelligence agent know exactly the types of cable traffic to which a low level Army analyst may or may not have access? Or rather, might he assess that people like Manning could know his identity? What might he calculate the chances to be that his name could be buried somewhere within 700,000 classified US government cables? Or what about Snowden's treasure trove that is estimated to include upwards of 1.5 million documents? (Kloc, 2014). A dedicated counter-intelligence service would surely invest the time and energy in combing through tens of thousands of cables to find – and connect – dots that would lead to the exposure of sources as was vividly illustrated by the Iranian revolutionary students who painstakingly reconstructed shredded US Embassy Tehran cables in 1979. Former Defense Secretary Robert Gates concluded, 'I spent most of my life in the intelligence business, where the sacrosanct principle is protecting your sources. It seems to me that, as a result of this massive breach of security, we have considerable repair work to do in terms of reassuring people and rebuilding trust, because they clearly – people are going to feel at risk' (Mick, 2010).

The next Oleg Penkovsky to volunteer to the CIA must be even more courageous than the last one. He would have to be in an era where it appears questionable whether America can keep its secrets from the front pages of major media outlets and the Internet. In fact, the next Penkovsky may well wish to volunteer his services but may be reticent lest his identity (or source-revealing information traceable back to him) be included in a possible deluge of American, South African, or other country's classified information. To secure their reputations in the digital age, intelligence agencies must satisfy both their official liaison partners as well as their clandestine sources that they can continue to protect sensitive information. Before the cyber age, mass disclosure of classified information was never part of the risk calculus of a potential human intelligence source. Surely, it is now.

New Dimensions, Same Craft

Moving forward, will technological collection types such as SIGINT, ELINT, OSINT or SOCMINT supplant HUMINT in the digital age? Emphatically, no. No more than cyber operations will replace traditional military operations will digital or cyber capabilities supplant HUMINT. To be sure, technological innovation will add new capabilities as well as add new challenges to HUMINT

operations. It will further enable some types of operations, and cause a reassessment of the necessity or wisdom of other HUMINT operations. Challenges such as rampant biometrics and data mining will need to be dealt with, as will the ease with which even a curious person with an internet connection and search engine can seriously challenge an operations officer's cover. Further, social media will present both counterintelligence problems and positive intelligence opportunities for intelligence and security agencies. Despite the remarkable capabilities of encryption and the dark web, cyberspace cannot be the only world in which agents meet with their handling officers. Moreover, the challenges of hacking, phishing, and mass leaks have the potential to derail on-going intelligence operations and preclude future ones. To these, there are no easy solutions, but certainly any solutions will involve more than just the intelligence community – these are national and international problems that require as much innovation and creativity as the technologies that enabled them. In the cyber era, HUMINT will become even more complex, and case officers, their managers, and their political masters will need to understand the significant role of technology in their operations, the creative and persistent counterintelligence threats, and how intelligence collection is evolving faster than ever before.

Notes

1. 'Gray literature' is information, usually printed, that is not secret or otherwise classified but may be restricted by the author or recipient in some way. Conference proceedings and scientific papers are examples of this.
2. This is not a break with previous counterintelligence practice in such situations, but the real-time ease of checking the story as relayed gives the advantage to the counterintelligence service.
3. There are nearly unique exceptions to this rule, such as the handling of FBI Agent Robert Hanssen. Hanssen never met his Soviet/Russian handlers in person, but as a professional intelligence officer, he could dictate the terms and his information was beyond reproach.
4. The focus here is the particular added challenge for intelligence officers who deal in the clandestine collection of secrets such as the plans and intentions of adversarial governments.
5. The highest level of classification that Manning revealed was 'Secret'. CIA operational cables carry additional access code words and handling controls beyond 'Secret' that Manning's disclosures did not include.
6. CIA source identities are sacrosanct and they are exempt from FOIA requests. See http://www.foia.cia.gov/frequently-asked-questions.

Bibliography

Burkett, Randy (2013) 'An Alternative Framework for Agent Recruitment: From MICE to RASCLS', *Studies in Intelligence*, 57(1), pp. 7–17.

Campbell, Stephen H. (2013) 'Intelligence in the Post-Cold War Period: The Impact of Technology', *The Intelligencer*, 20(1), pp. 57–65.

Clark, Colin (2014) 'Biometrics May Mean the End of a Spy's Disguise', *Breaking Defense*, 20 October. http://breakingdefense.com/2014/10/biometrics-may-mean-end-of-the-spys-disguise/.

Cummings, Charles (2015) 'What's the Point of Spies?' *The Telegraph*, 16 June. http://www.telegraph.co.uk/culture/books/bookreviews/11648193/Whats-the-point-of-spies.html.

Gannon, John (2001) 'The Strategic Use of Open-Source Information', *Studies in Intelligence*, 45(3), pp. 67–71.

Gewirtz, David (2015) 'After OPM Breach, Snowden and Manning are Just the Beginning', *ZDNet*, 15 June. http://www.zdnet.com/article/after-opm-snowden-and-manning-are-just-the-beginning/.

Gosztola, Kevin (2013) 'The State Department & the 'Chilling Effect' Caused by Bradley Manning's Release of Diplomatic Cables', 5 August. http://dissenter.firedoglake.com/2013/08/05/the-state-department-the-chilling-effect-caused-by-bradley-mannings-release-of-diplomatic-cables/(blog).

Hosenball, Mark (2009) 'To Disclose Or Not To Disclose: A Fight Inside The CIA', *The Daily Beast*, May 29. http://www.thedailybeast.com/newsweek/2009/05/29/to-disclose-or-not-to-disclose-a-fight-inside-the-cia.html.

Kimball, Warren F. (2007) 'Arguing for Accountability: Openness and the CIA', *Studies in Intelligence*, 10(1), pp. 63–67.

Kloc, Joe (2014) 'How Much Did Snowden Take? Not Even the NSA Really Knows', *Newsweek*, 9 June. http://www.newsweek.com/how-much-did-snowden-take-not-even-nsa-really-knows-253940.

Lyngaas, Sean (2015) 'How (And Why) the CIA Plans to Expand Cyber Capabilities', *Federal Computer Week*, 24 February. https://fcw.com/articles/2015/02/24/cia-expand-cyber.aspx.

Mercado, Stephen C. (2004) 'Sailing the Sea of OSINT in the Information Age', *Studies in Intelligence*, 48(3), pp. 45–55.

Mick, Jason (2010) 'Taliban Thankful that Wikileaks Exposed U.S. Allies, Vows to 'Punish' Them', *Daily Tech*, 30 July. http://www.dailytech.com/Taliban+Thankful+That+Wikileaks+Exposed+US+Allies+Vows+to+Punish+Them/article19221.htm.

Omand, David, Jamie Bartlett and Carl Miller (2012) 'Introducing Social Media Intelligence (SOCMINT)', *Intelligence and National Security*, 27(6), pp. 1–23.

Reuters (2015) 'Anthem Says at Least 8.8 Million Non-Customers Could Be Victims in Data Hack', 24 February. http://fortune.com/2015/02/24/anthem-says-at-least-8-8-million-non-customers-could-be-victims-in-data-hack/.

Shane and Andrew E. Lehren (2010) 'Leaked Cables Offer Raw Look at U.S. Diplomacy', *New York Times*, 28 November. http://www.nytimes.com/2010/11/29/world/29cable.

Smith, David (2015) 'South Africa Scrambles to Deal with Fallout from Leaked Spy Cables', *The Guardian*, 24 February. http://www.theguardian.com/world/2015/feb/24/south-africa-scrambles-to-deal-with-fallout-from-leaked-spy-cables.

Takala, Rudy (2015) 'Cyberexpert Says OPM Hack Affected Hundreds of Millions', *Washington Examiner*, 20 August. http://www.washingtonexaminer.com/cyberexpert-says-opm-hack-affected-hundreds-of-millions/article/2570560.

Traynor, Ian (2010) 'Wikileaks Cables Claim First Scalp as German Minister's Aide Is Sacked', *The Guardian*, 3 December.

UK Ministry of Defense Announcement (2011) 'MOD Launches Personal Online Security Awareness Campaign', 1 June. https://www.gov.uk/government/news/mod-launches-personal-online-security-awareness-campaign.
United States Department of Defense (2015) 'Social Media Education and Training', http://www.defense.gov/socialmedia/education-and-training.aspx/.

Dr. David V. Gioe is Assistant Professor of History at the United States Military Academy at West Point, where he also serves at the History Fellow for the Army Cyber Institute. Previously David spent a decade in the US intelligence community, including multiple overseas tours as a CIA case officer. This chapter reflects his analysis and does not necessarily reflect the view of any US government department or agency.