3rd Place
COIN Writing Competition

Counterinsurgency Intelligence in a "Long War" The British Experience in Northern Ireland

Brian A. Jackson, Ph.D.

HISTORY DEMONSTRATES that insurgents armed with conventional weapons (the gun, the bomb, the rocket) can sustain violent campaigns against state militaries over long periods of time. Victory against such insurgents rarely comes from destruction of troops on a battlefield and, as they typically blend into the population, the enemy is often more difficult to find than to neutralize. In many recent conflicts, resilient and adaptive insurgent organizations using hide-and-seek tactics have checked nations and, in some cases, have prevented them from achieving foreign policy goals.

After seeing the clearly demonstrated effectiveness of U.S. forces in rapid, decisive operations against conventionally arrayed opponents, future U.S. adversaries will almost certainly apply insurgent-like tactics, whether those adversaries are insurgent groups or state forces simply striving for asymmetric advantage. Therefore, in the current environment, the ability to effectively wage counterinsurgency (COIN) warfare is an important element of national power.

As events in Iraq demonstrate, military organizations that have optimized their effectiveness for rapid, decisive operations experience a significant learning curve when engaging in counterinsurgency. Effective COIN operations are, in many ways, the opposite of rapid and decisive: They are slow and deliberate; success may come more from patient use of stabilizing security pressure than from the outcome of defined battles; and depriving combatants of their political support and appeal may be a straighter path to victory than direct engagement. Successful COIN campaigning will often require a significant shift in perspective to clearly grasp the challenges inherent in this kind of warfare and to select the right tools to overcome those challenges.

Where information is needed to identify the enemy, determine how to neutralize or isolate him, and guide security actions across the full spectrum of conflict, intelligence is a central—perhaps the most important—tool for effective COIN. However, another challenge to traditional military organizations in COIN is that the necessary approach to intelligence diverges significantly from conventional modes of operation. Simply applying familiar approaches developed in other contexts can undermine rather than promote mission success.

Learning from the British

A study of historical cases can sometimes provide new perspectives on current problems and help improve organizational performance. One often cited

Dr. Brian A. Jackson is a physical scientist at RAND Corporation, Santa Monica, California, conducting research on such topics as homeland security and terrorism. He holds a doctorate in bioinorganic chemistry from the California Institute of Technology, Pasadena. He wishes to acknowledge David Frelinger and Tom McNaugher, of RAND Corporation, for providing input to early drafts of this manuscript.

PHOTO: A British soldier grabs a Catholic protester during a civil rights march on Sunday, 30 January 1972, in Londonderry, Northern Ireland. The event became known as "Bloody Sunday," because British soldiers killed 13 civil rights marchers and wounded several more. (AFP) case is the British experience in Northern Ireland, particularly the fight against the Provisional Irish Republican Army (PIRA) that began in 1969.[1] A number of other terrorist organizations were active in Northern Ireland at the time, but PIRA's capabilities posed the most potent threat.[2] PIRA has been characterized as a sophisticated, intelligence-led terrorist group because of its capability and operational precision.[3] Only recently, with the reported completion of the group's decommissioning, has its armed campaign come to an apparent end.

Compared to many nations entering insurgent conflicts, the United Kingdom came to the hostilities in Northern Ireland with significant experience in COIN and its modern adjunct, counterterrorism. Some of the U.K.'s previous insurgent conflicts have been held up as examples of effectiveness in such wars. In spite of that experience, however, the conflict in Northern Ireland did not begin well or go smoothly. Poor intelligence operations were a key source of the problems: as reported by historian Chris Ryder, "the principal weakness, according to the Chief of the General Staff who visited Northern Ireland [in 1971], was in intelligence gathering."[4]

In the context of an insurgency, intelligence must deliver the strategic insight needed to know what actions will be effective and what levels of commitment are required, the tactical insight to hit the insurgent target when military action is taken, and the context needed to understand the broader political and other effects of potential security activities. Analyses of the Northern Ireland conflict from military and other perspectives highlight problems in each of these areas:

- Misunderstandings by political leaders about the root causes of the violence.[5]
- Unrealistic expectations about the length of time needed to resolve the situation.[6]
- Tactical intelligence shortfalls that led to action more beneficial to PIRA than to advancing the fight against it.[7]
- Failure to appreciate how covert offensive actions—even successful ones—by special operations or intelligence organizations would play out in the political arena and other spheres.[8]

Over the course of the conflict, security and intelligence organizations adapted by studying the overall effects of their actions and learning from each engagement.[9] In time, they became extremely successful. Consistent with the nature of COIN operations, that success did not translate into traditional measures of military progress, such as discrete battles won or numbers of enemy soldiers eliminated. Rather, it paid off in increasingly effective linkage of security activities into the overall political conflict and drastic reductions in PIRA's freedom of action and effectiveness. In one of the highest compliments a combatant can pay to the intelligence efforts of his opponents, PIRA member Brendan Hughes said that intelligence efforts had "effectively [brought] the IRA to a standstill where it could move very, very little."[10]

The totality of the British intelligence experience in Northern Ireland, both its successes and challenges, is what makes it a valuable example from which to draw insight to shape contemporary COIN intelligence operations.[11] Had the practices from earlier British conflicts transferred seamlessly and flawlessly into the fight against PIRA, the value of the Northern Ireland experience as a case study would likely be much more limited. Given the adaptability of insurgent groups and the specificity of local circumstances, effectively implementing COIN operations will almost always demand learning and adaptability on the part of military and intelligence organizations. These units must shape themselves appropriately for the fight, apply the right tools to collect and analyze intelligence, and use the intelligence effectively against the insurgency. The British experience provides lessons in all these areas.

Building the Right Coordination Structures

Multiple organizations were involved in the intelligence fight against PIRA. At the beginning the Royal Ulster Constabulary (RUC), which might have been expected to spearhead intelligence collection to prevent terrorism, was not in a position to conduct such activities. This prompted the British Army to intervene in Northern Ireland and forced it (and other intelligence organizations) to take the lead in intelligence activities.[12]

As the conflict became more intense, many different intelligence units from military, law-enforcement, and intelligence agencies became involved. Later, national organizations (MI5 and MI6, the Security Service and the Secret Intelligence Service, respectively) also initiated operations to collect political intelligence.[13] In an effort to describe the organizational landscape of the intelligence activities fielded in Northern Ireland, Mark Urban lists nearly 20 units that were formed or evolved from one another between 1969 and 1983.[14] Many were added to bring diverse intelligence capabilities to bear.[15] However, as new agencies and units became involved in operations, no focused attempt was made to weave them into a single, coordinated intelligence effort. This is not surprising, given that such coordination activities require time and effort that could not then be directed at the adversary. Also, efforts involving many organizations almost invariably generate interagency conflicts that inhibit coordination.[16]

The initial lack of coordination had real operational costs. Poor integration meant specialized teams and capabilities were not always used well. For example, Ryder writes, "Owing to a misunderstanding of its role, the SAS [Special Air Service] was misused at first, its special skills wasted because ordinary infantry commanders did not know how to make best use of them."[17] Failures to share also meant security forces might respond to incidents without the information necessary to be effective or to protect themselves. For instance, not sharing new intelligence on PIRA bomb designs with explosives ordnance disposal (EOD) officers who responded to bomb incidents nearly resulted in EOD casualties.[18]

Parallel intelligence efforts in separate organizations also generated inefficiency. Because of security concerns, army officers stationed in the area on short tours developed their own intelligence sources rather than rely on the police, who were permanent residents.[19] Such efforts produced security classification issues that further complicated sharing and coordination. Ryder says, "Further hostility was caused when the army frequently classified material 'For UK eyes only,' which denied the RUC sight of it."[20]

Such parallel streams also generated the potential for single sources to provide (or sell) the same piece of information to more than one intelligence agency, so that when the agencies did attempt to share data, multiple reports could be interpreted as independent confirmations rather than simply multiple contacts with the same source.[21] Problems in coordination also reportedly resulted in the unintentional compromise of sources, hurting the ability of all agencies to collect information.[22]

Although they took years to develop and implement, mechanisms were eventually put in place to address intelligence coordination challenges.[23] Changes included centralization of overall command and control for security activities, including appointment of an "intelligence supremo" and coordinating apparatus.[24] One key to this shift was the development of tasking and coordination groups (TCGs) that brought together the tactical activities of various organizations involved in the intelligence fight. According to Urban, "the TCGs attained a critical role in what security chiefs called 'executive action'—locking together intelligence from informers with the surveillance and ambushing activities of undercover units."[25]

While such structures are needed to bring together information produced in disparate operations staged by different organizations, they also provide critical control. They limit duplication of effort and help deconflict the actions of various organizations to ensure those operations do not interfere with one another.[26] Such structures are also needed to concentrate intelligence forces as effectively as possible. The diverse capabilities that different agencies can

…parallel streams [parallel intelligence efforts in separate organizations] also generated the potential for single sources to provide (or sell) the same piece of information to more than one intelligence agency, so that when the agencies did attempt to share data, multiple reports could be interpreted as independent confirmations rather than simply multiple contacts with the same source.

bring to a fight add value only if those capabilities can be brought to bear when needed.[27]

The Right Tools for Intelligence Collection

Any intelligence effort must be able to collect information. However, the nature of the COIN mission challenges traditional ways of thinking about intelligence collection, especially against members of a comparatively small insurgent organization within a larger civilian population.

Intelligence collection is generally thought of as a distinct activity in which intelligence-specific tools are used to gather data for analysis and application. The COIN intelligence mission has elements that fit readily within this view. For example, developing and exploiting informers or infiltrators clearly requires the same compartmentalization and protection that is standard intelligence practice. Informers within PIRA were of critical importance in the COIN effort and played an important part in the intelligence fight.

That said, the British experience in Northern Ireland demonstrates that COIN intelligence collection efforts must diverge considerably from "classical intelligence" methods. Limits to the availability of clandestine sources mean that other collection tools must be developed and applied. The effectiveness of these other tools depends on the relationship of intelligence specialists with other parts of the security force and even with the general population in the area affected by the insurgency.

Tool 1: Collecting low-grade intelligence. While infiltrators or informers can provide valuable data, they might not be available in sufficient numbers for success in a broad COIN effort. The complement for high-grade intelligence that such sources provide is large amounts of low-grade information that, added together, can provide a picture of insurgent operations.[28] This approach, attributed to General Sir Frank Kitson, requires an intelligence collection approach that is a hybrid of military intelligence, law enforcement, and traditional intelligence agency approaches.

The building up of low-grade intelligence is particularly important against groups like PIRA that adopt decentralized structures for security purposes.[29] British security forces were quite successful in decimating a number of other terrorist groups that operated in Northern Ireland using more centralized structures. Keith Maguire says, "The ability of British security forces to turn *any* members of these [centralized] groups made possible the identification of entire geographic units. In the case of the INLA [Irish National Liberation Army] or the Red Hand Commando, one defection led to the identification of the entire leadership of the organization and perhaps its entire membership within a few months."[30]

Where does such low-grade intelligence come from? The primary sources are direct security force observation and interaction with members of the public.

- *Every soldier a collector*. Direct collection of low-grade intelligence by security forces relies on the eyes and ears of the entire force, not just the efforts of intelligence specialists.[31] Because insurgents and terrorists blend in with the general population, familiarity with what is normal in an area provides the basis for detecting anomalous behavior that might indicate insurgent activity. Like the community patrolling police officers do, this strategy leverages an individual's ability to learn what the baseline activity is in his area of responsibility and then apply his own human processing power to identify activities of concern.[32]

In Northern Ireland, troops pursued this strategy extensively with "constant mobile and foot patrols, which allow[ed] troops to familiarize themselves with their area and to pick up background information."[33] Priming patrols to look for key elements (such as using "face books" of insurgent suspects

Direct collection of low-grade intelligence by security forces relies on the eyes and ears of the entire force,… this strategy leverages an individual's ability to learn what the baseline activity is in his area of responsibility and then apply his own human processing power to identify activities of concern.

AP

An armed British soldier patrols a street in Belfast, Northern Ireland, in February 1972.

whose positions and activities were of particular interest) increased the intelligence gathered.[34] For this strategy to be truly effective, however, the various pieces of information obtained must be brought together in a way that addresses intelligence needs at all levels, from the need for information to shape tactical operations to the requirement to synthesize data to drive strategic decisions about the entire conflict.[35] The British relied on debriefings after patrols to collect information and build the overall intelligence jigsaw of the conflict.[36] In *The British Army in Ulster,* David Barzilay writes, "A patrol never ended up at the main gate [of the military base]. We would get a quick cup of tea, have a cigarette and in a relaxed atmosphere the patrol would be discussed and every piece of relevant information written down and passed on to the company intelligence section."[37]

While individual soldiers or units can be effective intelligence gatherers, standard military practices of compressed tours of duty and frequent troop rotation can make reliance on this strategy problematic. Detailed local knowledge is only built up over time, and the departure of soldiers at the end of their tours takes them away when they might be operating at their highest performance level.

Early in its activities, the British military took few steps to aid knowledge transfer between units rotating into and out of the theater. According to Michael Dewar, "During the early years, battalions were rushed out at little or no notice as both the government and the military merely reacted to events."[38] Over time, to help with knowledge transfer, the army developed processes to overlap the command and intelligence functions of incoming battalions with units already operating in theater.[39] Such processes began to erode the advantage held by the insurgent, who lived and operated in theater and, therefore, could maintain and apply a higher level of local knowledge.

● *Think "people first*." Even if it is possible to harness the eyes and ears of each soldier in a COIN theater, there will always be areas that security forces cannot access. Therefore, the counterinsurgent must rely on the other eyes and ears in theater—those of the general population in which insurgents hide. As members of the public go about their daily business, they will almost certainly observe actions or overhear information of immeasurable value to security forces.

In Northern Ireland, the general public provided key intelligence at times. Some input came via a confidential telephone system put in place by security forces.[40] However, direct interaction between members of the public and security forces was frequently key to gathering this type of intelligence.[41] At regularized interactions with security forces, such as at checkpoints, individuals sometimes took the opportunity to pass on intelligence data.[42] In contexts like these, collection depends even more on individuals outside intelligence organizations or specialties. The nature of interaction between individual soldiers and members of the public can determine success. To ensure that every soldier's actions were consistent with overall goals, soldiers were taught to be courteous but firm: "Slowly it was sinking in that the way a battalion behaved made a big difference to its overall success. Toughness was acceptable; roughness was not."[43]

For interaction and information exchange to be possible between the public and security forces, soldiers have to be able to speak the population's language. In Northern Ireland this wasn't a problem, as it is in Iraq, where security force members who can speak the language are critical assets. If a member of the public who has critical intelligence approaches a soldier and cannot make himself understood, he might not persevere to find another person who can understand his language.

● *Public opinion drives collection.* In COIN, image matters. The population's potential to provide valuable information means that perceptions—the public image of security forces and their activities—have operational consequences. If, for example, citizens believe they will not be protected from retributive violence, their willingness to participate with authorities will be understandably reduced.[44] Where insurgents or terrorists take actions that are perceived as particularly brutal or inexcusable by the general population, citizens may pass on information in spite of such fear. However, relying solely on the adversary's tactical mistakes to spur the flow of intelligence is not sufficient for a robust COIN effort.

Actions matter too. When the actions of security forces are seen as inappropriate or repressive, public trust can be quickly lost. Interrogation of suspects is a good example. While interrogation can provide a key information stream for intelligence purposes, how interrogation practices are perceived publicly is important.[45] If the counterinsurgent's practices are unduly harsh, the insurgent will use them for propaganda purposes. This was certainly the case in Northern Ireland where so-called "interrogation in-depth had revealed a great deal of information in a war where intelligence was at a premium. But success in counterinsurgency operations cannot be measured in purely military terms. The interrogation issue was a political setback for the security forces and a propaganda victory for the IRA."[46]

The value of information obtained via tough interrogation methods must be traded against the methods' potential to shut down voluntary cooperation from the population.[47] Bad perceptions can also lead to political reactions that constrain intelligence gathering. Tony Geraghty tells us that "the political storm raised by [troops' internment and interrogation practices] resulted in official limitations on interrogation which gave the IRA a real military prize."[48]

Similarly, actions taken by security forces that affect the general population must be assessed with a view toward their influence on public opinion. While large-scale operations such as cordon-and-search might provide ways to collect information on broad portions of an area's population, they frequently antagonize the public and inhibit cooperation. Limiting broad operations and using other intelligence-gathering methods can pay dividends in effectiveness and public image.[49]

Tool 2: Specialized operations and units. While broad efforts to collect intelligence data can provide much information useful for COIN, other needs require more specialized tools. Some focused

If…citizens believe they will not be protected from retributive violence, their willingness to participate with authorities will be understandably reduced.

intelligence operations applied in Northern Ireland were quite simple in concept. For example, security checkpoints (particularly rapidly implemented "snap" checkpoints) were used to collect information on the movement of individuals and vehicles.[50] Similarly (and despite the risk of creating ill will in the population), stop-and-search operations of individuals in areas of security concern helped collect certain types of information.[51] Other operations were more complex and required specialized units and capabilities to carry them out.

Observation posts (OPs) were a major part of the intelligence fight. Some OPs were overt, such as the one on top of Divis Flats in West Belfast, where observers continuously scanned the streets using high-powered binoculars and, at night, infrared sights.[52]

Covert surveillance posts (complemented by soldiers patrolling undercover) were also used in problem areas to enable long-term monitoring.[53] At such posts, continuity in staffing helped build up baseline local knowledge, making it easier for an observer to detect anomalies that might suggest PIRA activity. According to Barzilay, "Each time the OPs changed, the same marines went to the same positions and took over the same watches [so they] could get used to the routines of the day, such as the milk float on its rounds, the dustman calling, the paperboy on his rounds, and the pubs opening and closing. In this way each marine became familiar with the personalities and locality and was able to spot a change of routine when it occurred."[54]

Overt observation was challenging. In close-knit neighborhoods, strangers could be readily identified and were rapidly challenged, making it difficult to carry out overt and static surveillance activities. This necessitated development and application of a wide range of specialized teams with training in close observation of individuals and other methods of focused intelligence gathering. Groups such as the 14th Intelligence Company, special close-observation platoons, the E4A unit in the police department, and the SAS all played these roles in different parts of the intelligence fight in Northern Ireland. Some military intelligence teams operated for extended tours (compared to the shorter rotations of other units) to provide continuity and to allow them to build up local knowledge and expertise.[55] Having units that could monitor areas and individuals covertly made it possible to gain additional intelligence through the use of challenge-response type operations, in which overt actions by security forces were combined with close observation to capture any PIRA activities or defensive actions "flushed out" by the overt element.[56]

Tool 3: Flexible technical means. While British security services deployed a range of intelligence efforts that relied on direct observation and information collected by individuals, such operations always had inherent, and frequently significant, risks. Therefore, technical tools were needed to provide alternative and complementary ways to gather information. Such tools were also important force multipliers because there frequently weren't enough specialized surveillance operatives to satisfy the demand for their services.[57]

Strategies applied in Northern Ireland included such traditional means as airborne sensors with live-feed television, sophisticated photographic devices, and infrared detection systems.[58] Listening devices, phone taps, hidden cameras, motion detectors, and technologies that intercepted communications traffic also played critical roles.[59] Reportedly, a variety of devices were deployed in areas of particular interest, from zones where PIRA operatives moved across the border between Northern Ireland and the Republic of Ireland to underground tunnels where terrorist operations were suspected.[60]

Technical surveillance efforts were also specially adapted for COIN. Technologies were molded to the mission, not vice versa; they augmented the collection effort instead of determining how it would be done. As a case in point, the critical task of identifying and tracking PIRA activities meant that photographic surveillance approaches were applied in ways more akin to how they would be used by law-enforcement agencies than in traditional military intelligence gathering.

Photographing terrorist suspects and using photos of them to identify their associates was key to building dossiers and identifying people who might be recruited as agents.[61] When security forces identified sites (such as arms caches, residences, or commercial buildings) that terrorist group members used, security forces frequently chose to monitor the sites with audio and video surveillance for extended periods in an effort to identify unknown terrorists or supporters.[62]

Another intelligence tool particularly suited to tracking PIRA operational practices was the tracking transmitter, which helped security forces map

When security forces identified sites …that terrorist group members used, [they] frequently chose to monitor the sites with audio and video surveillance…to identify unknown terrorists or supporters.

the movement of particular vehicles or materials through the terrorist infrastructure. Transmission devices in vehicles made it possible to track the position of an informer or a suspect's vehicle as it called on various locations in Northern Ireland. Mapping such travels helped identify sites that might merit follow-up investigation.[63] In the middle to late 1970s, improvements in technology made it possible to surreptitiously place similar tracking devices in weapons and explosives discovered in PIRA arms caches.[64] The practice, known as jarking, made it possible to trace the marked arms' progress through the group's logistical system. When devices were produced that could capture audio, they were also used by security to listen to conversations occurring around the weapon.[65]

The Right Capabilities for Analysis

The many collection modes deployed against PIRA answered Kitson's requirement for masses of low-grade information on the insurgency and its activities. However, without robust analytical capabilities to make sense of the information, a COIN effort can drown in data rather than gain greater knowledge of the situation on the ground. Desmond Hamill says, "[W]hat was needed, then, was for it all to be brought together and meshed into a constructive and useful pattern."[66]

Correlating the snippets of information collected by COIN intelligence efforts into a coherent picture requires a commitment of manpower and capability.[67] Early on the British military reportedly did not commit the manpower needed to do the job. According to Bruce Hoffman and Jennifer Taw, "In 1973, the number of military intelligence specialists 'involved in collating and assembling this information were left to each unit, but the numbers were comparatively small, around the normal wartime establishment of six men.'"[68] Effective interpretation and dissemination of the large volumes of data produced required much more, with the effort eventually growing into a "large organization [to utilize] the information brought in by the troops in the field."[69]

While the effective use of intelligence requires sufficient analytical capability, technology (databases and computational power) also plays an important role in weaving the "points" of low-grade intelligence data together into a coherent picture. Initially, data management included the use of banks of card files and lists of photographs of potential PIRA members or sympathizers.[70] As the counterinsurgency continued, these tools evolved into complex databases and computerized information management systems. Descriptions of intelligence efforts indicate that there were individual systems for data on vehicles (code named Vengeful) and individuals (code named Crucible).[71]

Critically, data was collated from across the collection spectrum. Law-enforcement organizations, for instance, fed their intelligence into a unified criminal intelligence system: "Monitoring of terrorist suspects and their supporters was also carried out and the details forwarded to an intelligence-collating facility. . . . These details would be entered into a computer system, where an easy and retrievable reference could be made and a composite printout of the date, time, and place of the sighting of the particular vehicle/vehicles could be accessed."[72] Ryder tells us, "Every single piece of information reaching the RUC from any source was . . . systematically collated. The ballistic and forensic reports on every incident were married with even the most inconsequential scraps of intelligence."[73]

Such systems were constructed and populated through systematic gathering of framework data (geographic, census, and other descriptive information about the theater and its inhabitants) to provide context for collected intelligence information.[74] Committing the time and resources necessary to construct and feed such systems requires up-front investment, but in a long-term fight against an insurgent group such investment makes sense. The systems' return accrues over time as the information they hold increases and their capabilities expand.

Additional knowledge-based features were reportedly added to the data-collation systems to improve analysis of data and pattern recognition, which made it possible to apply such techniques as traffic analysis and network analyses of groups and to detect even small changes in suspects' behavior.[75] For example, if the systems lost track of specific PIRA suspects, attention was then focused on locating those individuals to determine the reasons for the change in behavior.[76]

The computer systems' rapid retrieval capabilities also provided soldiers on the ground with quick access to intelligence to guide action. Barzilay writes, "Soldiers on foot and vehicle patrol [would look] for particular men and vehicles. When the target [was] spotted a full report [was] radioed to the battalion headquarters and then passed on to the intelligence officer, who pass[ed] that information to the computer, if necessary in a matter of seconds. At many bases throughout Ulster there [was] a direct terminal link to the computers. That link also enable[d] the intelligence officer or operator to see what [was] on 'file' about the particular target and pass this information back to the man on the ground. It could be a simple piece of information that a man is often seen in the area where he has been spotted, or it may refer to the fact that he should be approached with caution because he is known to have been involved in terrorist activity and armed."[77]

Feeding information back to soldiers on the ground generated more and better data collection. Barzilay continues, "Those who mount vehicle checkpoints, whether Royal Military policemen or ordinary soldiers, [were] given a daily briefing on what to look out for. That information might have come as a tip-off, from police criminal intelligence or Special Branch, or it might have come from other information which had previously been fed into the computer [intelligence systems]." [78] Getting such information made the soldiers see the system's tangible benefits. It gave them incentive to contribute information to the systems.

Applying Intelligence in a Long Fight

In military intelligence activities, the focus is usually on moving as quickly as possible from collecting information to acting on it—transitioning from sensor to shooter, as the U.S. Army calls it—in an effort to capitalize effectively on all available information. Intelligence in counterterrorism and counterinsurgency sometimes enables successful operations in which terrorist-insurgent plans are disrupted; adversaries are shot, killed, or captured; cells are rolled up and prosecuted in the courts; or logistical bases are captured and supply lines broken. Examples of such operations can be found throughout the history of the violence in Northern Ireland. In a long-term fight, however, such actions might be the exception rather than the norm. High-profile victories are not the most common—or even always the most desirable—outcomes of COIN intelligence efforts.

In Northern Ireland, applying intelligence immediately and actively was risky, not only for military or police personnel, but for intelligence sources whose identities and activities might be discovered as PIRA carried out its own post-mortem investigation of security force success.[79] A balance had to be struck between acting immediately on actionable information, thereby gaining a local victory, and "continuing to watch" in an effort to build up a sufficiently detailed picture of the insurgents' activities, plans, and order of battle to enable more effective action at a later time.[80] This balance necessitates different strategies for acting on intelligence in a COIN environment.

Because of the risk of revealing sources and methods, intelligence in Northern Ireland was often used to frustrate rather than to strike directly at PIRA. Based on knowledge of a planned terrorist attack, for example, security forces shaped the environment so PIRA would choose to abort the operation. Urban tells us that "an IRA team sent to assassinate a [member of the security forces] will not press home its attack if there are several uniformed police, perhaps stopping vehicles to check their tax discs, outside his or her house. The police or soldiers involved will almost always be ignorant of the covert reason for their presence."[81]

Such disruption operations did not even have to involve overt action by security forces. Urban continues, "An intelligence officer relates one incident where it was known that an IRA team was to travel along a particular route on its way to an attack. They [the security forces] arranged for a car 'accident' to take place on the road. 'There wasn't a uniform in sight,' he recalls, 'but it was assumed that they [the insurgents] would get unnerved sitting in the tailback, thinking the police were about to arrive.' The ploy succeeded."[82]

AP

Members or the Royal Ulster Constabulary remove a Catholic demonstrator from the city walls of Londonderry, Northern Ireland, before the start of the Protestant Apprentice Boy Parade on 12 August 1995.

Other strategies included simply depriving the terrorists of their targets. If word of a planned ambush on a security-force patrol came in from intelligence sources, the area could simply be put out of bounds for patrols, meaning that the PIRA attack team would sit in position waiting for a target that never appeared.[83] More subtle deployments of security forces were used to divert terrorist teams down particular routes and to influence how terrorist lookouts ("dickers") would report the risk of staging operations around particular security-force bases or sites.[84]

This approach to applying intelligence, where security forces essentially "play for a tie" (and no direct damage is done against either side, but the terrorists' planned operation is thwarted) takes a long-term view of the conflict. It acknowledges that there is value in frustrating operations while preserving intelligence sources, rather than going for a tactical win immediately. While "playing for a tie" does not directly attrit insurgent weapons or personnel, it constrains the insurgent organization's freedom of action and costs it the time and effort invested in the disrupted plans.

Changing the Vocabulary for COIN

The U.S. Department of Defense recently adopted "the long war" as a descriptive term for the current struggle against the insurgency in Iraq and the more general fight against global terrorism. Such a change in vocabulary is significant, given that much of contemporary U.S. military planning has focused on how to win a short war by bringing together force, precision, agility, and speed to make quick victory possible. However, waging war effectively requires more than acknowledging that wars are fought and won on different time scales. As the British experience in Northern Ireland shows, it is not enough merely to adopt the long-war terminology; rather, the U.S. military will have to make a broad set of changes if it wants to build organizations that can win such conflicts. Winning a long war is not the same as winning many short wars in succession. Rather, winning a long war requires applying an entirely different, sometimes antithetical set of tools than those optimized for achieving victory through rapid, decisive action.

Perhaps not surprisingly, Northern Ireland provides many examples of organizations making the transition from seeking quick victory to waging long-term operations. When it deployed, the British Army did not expect to be involved in a conflict for decades, and its early actions were not designed with the requirements of a long-term fight in mind.[85] According to Graham Ellison, the police organizations involved in the conflict adopted the Army's viewpoint, believing that strong action in the short-term could tighten the noose on the terrorists and win the fight.[86]

The same was true for PIRA. Early on, PIRA approached its fight from the perspective that "just one more heave" would push the British from Northern Ireland. The organization only transitioned away from that view much later, to an approach focused on maintaining its survivability over the long-term and integrating its violent action with a more explicit political strategy.[87] Both sides made these changes because strategies based on winning quickly, and primarily through military means, produced results that were unsatisfactory at best and frequently quite damaging to their interests.

For security organizations, truly adopting a long-war approach entails a shift from decisive to patient operations; it means understanding how security efforts contribute to or detract from political and other efforts against an insurgency. It is important to consider the overall impact of security actions because many COIN intelligence activities do not produce clear military results that can be measured in adversary casualties or materiel destroyed. Collecting extensive data on individuals in an area of responsibility and debriefing soldiers returning from patrol on the "feel" of neighborhoods might seem unsoldierly to military intelligence traditionalists, but it works.

AP

A youngster walks past Real Irish Republican Army graffiti on walls in West Belfast, Northern Ireland, 4 March 2001.

Similarly, larger considerations might dictate limited action, perhaps only quietly disrupting insurgents' plans, or even foregoing the opportunity to strike an identified target, in order to collect needed information. Because military intelligence typically strives to move actionable information into target folders and onto strike lists, it might be difficult to pass up an attractive, valuable target, whatever the potential payoff in future intelligence opportunity. Patience and discipline, however, not scattered tactical victories, overcome insurgencies.

The vagaries of COIN make collecting, analyzing, and applying intelligence quite different from traditional military intelligence operations, which are optimized for rapid, decisive action. The long collection-and-analysis cycles involved and the sometimes subtle uses of data also make it difficult to assess the outputs of COIN intelligence in purely military terms. For example, when the outcome of an extensive intelligence operation is a standoff or draw, the military utility of the activity might seem limited at best; however, in the context of an integrated political and military effort, there might be a great deal of utility in such an approach. When you neutralize the enemy's ability to cause harm, you create opportunities for other action along other lines of operation.

Because insurgencies are usually ended by political means, the mission of security forces might not be to destroy the insurgent organization and its membership. Instead, it might simply be to prevent the insurgency from shaping its environment through violence. Once security forces have effectively rendered the insurgency impotent, broader action on political and other fronts can catch up and render it irrelevant. ***MR***

NOTES

[1] See, for example, Conor O'Niell, "Terrorism, Insurgency and the Military Response from South Armagh to Falluja," *RUSI* (2004): 22-25, online at <www.rusi.org/publication/journal/ref:P417394CE896AE/>.

[2] For simplicity, I refer to the conflict as being against PIRA, although activities in Northern Ireland focused on a wider variety of terrorist organizations.

[3] Former law-enforcement member, interview by author, March 2004, Northern Ireland.

[4] Chris Ryder, *A Special Kind of Courage: 321 EOD Squadron-Battling the Bombers* (London: Methuen, 2005), 47.

[5] See, for example, Tim Pat Coogan, *The IRA: A History* (Niwot, CO: Roberts Rinehart Publishers, 1993), chap. 16; Desmond Hamill, *Pig in the Middle: The Army in Northern Ireland, 1969-1984* (London: Methuen, 1985), chap. 1-2.

[6] David Barzilay, *The British Army in Ulster,* vol. 2 (Belfast, UK: Century Books, 1975).

[7] Early in the conflict, improperly targeted actions such as large-scale internment operations invigorated rather than broke the back of the terrorist group. (See Coogan.)

[8] Bruce Hoffman and Jennifer Taw, *A Strategic Framework for Countering Terrorism and Insurgency* (Santa Monica, CA: RAND Corporation, 1992), online at <www.rand.org/pubs/notes/N35061>; Mark Urban, *Big Boys' Rules: The Secret Struggle Against the IRA* (London: Faber & Faber, 1992).

[9] J. Bowyer Bell, "The Irish Troubles Since 1916," Columbia International Affairs Online, 2002, online at <www.isn.eth2.ch/pubs/ph/list.dfm?v21=60981&v33=60242&click52=60242>.

10. Brendan Hughes quoted in Peter Taylor, *Brits: The War Against the IRA* (London: Bloomsbury, 2001), 302.

11. A wealth of information is available in the open literature, including first-person narratives of individuals on both sides, making it possible to explore these issues in more detail than in many other campaigns. Available sources include memoirs by individuals in military intelligence and special operations organizations, law-enforcement organizations, British Army units operating in Northern Ireland, and non-Army EOD units; and by infiltrators and informers in the paramilitary/terrorist groups. Also valuable are works looking at individual services or containing analyses cutting across the activities of intelligence and security forces operations in the conflict.

12. David A. Charters, "Intelligence and Psychological Operations in Northern Ireland," *RUSI* (1997): 22-27 (originally published in *Journal of the Royal Services Institute for Defence Studies* 122); Hoffman and Taw, 87.

13. Keith Maguire, "The Intelligence War in Northern Ireland," *International Journal of Intelligence and Counterintelligence,* vol. 4 (1990): 145-65.

14. Urban, 255. The various roles and agencies are also discussed in Tony Geraghty, *The Irish War: The Hidden Conflict Between the IRA and British Intelligence* (Baltimore, MD: The Johns Hopkins University Press, 2000), 130-31; James Rennie, *The Operators: On the Street with Britain's Most Secret Service* (South Yorkshire, UK: Pen & Sword Military Classics, 2004), 176.

15. Barzilay, vol. 1, 1973, 222.

16. Graham Ellison and Jim Smyth, *The Crowned Harp: Policing Northern Ireland* (London: Pluto Press, 2000); Hoffman and Taw, 97; Urban, 18-24; Geraghty, *Inside the S.A.S.: The Story of the Amazing Elite British Commando Force* (New York: Ballantine Books, 1980), 165-69; Jack Holland and Susan Phoenix, *Phoenix: Policing the Shadows* (London: Hodder and Stoughton, 1996), 139, 287; Bradley H.C. Bamford, "The Role and Effectiveness of Intelligence in Northern Ireland," *Intelligence and National Security*, vol. 20, no. 4 (2005): 581-607, 586.

17. Charters; Holland and Phoenix, 187.

18. Ryder, *A Special Kind of Courage*, 53.

19. Urban, 20, 22.

20. Ryder, *The RUC 1922-1997: A Force under Fire* (London: Mandarin, Random House UK, 1995), 157. See also Geraghty, *The Irish War,* 136.

21. Geraghty, *The Irish War,* 151.

22. Bamford, 593.

23. Law-enforcement member interview.

24. Hoffman and Taw, 22-23, 94-95.

25. Urban, 95.

26. Holland and Phoenix, 223-28.

27. See also Mark Bowlin, *British Intelligence and the IRA: The Secret War in Northern Ireland, 1969-1988* (Master's thesis, National Security Affairs, Naval Postgraduate School, Monterey, California, 1998) for discussion of the benefits achieved from coordination of intelligence organizations. Current U.K. COIN doctrine describes coordination and management processes for intelligence in greater detail. See U.S. Army Field Manual 1.0, *Combined Arms Operations,* vol. 1, part 10, "Counter Insurgency Operations (Strategic and Operational Guidelines)" (Washington, DC: U.S. Government Printing Office, 2001), chap. 6, Intelligence.

28. Ibid.

29. Brian A. Jackson, "Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to al Qaeda," *Studies in Conflict and Terrorism* 29, 3 (April-May 2006).

30. Maguire, 152.

31. The idea that good intelligence relies on the eyes and ears of the entire force echoes current Army efforts at making "every soldier a sensor"; in reality, however, the soldier is much more than simply a sensor, given that individuals have processing power and an ability to assess a situation to distinguish activities that are truly of interest from false positives. Simple technological systems cannot make this discrimination. For more information, see online at <www.army.mil/professionalvideo/movies/sensor.html>.

32. Law enforcement member interview.

33. Charters; Hoffman and Taw, 90.

34. Martin Dillon, *The Dirty War* (London: Arrow Books, 1991), 409.

35. Maximizing the effectiveness of patrolling to gather intelligence also might require changes in traditional ways military units respond to hostile situations and environments. For example: "The classic procedure for soldiers under fire is to take cover and return the fire. [Because of the IRA's tactics of firing and seeking to escape, soldiers] had to be taught that the only way to succeed, if at all, was to move forward very fast and straight away start entering the surrounding houses. There were three reasons for this new drill. First, if they got in quickly they had a fair chance of picking someone up, or at least the weapon. Second, if the incident had been bloody, people inside would be in a state of shock and might say things that they would normally suppress. And, third, the more houses they visited the less chance there was that those who did talk would be identified. However, there were dangers in doing even this regularly, because it could set up a patrol for a devastating ambush" (Hamill, 140-41).

36. Michael Dewar, *The British Army in Northern Ireland* (Swindon, Wilts, UK: Guild Publishing, 1985), 182-83.

37. Barzilay, vol. 2, 218.

38. Dewar, 181.

39. Hamill, 243.

40. Openness to public information has obvious risks. PIRA used such systems to inject misinformation into the police system and to lead security forces into ambushes. See Geraghty, *The Irish War,* 52; Alan Barker, *Shadows: Inside Northern Ireland's Special Branch* (Edinburgh, Scotland: Mainstream Publishing, 2004), 101-102, 115; Barzilay, vol. 1, 221-22; Hoffman and Taw, 96; Ryder, *The RUC,* 124-25; Sean MacStiofáin and Gordon Cremonesi, *Memoirs of a Revolutionary* (Edinburgh: R & R Clark, Ltd., 1975), 331, as well as "law-enforcement officer interview" (above). Developing overlapping processes required information systems and practices adept at assessing and validating likely "imperfect" intelligence data. The overlap might necessitate additional research and surveillance operations. (See Barker, 115.)

41. Barzilay, vol. 2, 218.

42. Ibid., vol. 4, 24-25.

43. Hamill, 141.

44. Maguire, 152.

45. Ellison and Smyth. The value of interrogation as a source of a range of intelligence reinforces the importance of security forces being able to communicate in the local language. Effective interrogation frequently requires communication with individuals over extended periods of time. Shortages of security force members (especially those trained in interrogation processes) who can communicate directly with prisoners can make effective interrogation difficult, particularly if numbers of detainees begin to significantly exceed the number of trained and linguistically skilled interrogators. The pressure to "speak with everyone" can lead to abbreviated interrogation processes that greatly reduce the potential take of information from any single detainee.

46. Charters; Hamill, 60-61.

47. Although length constraints for this article do not allow a full exploration of interrogation techniques, it is important to note that effective counterinsurgency requires a variety of information that could be sought through interrogation. While the focus of interrogation is frequently tactical in nature (seeking details of upcoming operations), strategic information to provide more general insights into insurgent organizations is also needed. As a result, interrogators must be appropriately trained for COIN operations to ensure that the full value of interrogation operations can be realized. (See Geraghty, *The Irish War,* 60-61.) Using official and operational secrecy to shield intelligence activities in an attempt to avoid their negative effect on public opinion can be effective, but might simply defer the accounting.

48. Geraghty, *The Irish War,* 51.

49. Urban, 108.

50. Charters; Barker, 56.

51. Dewar, 177-88; Dillon, 32-33.

52. Dillon, 409; see also Barzilay, vol. 3, 142.

53. Dillon, 32-33; Holland and Phoenix, 113-17; Barzilay, vol. 4, 28; Rennie, 15.

54. Barzilay, vol. 2, 215.

55. Barker, 43; Barzilay, vol. 4, 23-28; Barzilay, vol. 3, 106; Urban, 45, 47; Ellison and Smyth; Sarah Ford, *One Up: A Woman in Action with the S.A.S.* (London: HarperCollins, 1997), 2-3, 155-56; Rennie.

56. Hoffman and Taw, 90.

57. Urban, 119.

58. Barzilay, vol. 1, 76; Dillon, 409, 411-12; Geraghty, *The Irish War,* 131; Urban, 118.

59. James Adams, Robin Morgan, and Anthony Bambridge, *Ambush: The War Between the SAS and the IRA* (London: Pan Books, 1988), 3-5; Dillon, 398-401; Geraghty, *The Irish War,* 134-35, 147; Taylor, 248.

60. Dillon, 409-11; Geraghty, *The Irish War,* 134-35.

61. Barker, 133; Dewar, 76-77; Barzilay, vol. 4, 28.

62. Dillon, 398-99; Rennie, 221-23; Geraghty, *The Irish War,* 135.

63. Dillon, 398-401; Martin McGartland, *Fifty Dead Men Walking* (London: Blake Publishing, Ltd, 1997), 116, 144; Ford, 162.

64. Ford, 205; Rennie, 173; Urban, 118-19; Dillon, 401-402; McGartland, 258; Geraghty, *The Irish War,* 147.

65. Urban, 118-19; Dillon, 401-402.

66. Hamill, 242.

67. George C. Styles and Bob Perrin, *Bombs Have No Pity: My War Against Terrorism* (London: William Luscombe, 1975), 111.

68. Hoffman and Taw, 90; see also Hamill, 134-35.

69. Hoffman and Taw, 90.

70. Barker, 94; Urban, 116.

71. Barker, 57; Barzilay, vol. 4, 24; Geraghty, *The Irish War,* 158-59; Urban, 115-17; Rennie.

72. Hoffman and Taw, 91; Barker, 57.

73. Ryder, *The RUC,* 150.

74. Dewar, 177-88; Charters; Hamill, 134-35; Barker, 94-95.

75. Geraghty, *The Irish War,* 160; Karl M. van Meter, "Terrorists/Liberators: Researching and dealing with adversary social networks," *Connections* 24 (2002): 66-78, 68-69, online at <www.insna.org/Connections-Web/Volume24-3/Karl.van.Meter.web.pdf>.

76. Canadian Security Intelligence Service (CSIS), Irish Nationalist Terrorism Outside Ireland: Out-of-Theatre Operations 1972–1993, 1994, 2005; Dillon, 406.

77. Barzilay, vol. 4, 24.

78. Ibid., 25. It should be noted that even in Northern Ireland where multiple bombings occurred every day during periods of the violence, questions were raised about how intelligence-gathering efforts affected individual rights to privacy. (See Barzilay, vol. 4, 23.)

79. Nuala O'Loan, "Independent Investigation into Police Conduct in an Environment of Terrorism," in *The Eighth Annual Conference of NACOLE,* Cambridge, Massachusetts, 1 November 2002, online at <www.nacole.org/OLoan_11_02.htm>.

80. Urban, 107; Ford, 206.

81. Urban, 213.

82. Ibid.

83. McGartland, 77, 175-78.

84. Urban, 207, 213.

85. Barzilay, vol. 2.

86. Ellison and Smyth.

87. C.J.M. Drake, "The Provisional IRA: A Case Study," *Terrorism and Political Violence*, vol. 3 (1991): 43-60, 47.