DISRUPTING ARMED GROUPS: HUMAN INTELLIGENCE STRATEGIES[1]

by

Jeffrey H. Norwitz

The future of war, conflict, and societal unrest will be increasingly defined by non-state actors who reject traditional notions of sovereignty, national identity, and international norms of behavior. This chapter will suggest applications for human source intelligence in order to neutralize emerging challenges from dangerous armed groups and related movements.[2] The chapter explores ways to influence decision-makers who lead criminal and terror organizations so as to effectively inhibit their ability to operate. Then, the chapter discusses how individuals within the group can be manipulated causing friction or fissures among members thereby reducing group cohesion and effectiveness. Organizational and group behavior provides a perspective on where to find or develop these fissures. Operational human intelligence techniques provide the leverage to exploit these fissures in order the break the structure.

Let's be clear about the outcome. Outright destruction, annihilation, or eradication of armed groups is probably impossible. We can however influence the behavior of organizations and their members thereby reducing the threat. This is an ongoing struggle with long-term objectives. Continued vigilance is part of any influence strategy. Methods must be uninterrupted. Tactics must be relentless. And victory is only temporary. In truth, the struggle is unending.

Armed Groups Defined

What exactly is an armed group? The two words *armed* and *group* are clear enough and, when used together, conjure up any manner of mental images. Unshaven men in Western attire holding dirty rifles with straps of bullets hanging from their shoulders. Prohibition-era bank robbers standing on the running boards of a Ford Phaeton with Thompson machine guns tucked under their arms. Wild-eyed horsemen wearing furs charging across a Mongolian plateau. Somali teenagers hanging from the back of a speeding truck, hoisting AK-47 assault rifles. Heavily armed men in sunglasses escorting a political figure from an airplane.

For our purposes, this chapter will consider armed groups to include classic insurgents, terrorists, guerrillas, militias, police agencies, criminal organizations, war-lords, privatized military organizations, mercenaries, pirates, drug cartels, apocalyptic religious extremists, orchestrated rioters and mobs, and tribal factions.

Armed Groups Are Human Networks

Understanding group dynamics begins with the leader. In any group, someone is in charge. They may appear to share power but upon close examination, there will be a dominant decision-maker. If we are to effectively influence how the group behaves, we need to first identity the leader and then study their background, what they believe, where they get their information, and how they relate to others. Influencing the activities of leaders cannot be achieved without understanding what makes them tick.

Studies of leaders in a political context suggest there are four distinct considerations dealing with how leaders receive, and are therefore influenced by, information.[3] The first consideration looks at ***personal characteristics*** and focuses on the leader's self-image to include confidence, ideology, philosophy, motivation, beliefs, values, as well as likes and dislikes. Other

personal characteristics deal with background and skills. Among them are age, where the leader was born, raised, and relevant socialization factors. Also included are marital status, the nature of the marital relationship, and relationships with immediate and extended family, and the nature of those relationships. Interests, schooling, including the type of student the leader was and focus of study, former positions held, and key personal associates are also important to know. It's crucial to understand the leader's norms which include their views on how individuals should behave, impertinent behaviors, words or phrases that can be insulting, and views of the role of minority or majority groups.

The second consideration looks at the leader's ***operating environment***. This includes how the leader came to power, groups or individuals that constrain the leader, and whether or not the leader challenges restraint. Incorporated in this are perceptions about others, the leader's degree of ethnocentrism, and distrust for others. We want to know how the leader views others and also how others view the leader. The focus is on existing perceptions about the leader on a variety of perceptual planes and at a more basic level, whether the leader is liked or disliked and by whom. Also relevant is how the leader views their defined constituency or followers. Finally, the leader's operating environment includes sources of finance and likelihood of corruption.

The third consideration deals with the leader's ***advisory system***. Some of the most significant people are the leader's advisors. When examining the leader it is important not to become caught up in the formality of line and block charts because they may not really tell us who is influential. Rather, we have to look at the leader's formal and informal network of advisors who may change over time. For a variety of reasons advisors can also fall out of favor or new ones may emerge. When the most influential advisors are identified, the potential spin, personal agenda, or filtering of information by advisors should also be discerned. Some leaders may not even care about advice from others. As a result, they may pay lip service to their advisors and instead, consider themselves the ultimate authority on all issues. Last is the degree of control the leader needs over the policy process and their interest and level of policy expertise.

The final consideration looks at the leader's ***information environment***. This involves the degree of complex thinking the leader exhibits. For example, some individuals are open to information, deal well with ambiguity, and have an ability to grasp nuance. These types of leaders usually want diverse information. Those who lack in cognitive complexity are black and white thinkers. They are essentially closed to conflicting information, do not seek out alternative views, and do not care about supplementary information. Whether complex or not, the type of information the leader pays attention to, the sources of this information, and how the leader prefers information to be presented, will aid in designing an influence strategy.[4]

Religion and Leadership Thinking

Contemporary circumstances demand additional discussion of *religion* as it pertains to how leadership thinking is shaped. Within the context of this chapter, spiritual convictions have their origins in all aforementioned areas of consideration for how leaders receive and process information. For instance, personal characterizes of upbringing, family, values, and socialization are strongly influenced by the presence or absence of religious principles. The operating environment as evidenced by a leader's view of others, constituency, and followers can reveal religious influence or lack thereof. Dogmatic or strident rule-sets of a leader's advisory system

may echo prescriptive righteous devotion. Likewise, a leader may deal with complexity by turning to pious spiritual doctrine as a way of managing ambiguity.

This chapter is concerned with the degree to which religion drives a leader's decision-making because if we are going to influence leadership behavior, we must consider the extent theology drives behavior. The reader is strongly encouraged to study the particular religion if it is an important decision-driver for a target leader or armed group.

Human Intelligence about Human Networks

Armed groups and criminal enterprises are human-centric activities. In other words, while groups may embrace technology in weapons and communications, they are essentially *humans* doing things that *humans* do in ways that *humans* do them. Psychology, sociology, and anthropology inform us on human behavior in general. But particulars about a leader, group, and its members must be individually discerned. Human intelligence is the answer.

Human intelligence, commonly abbreviated as HUMINT, is that which is derived from human sources. In contrast to intercepted phone conversations (signals intelligence), photos (imagery intelligence), and other technical or scientifically derived intelligence; HUMINT is the cornerstone of intelligence work and reveals secrets of the mind. Let's examine HUMINT in a bit more detail. Mark Lowenthal, with twenty-seven years of experience as an intelligence official in the executive and legislative branches of government and in private sector offers;

> HUMINT is espionage – spying – and is sometimes referred to as the world's second-oldest profession. Spying is what most people think about when they hear the word intelligence, whether they conjure up famous spies from history such as Nathan Hale or Mata Hari (both failures) or the many fictional spies such as James Bond.
>
> HUMINT largely involves sending agents to foreign countries, where they attempt to recruit foreign nationals to spy. Agents must identify individuals who have access to the information that we may desire; gain their confidence and assess their weaknesses and susceptibility to being recruited; and make a pitch to them, suggesting a relationship.
>
> For intelligence targets where the technical infrastructure may be irrelevant as a fruitful target – such as terrorism, narcotics, or international crime, where the signature of activities is rather small – HUMINT may be the only available source.
>
> HUMINT also has disadvantages. It cannot be done remotely, as is the case with various types of technical collection. Likewise, it requires proximity and access and therefore must contend with the counterintelligence capabilities of the other side.
>
> Some critics argue that [HUMINT] is the most susceptible to deception. The bona fides of human sources will always be subject to question initially and, in some cases, never be wholly resolved. Why is this person offering to pass information – ideology, money, revenge? Is this person a double agent who will be collecting information on your HUMINT techniques?[5]

HUMINT provides an otherwise unattainable window into the personality, emotional make-up, and innermost secrets of those who are being targeted for influence operations. HUMINT is unmatched in its ability to uncover this often private, subtle, and privileged information about individuals and groups who we want to influence. According to Lowenthal;

> HUMINT involves the manipulation of other human beings as potential sources of information. The skills required to be a successful HUMINT collector are acquired over time with training and experience. They basically involve psychological techniques to gain trust, including empathy, flattery, and sympathy. There are also more direct methods of gaining cooperation, such as bribery, blackmail, or sex.[6]

As it pertains to recruiting sources inside armed groups, experience shows that regardless of culture, language, age, gender, political, religious, or educational background; the four most common motivators for people to deceive trusted comrades are 1) greed, 2) anger or revenge, 3) thrill or excitement, and 4) visions of self-importance (ego, vanity). Others simply volunteer their services for ideological motives. HUMINT officers perfect ways to exploit each of these scenarios and literally develop scores of persons acting as psychological hostages. Even in those relationships that seem to start with full cooperation; a measure of coercion will be contrived in order to "hook" the source lest he or she develop remorse.

Professional intelligence officers who specialize in human source intelligence are customarily called "HUMINTers." They are not intelligence analysts nor are they staffers who write reports. Rather, HUMINTers are operational people, specially trained and highly skilled to blend into any environment wherein human relationships are the essence. Human source intelligence work is part clinical psychologist and part theatrical actor. As you read this, throughout the world, thousands of men and women are quietly gathering intelligence, manipulating human relationships, assessing likely informants, and influencing leaders.

Thus the world of HUMINT is in a continuous reciprocating ballet of spy vs. counter-spy, sometimes using very different rule-sets. For example, a democratic nation will, by the very nature of the form of government, follow a set of norms embodying ―rule of law‖ and human dignity, unlike some adversaries, which justify ends by any means. Therein emerges a tension when armed groups violently attack democracies. Yet measured state responses are a necessary moral obligation.

Intelligence Operations in a Democracy

One of the quintessential thinkers on intelligence matters and democratic norms of behavior is Stansfield Turner, retired Navy Admiral and former Director of Central Intelligence (1977-1981). Citing a perceived "lack of discussion of how our democracy affects and is affected by what we do to deter terrorism," Turner wrote a book on the very subject.[7] His conclusions:

> One of the key elements for us in combating terrorism is international cooperation…If we are going to defeat international terrorism—not just Osama bin Laden but the broader sweep—we will need an analogous multinational program that will put pressures on the movement of individuals terrorists and on their bases of support in our societies. Only when we truly analyze which alternatives promise the best payoffs will we begin moving towards a long-run solution to terrorism. And only then will we deserve the respect that

> we'll need to lead the responsible nations of the world in a coordinated campaign to suppress this scourge against mankind. Terrorist are not invincible: the Zealots, Assassins, and others were suppressed in time. Today many countervailing strengths come from the very fact that we have a democratic system. But that means we need public understanding of our options for curtailing the current wave of terror and the wisdom to avoid actions that might undermine the democratic process we are defending.[8]

Security professionals must be proactive to frustrate threatening organizations. We have to go after the group, not wait for the group to attack us. We are often too reactive in our dealings with armed groups. Yet we cannot allow open society and freedoms to become a force-multiplier for our enemies. For example, democracies and representative forms of government are characterized by transparency, free press, the ability to dissent, accountability, rule of law, and international responsibilities under treaties and other sovereign obligations.

An enemy which is committed to an opposite political and moral framework can cleverly operate with impunity in an open society enjoying the tolerance of democratic laws and norms. At the time of their choosing an enemy can emerge from within the populace having planned, recruited, resourced, and executed an attack right under the noses of the target population. Because of the constraints faced by representative democracies which recognize the rule of law, they are often perceived as weak by the adversary who follows no set of laws.[9] Furthermore, proactive approaches, especially those using human source networks to attack human source networks, require the utmost in secrecy. And this runs counter to a free, open press and an informed population. Nonetheless, the ability to break armed groups will be proportional to the ability for security forces to operate clandestinely within a legal framework. This then begs the quintessential question, *how much openness is too much?* In other words, to what extent should our intelligence operations and capabilities be subject to public scrutiny by the media and by the public?[10]

In 2013, the American public and the world became aware of highly classified and decidedly sensitive information about the capabilities of the National Security Agency (NSA) to conduct surveillance of electronic communications. Edward Snowden, a former NSA worker with access to the agency's secrets, disclosed the inner workings of NSA to foreign journalists and later the Russian government in violation of U.S. espionage laws.[11] His supporters hold that Snowden is a hero in that he disclosed the extent to which private communications can be collected by the NSA. Experts claim that Snowden did irreparable damage to American intelligence gathering thereby making the nation more susceptible to attack.[12]

Thinking about the Law

In point of fact, based on past abuses as investigated by the Senate Church Committee[13] in 1975, there are laws and Presidential orders which clearly define how America conducts intelligence activity and still protects constitutional underpinnings. Some of the key legal boundaries by which American intelligence agencies must adhere are articulated in Executive Order 12333, "United States Intelligence Activities"; DoD Directive 5240.1 DoD, "Intelligence Activities"; National Security Act of 1947, [50 U.S.C. § 401]; Foreign Intelligence Surveillance Act (FISA) of 1978 [50 U.S.C. §§1801-1811, 1821-29, 1841-46, and 1861-62]. But what about the future as it relates to the law? Do we have the necessary legal tools to disrupt human networks which pose a national security threat?

Shortly after the September 11, 2001 attacks, I wrote a foretelling article entitled, "*Combating Terrorism: With a Helmet or a Badge?*" In it, I examined the underlying challenges of treating terrorism as a crime and thereafter, the efficacy of America's concept of judicial justice in the face of 9/11.[14] The article begins with a fictitious scenario wherein Osama bin Laden[15], with a team of defense attorneys, surrenders himself to American authorities and thereafter starts a cascade of legal challenges in court. That vexing scenario is unfortunately what has emerged. A senior prosecutor in the Department of Justice, speaking at the U.S. Naval War College, opined that America was no closer to clarifying Constitutional complexity dealing with detained terrorism suspects than on 9/11. For example, even after the Supreme Court rendered opinions in Rasul v. Bush1[16], Hamdi v. Rumsfeld[17], and Hamdan v. Rumsfeld[18], they seemingly confused the matter even more in Boumediene v. Bush[19] which held that prisoners at Guantanamo had a right to the *habeas corpus* under the United States Constitution. This meant that detainees could contest their continued detention without having been charged with a crime. As of this writing, sixty-one men remain jailed in Cuba.[20] [21]

Craig H. Allen, Judson Falknor Professor of Law at the University of Washington and formerly the Charles H. Stockton Chair in International Law at the U.S. Naval War College writes about the future legal challenges posed by enemy human networks.

> The threats posed by armed groups plainly challenge our traditional paradigms for preventing and controlling large-scale violence. Conflicts with armed groups such as Al Qaeda—whose members are not found on the battlefield, who "hide in plain sight" among civilians, and who flout the principles of distinction and humanity that are so central to the law of armed conflict—do not fit nicely into the "war" construct, and yet the magnitude of the risk posed by those groups does not fit within our traditional understanding of "crime." In short, the threat is too lethal to be treated as a mere crime and too private to be called a war.
>
> Perhaps it is time to reject the binary thinking that fuels the present destructive debate and acknowledge that the existing regimes do not, individually or collectively, adequately address the present needs for an ordered approach to the myriad forms of contemporary large-scale violence by armed groups. Such a declaration is, perhaps, the indispensable first step in formulating a new and more flexible regime that will allow us to harness law as an ordering force in what has become an increasingly disordered world.
>
> But many are reluctant to take seriously any reform proposals, whether at the international or national level. They argue that there is not sufficient international will or cohesion to develop and ratify a new international regime. Perhaps they also fear that an admission that the existing regime does not cover the present situation would be an invitation to an unprincipled nation or its executive to exploit the gap, while arguing that the law does not constrain it. On the national level, the fierce and debilitating partisan divide and the dizzying sine curve of public opinion cast serious doubt on the prospects for any reform, particularly one that would establish a basis for preventive detentions and provide for criminal trials with fewer protections than those afforded to ordinary criminal defendants.

> In the final analysis, program analysts and policy makers must determine which approach best provides the optimal level of security, liberty, and protections for the accused. More than a half century ago Abraham Maslow reminded us that in the hierarchy of human needs none is more fundamental than security. If security is defined as the freedom from violent acts, an effective security regime must do more than merely respond to attacks; it must also prevent them when possible—particularly those that might include unleashing a weapon of mass destruction.[22]

For the purpose of this chapter, the reader is encouraged to remain abreast of rapidly changing domestic, military, and international law as it relates to definitions of criminals, combatants, and the use of force to disrupt armed groups.

Neutralizing Armed Groups

At some point in every individual's life, he or she joins a group. This can be a weekly coffee get together with friends or colleagues, the boy scouts, a political party, the military, which bring people together for a common purpose. Individuals seek interaction with others and want a shared identity. Humans after all are tribal by nature. One way to achieve this is to join a group. Once a person is part of a group they acquire a shared group identity. This comes with constraints, obligations, responsibility, and commitments. While of course personal identity is still important, the member also adopts a group identity. Outward evidence may be clothing, tattoos, distinct language, or even ways of walking. Even though groups are made up of individuals, certain group dynamics can and do affect the behavior of individuals. The group becomes a powerful shaping force.

According to some social psychologists, when individuals join groups, previous group identities are stripped away. [23] Moreover, individuals who join groups attain a level of anonymity. Writing for bigthink.com, Harvard lecturer David Ropeick says, "Tribalism is pervasive, and it controls a lot of our behavior, readily overriding reason."[24] Personal accountability and responsibility shifts from the individual to the group. Group members often behave in ways very different from when they were unaffiliated. Sometimes when individuals join secretive groups, they are pressured to sever certain outside connections. The purpose is to protect the group from unwanted scrutiny. When individuals are being assessed for recruitment, group indoctrination is important and group propaganda is central to this indoctrination. The group central messages are constantly reinforced. Indoctrination is an on-going process and individuals are expected to put the group above everything else.

The group, with its like-minded members, becomes the individual's identity, and the group is now the new family for the recruit. There are indeed perceptions about what a prototypical member should be. Therefore, a recruit is expected to conform to and obey the norms of the group and participate in group behavior. These norms are usually articulated by those in central leadership positions and pressure to conform comes from all levels and members. However, for some, their attraction to the group fades. Their level of commitment dissipates. They become marginalized and no longer feel a sense of camaraderie. These are the potential deviants we can exploit and skillful human intelligence tells who they are.

Group Fissures

Groups are not always cohesive. They often suffer from internal discord or fissures. The most significant fissure points which derail the functioning of groups are conflicts between members. Research suggests that group dissention can lead to power struggles between members and that differences of opinion can result in factional disputes. [25] These power struggles cause factions to emerge. Power struggles can result in splits so severe that individuals leave a group and form another, often with competing agendas. Furthermore, power struggles can destroy a group causing members to turn on one another and even eliminate rivals. But conflict between individuals is not necessarily always because of power. Members can have basic personality conflicts and may become marginal or even deviant affiliates that threaten group cohesion. At some point individuals seek to leave the group if this tension exists, or may be pressured to leave by other more prototypical members. Thus, any type of individual conflict in the group is an exploitation opportunity for an informational influence campaign because when tension occurs, the level of commitment of certain members may be shaken. Any type of unhappiness is exploitable, and where none exists, it can be created.

Groups that must maintain a high security posture go to great lengths to ensure internal security. Groups warn members that they are always the target of security forces and must be vigilant to protect against such penetration. Groups tend to continually watch their members for potential betrayers. Armed groups tend to create their own counterintelligence wings not only to stop penetration from the outside, but to find betrayers within. This can and does create potential for serious mistrust between members. We can seize on and exploit mistrust that already exists and we can also create distrust between members.

Research further suggests that there are often considerable policy and procedural fractures in groups.[26] Unless the group is highly cohesive, there are often disagreements about the way things are done and the methods and goals of the group. These disagreements can and do create rifts between members of groups. From there, cliques may form, and members will compete with each other. However, more dominant cliques or individuals may also have the power to expel others. On the other hand, individuals may leave the group, form another, and press forward with their agenda. Thus we can facilitate the fracture, exploit it, destabilize a group, and if new groups are formed, ultimately cause them to turn on each other.

Identifying marginal and deviant members is extremely important to any informational influence campaign. Groups have norms and members are expected to follow them. Marginal and deviant group members are problematic because they don't conform and therefore threaten the cohesiveness of the group. They also threaten the obedience of other members and promulgate irregular behavior. Additionally, marginal members and deviants often bring negative attention to the group. On occasion, group norms require participation in violence as a vetting process. Members may fail or refuse to take part. Marginal members and deviants who cannot be rehabilitated are dealt with through conformity measures or they are expelled or killed. Once questions are raised, groups tend to want to find the answers. Suspicion is then cast on members of the group. And when suspicion is raised, the sense of threat becomes heightened. Members tend to turn on each other. Turncoats are not taken lightly in armed groups. They violate norms and challenge the cohesion of the group. They are the betrayers.

Marginal members and deviants are the dream of an influence operator. For one, deviants are always on the fence. While the group may tolerate them, there will come a point when deviants push the limits too far. The reasons for their behavior are varied, but the bottom

line is that deviants don't like to follow the rules. It is important to find out why, and then use these non-conforming members to cause dissention in the group. Again, human intelligence informs us of the situation.

Strategies for Exploitation

One of the first jobs of an influence planner is to identify those weak links in the group. We can exploit these fissures in various ways. We can seize upon already deviant behavior and twist the circumstances to our advantage. Or we can encourage such behavior which creates dissension and individual defection from the group. Or we can manufacture the appearance of deviance, even when none exists. Imagination and deviousness are all that are necessary to exploit fissures.

One of America's most successful yet unheralded HUMINT intelligence officers is Duane R. "Dewey" Clarridge, retired senior official of the Central Intelligence Agency (CIA). For 32 years, Clarridge was a legendary CIA operations officer deeply involved in many of the Agency's most important covert actions in the cold war.[27] Clarridge ran some of most clandestine yet indispensable campaigns of the twentieth century to disrupt, influence, and in some cases totally destroy armed groups with aims inimical to the United States.

Commonly referred to a covert action, Clarridge's activities showcase the effectiveness and efficacy of disruption and influence campaign strategy.[28] Working against the deadly Abu Nidal Organization (ANO), Clarridge headed the CIA Counter Terrorism Center (CTC) in 1986. Based on the recruitment of an ANO member and good analysis, Clarridge's shop developed superb intelligence about Abu Nidal himself. In his autobiography, Clarridge shares a rare glimpse into the mind of a master of influence operations.

> From our ANO agent penetration, we began to accumulate a lot of knowledge about Abu Nidal's "diplomacy" (internal and external behavior) and his financial dealings which led us to ANO activists and backers in France, England, and Germany. Abu Nidal had an extensive commercial network in Eastern Europe, Greece, Cyprus, Yugoslavia, and to a lesser extent, Western Europe. These businesses had three purposes – their profits financed the organization; their structure provided cover and support apparatus for terrorist operations; and they gave cover to Eastern European intelligence services in some instances. Under the umbrella of these "legitimate" businesses, the ANO could move and hide funds, acquire and transports weapons, and arrange meetings and liaisons.
>
> I arrived at the conclusion that the best way to attack Abu Nidal was to publically expose his financial empire and his network of collaborators. We decided to go for the public expose, revealing the support of some countries for the ANO in an effort to embarrass or pressuring them into desisting. I proposed the Department of State issue an explosive little tome called *The Abu Nidal Handbook* which laid out chapter and verse on the ANO, its members and accomplices, and its crimes. It even had an organizational chart.
>
> The publication of our handbook had the desired effect. Governments in Europe squirmed, but they terminated their dealings with Abu Nidal. Even the Poles and East Germans divorced themselves from him. We decided to make recruitment pitches to ANO personnel in various countries. Most of the approaches did not result in agent

penetrations of the ANO but our pursuit of Abu Nidal's organization and personnel eventually paid off in a very different way.

Seeing his financial empire under attack and listening to reports of CIA efforts to recruit his cadres, Abu Nidal was aware that we were coming after him and his people. He, like many in his line of work, was paranoid. CIA fueled his hysteria over plots against him – feeding fear to a paranoid is something we know how to do. Not surprisingly, Abu Nidal panicked. Those who reported having been approached by us were not rewarded for their loyalty, because Abu Nidal never quite believed that anyone in his group had turned us down. Their loyalty was suspect thereafter, and punishment was torture and death.

By 1987, a fearful Abu Nidal had turned his terror campaign inward. The ANO was starting to drown in the blood of its disciples. A simple allegation was sufficient; usually there was no investigation. Accused followers were tortured to confess, then executed on the basis of the confession. After the effective ANO apparatus in southern Lebanon fell under suspicion, over three hundred hard-core operatives were murdered on Abu Nidal's order. On a single night in 1987, approximately 170 were tied up and blindfolded, machine-gunned, and pushed into a trench prepared for the occasion. Another 160 or so were killed in Libya shortly thereafter. Distrust reached high into the politburo ruling the ANO. Even his lieutenants began to believe he was insane. Abu Nidal's paranoia, fed by our crusade against him, caused him to destroy his organization.[29]

Creating fissures with marginal members or deviants involves fabricating the aura of dissension, even when it doesn't necessarily exist. We are going to play upon the penchant of individuals to distrust the activities of others when security is paramount. The perception merely needs to be created that something isn't quite right with the members of the group.

Implementation of an Influence Strategy

Let's suppose we want to create an atmosphere of suspicion around a member who has access to the group leadership but for some reason, is not considered part of the inner circle. Our goal is to drive the target into our camp by causing such chaos within the group that the target has no choice but to seek sanctuary with us. We start our influence operation with surveillance by which we establish the target's routine so we can predict travel patterns. If by car, we're in luck. Choosing a spot where there will be plenty of witnesses, we arrange for a police car to stop our subject in what appears to be a normal traffic stop for some sort of moving violation. It will be important that such a traffic stop create as much commotion as possible cleverly designed to draw the public's attention to the activity. Disrupt the traffic flow. Use lights and siren. Use loud speakers. Next, our collaborating police officer is seen walking back and forth from the subject's car to the police car. The officer is seen talking to the subject for an inordinate amount of time. The subject is asked to join the officer in the police car where they are seen talking even more. As they walk back to the subject's car, our theatrical officer is seen laughing and patting the subject on the back after which the subject drives away (totally confused) but with the officer waving.

If the scenario is played out with the right audience, word of the event will quickly get back to the group and thereafter, the subject member we've targeted will be under great

suspicion – totally unable to explain the police behavior. This will appear even more traitorous. If a similar contrived "friendly" association with law enforcement can be repeated, the target member will eventually realize they are being manipulated by police but it will be too late to convince group peers. With the proper incentive and approach, there is a good likelihood our target will become our asset in return for protection. The seeds of doubt will have been planted in the group it will cause them to look at other members as suspect; perhaps the member's confidants, allies and so forth.

Operational tactics to break armed groups often, at some point, demand direct contact with a group member who our analysis suggests is most vulnerable to recruitment or can be manipulated to our advantage. Finding and vetting likely candidates is an ongoing process for human intelligence officers. The more recruited sources one has, the greater success at having the right source at the right time.

Dr. Norman A. Bailey of The National Security Studies Center at Haifa University writes about introducing agents of influence into an organization to disrupt cohesiveness between leadership and membership. But to be of any use, according to Bailey, an agent must actively participate in operations developing guaranteed trust within the higher echelons. This likely means participating in acts of violence against civilians. However effective, this may be unacceptable for the potential agent and the relevant agency itself. [30]

A final word about implementation strategies. Nothing can match the value of having a witting or unwitting person inside a secretive organization. This provides an otherwise unattainable window into the personality, emotional make-up, and innermost secrets of those who are being targeted for influence operations. Human intelligence is unmatched in its ability to uncover this often private, subtle, and privileged information about leaders and groups which we want to disrupt. In summary, strategies to exploit individual and group fissures in order to disrupt armed groups most often leverage the skills and operational tactics of human intelligence practitioners.

Social Media and Human Intelligence

Social media is becoming so synonymous with in-person communications such that it cannot be overlooked as a method to influence decision makers. Using web-based technologies, social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration.[31] Examples include Facebook®, Twitter®, Google+®, LinkedIn®, Reddit®, and Pinterest®. Social media differs from traditional information sources because it is designed to exchange information in a back-and-forth manner or become a one-way information feed. This makes social media a unique tool to steer decision makers.

Within the world of social media, there are persons who are known as "influencers" defined as individuals who have the power to affect decisions of others because of their (real or perceived) authority, knowledge, position, or relationship. An influencer is an individual whose actions and opinions carry more weight with their colleagues, social network and the general public than is the case with most other individuals.[32]

Within the context of this chapter, we can consider a social media influencer as a HUMINT operator. The method by which decision makers share thoughts and ideas (influence each other or become influenced by others), can be manipulated by clever use of social media. Belief systems of members and leaders of armed groups can therefore be shaped by social media to support an overall influence strategy.

Conclusion

The future is full of uncertainty and the implications are grave for the stability of security of nations who cherish freedom and the rule of law. Globalization and interconnectedness will fuel discontent in some regions while dissuading disputes in others. Armed groups are merely one vestige of mankind's struggle in an increasingly smaller world. Prevention of hostilities and rapid resolution thereof demands new solutions. This chapter suggests human intelligence can inform us about armed group leaders and become an enabler to disrupt groups thereafter neutralizing the danger from criminal and terrorist networks where, in all likelihood, the most serious threats will emerge. This is not new. George Will, the Pulitzer Prize-winning author and political scientist, said, "The future has a way of arriving unannounced." The purpose of this chapter is to prepare ourselves for when we discover, unexpectedly, that the future is here.[33]

****

Jeffrey H. Norwitz is a retired federal special agent with more than four decades experience in complex criminal, counterintelligence, and counterterrorism investigations. Following Army service as a Military Police Captain, Mr. Norwitz entered civilian law enforcement in Colorado Springs as a patrol officer. His specialties included SWAT team sniper and commander of the bomb squad. He later joined the civilian ranks of the Naval Criminal Investigative Service (NCIS) and served tours around the world including Counterintelligence Supervisory Special agent for New England. Mr. Norwitz also spent time at Camp Delta, Guantanamo Naval Station interviewing al Qaeda and Taliban fighters. For eight years he was Visiting Professor of National Security Studies at the U.S. Naval War College where he held the John Nicholas Brown Chair of Counterterrorism. He earned a graduate degree in National Security Studies from the Naval War College and was voted Eastern Kentucky University's Distinguished Alumnus in 2006. His scholarly work appears in Terrorism and Counterterrorism: Understanding the New Security Environment (McGraw-Hill: 2003), American Defense Policy 8th ed. (The Johns Hopkins University Press: 2005), Practical Bomb Scene Investigation (CRC Press: 2006), Defending the Homeland: Historical Perspectives on Radicalism, Terrorism, and State Responses (University of WV Press: 2007), Armed Groups; Studies in National Security, Counterterrorism, and Counterinsurgency (Naval War College: 2008), and Homeland Security and Intelligence (Praeger Publications: 2010). He is also widely published in professional journals and has lectured at the United Nations, to foreign militaries worldwide, and in Geneva Switzerland.

NOTES

[1] This chapter is a revision of Jeffrey H. Norwitz, "Disrupting Human Networks: Ancient Tools for Modern Challenges," in *Homeland Security and Intelligence* ed. Keith Logan. (Westwood: Praeger Publishers, 2010), 216-228.

[2] As used herein, an armed group refers to classic insurgents, tribal warlords, terrorists, guerrillas, pirates, militias, and organized criminal syndicates.

[3] The author acknowledges the contribution of Dr. Elena Mastors who collaborated on research for this chapter. Scholarly discussion of leader considerations and strategies to influence their decision-making as highlighted in this chapter can be found in Elena Mastors and Jeffrey H. Norwitz, "Disrupting and Influencing Leaders of Armed

Groups," in *Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency*, ed. Jeffrey H. Norwitz. (Newport: Naval War College, 2008), 323-341. See www.JeffNorwitz.com.

[4] For further discussion see Martha Cottam, Beth Dietz-Uhler, Elena Mastors and Tom Preston, *Introduction to Political Psychology*, (New Jersey: Lawrence Erlbaum and Associates, 2004).

[5] Mark Lowenthal, *Intelligence: From Secrets to Policy, 2nd ed.* (Washington DC: CQ Press 2003), 74-77.

[6] Ibid, 211.

[7] Stansfield Turner, *Terrorism and Democracy*, (Boston: Houghton Mifflin, 1991), xii.

[8] Stansfield Turner, *Ten Steps to Fight Terrorism Without Endangering Democracy*, (College Park: Center for International and Security Studies at Maryland School of Public Affairs, 2001): 18.

[9] A superb treatment of the challenges facing democracies to deter non-state actors is found in Yosef Kuperwasser, "Is It Possible to Deter Armed Groups?" in *Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency*, ed. Jeffrey H. Norwitz (Newport: Naval War College, 2008), 127-133. See www.JeffNorwitz.com.

[10] An example of an organization dedicated to government transparency is OpenTheGovernment.org. According to their Statement of Values, OpenTheGovernment.org believes, "[T]hat the People have a right to information held by and for our government. We believe that transparency is essential to ensuring integrity and accountability in the operation of our governing institutions. We believe that openness helps to ensure that policies affecting our health, safety, security and freedoms place the public good and well-being above the influence of special interests. Making government as open as possible also fosters confidence in representative government and encourages public participation in civic affairs, an essential feature of our form of government. For all these reasons, OpenTheGovernment.org seeks to advance the public's right to know and to reduce unnecessary secrecy in government." Accessed Aug 20, 2016, http://www.openthegovernment.org/we_believe

[11] According to publically available information, "Edward Snowden is a former National Security Agency subcontractor who made headlines in 2013 when he leaked top secret information about NSA surveillance activities. Born in North Carolina in 1983, Edward Snowden later worked for the National Security Agency through subcontractor Booz Allen in the organization's Oahu office. During his time there, Snowden collected top-secret documents regarding NSA domestic surveillance practices that he found disturbing. After Snowden fled to Hong Kong, China and met with Guardian journalists, newspapers began printing the documents that he had leaked, many of them detailing the monitoring of American citizens. The U.S. has charged Snowden with violations of the Espionage Act while many groups call him a hero. Snowden has found asylum in Russia and continues to speak about his work." Accessed Aug 20, 2016, http://www.biography.com/people/edward-snowden-21262897#aftermath

[12] The reader is urged to read U.S. Congress, House Permanent Select Committee on Intelligence (HPSCI), *Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden*, September 15, 2016. Accessed Nov 2, 2016. http://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_-_unclass_summary_-_final.pdf

[13] According to publically available information, "The Church Committee was the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, a U.S. Senate committee chaired by Senator Frank Church (D-ID) in 1975. A precursor to the U.S. Senate Select Committee on Intelligence, the committee investigated intelligence gathering for illegality by the Central Intelligence Agency (CIA), National Security Agency (NSA) and Federal Bureau of Investigation (FBI) after certain activities had been revealed by the Watergate affair." Accessed Aug 12, 2016. https://en.wikipedia.org/wiki/Church_Committee

[14] Jeffrey H. Norwitz, "Combating Terrorism with a Helmet or a Badge?" in *American Defense Policy, 8th ed*., Paul J. Bolt, (Baltimore: Johns Hopkins University Press, 2005), 424-432.

[15] Bin Laden was killed in Pakistan by U.S. Special Forces on May 2, 2011.

[16] Rasul v. Bush, 542 U. S. 466, 500–501 (2004).

[17] Hamdi v. Rumsfeld, 542 U. S. 507, 538 (2004).

[18] Hamdan v. Rumsfeld, 548 U. S. 557 (2006).

[19] Boumediene v. Bush, 553 U.S. 723 (2008).

[20] *"Guantanamo by the Numbers," Human Rights First*, accessed Aug 20, 2016, https://www.humanrightsfirst.org/sites/default/files/gtmo-by-the-numbers.pdf

[21] Information about the military detention facility at Guantanamo Naval Station, Cuba can be found here, accessed Aug 25, 2016. http://gutenberg.us/articles/Guantanamo_Bay_detainment_camp

[22] Craig H. Allen, "Armed Groups and the Law," in *Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency*, ed. Jeffrey H. Norwitz (Newport: Naval War College, 2008), 89-113.

[23] Marilynn Brewer and Wendi Gardner, "Who Is This 'We'? Levels of Collective Identity and Self Representations," *Journal of Personality and Social Psychology* 1996, Vol. 71, No. 1,83-93

[24] David Ropeik, "How Tribalism Overrules Reason, and Makes Risky Times More Dangerous," accessed Oct 5, 2016. http://bigthink.com/risk-reason-and-reality/how-tribalism-overrules-reason-and-makes-risky-times-more-dangerous

[25] Marika Rullo, Fabio Presaghi, Stephano Livi, "Reactions to Ingroup and Outgroup Deviants: An Experimental Group Paradigm for Black Sheep Effect." *PLoS ONE* 10, 5 (2015), doi:10.1371/journal.pone.0125605.

[26] Ibid.

[27] Interview with Duane Clarridge for CNN television series, *George Washington University, National Security Archive*, aired Feb 21, 1999, accessed August 10, 2016, http://nsarchive.gwu.edu/coldwar/interviews/episode-18/clarridge1.html

[28] Duane Clarridge, interview by author, July 2007. Clarridge died April 9, 2016.

[29] Duane Clarridge, *A Spy For All Seasons: My Life in the CIA*, (New York: Scribner, 1997), 334-336.

[30] Norman A. Baily, "A Grand Strategy For Winning World War IV," *The Intelligencer, Journal of U.S. Intelligence Studies*, Vol. 22, Number 2, Fall 2016, accessed Nov 29, 2016, http://acdemocracy.org/a-grand-strategy-for-winning-world-war-iv/

[31] http://whatis.techtarget.com/definition/social-media WhatIs.com® is a reference and self-education tool about information technology. The site provides readers with definitions for over 10,000 terms and over 1,000 fast references, cheat sheets and quizzes. This was last updated in September 2016

[32] Definition of Influencers, BusinessDictionary.com. WebFinance, Inc., accessed: October 10, 2016, http://www.businessdictionary.com/definition/influencers.html

[33] Jeffrey H. Norwitz, "Introduction", in *Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency*, ed. Jeffrey H. Norwitz (Newport: Naval War College, 2008), xxvi. See www.JeffNorwitz.com.