3. Function of Clandestine Cellular Networks

As explained above, clandestine elements of an insurgency use form—organization and structure—to compartmentalize and minimize damage due to interdiction by counterinsurgents by limiting information distribution and interface with other members of the organization. Clandestine networks use function—clandestine art or tradecraft—to minimize signature and thus detection by counterinsurgent forces, and facilitate the communication between compartmented elements. In essence, *functional* compartmentalization, in addition to compartmentalization through organizational *form*, as explained above, are the ways that insurgents protect themselves to ensure long-term survival—the "logic" behind the use of the organizational form and function—in order to defeat the government or occupying forces.

Function is defined as "an action or use for which something is suited or designed."[129] It is the function of clandestine art or tradecraft to keep the network signature low so the daily interactions of the network members remain undetectable by the counterinsurgent force.[130] These functions in clandestine cellular networks revolve around minimizing signature and detection of the interaction of members of the network and their operational acts. The ability of insurgents to do this effectively has noticeable effects. For example, in 2005, RAND Corporation's Bruce Hoffman published an analysis of the insurgency in Iraq, concluding that the insurgency was a cluster of uncoordinated and disconnected local insurgent groups with no centralized leadership.[131] As he explains, "The problem in Iraq is that there appears to be no such static wiring diagram or organizational structure to identify, unravel, and systematically dismantle."[132] However, in hindsight it is obvious that the assumption of a disconnected insurgency was incorrect. Instead, the insurgency was primarily made up of clandestine cellular networks, applying excellent tradecraft to remain hidden and to hide the connections between the individuals in the movement. Thus the unseen linkages or networks that connected the seemingly distributed cells were the clandestine infrastructure (form), further protected by clandestine arts (function), to minimize signature so that the clandestine cellular networks were not readily visible to the counterinsurgents as shown in Figure 12.[133]

The visible parts of the networks were only the cells that were in direct contact with the counterinsurgent forces, at the periphery or edge of the organization, which practiced poor tradecraft and were detected and interdicted (see Figures 6-8). Units that conducted operations against these cells had success until they hit a compartmentalization mechanism, or cut-out, that stopped the exploitation, thus marking the boundary or edge of the clandestine organization (see Figure 7 and Figure 8).[134] Interestingly, where one cell or network is effectively interdicted, in a short period of time, a new cell or network appears to take its place.[135] As one former battalion commander commented to the author in 2006, "My battalion would [kill or capture] a cell and a new one will take its place within a couple of weeks at the most."[136] In hindsight, it is obvious that the insurgency was connected and coordinated behind the veil of the clandestine space.[137]

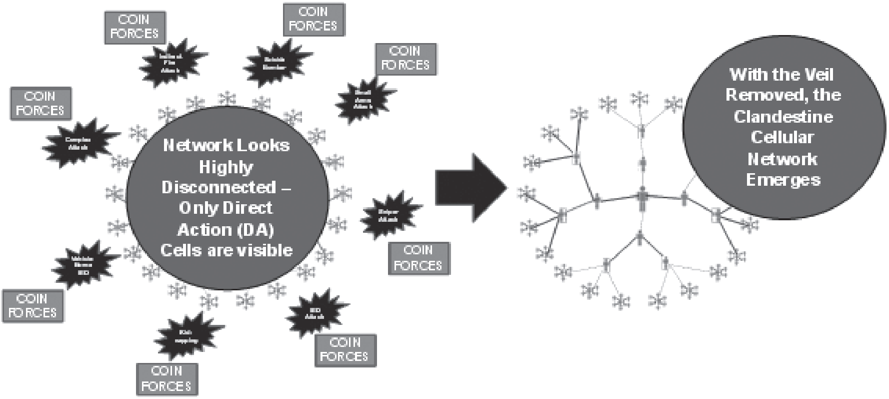

Figure 12. The Emergence of the Clandestine Cellular Network[138]

Although much of this hidden network relied on structural form to protect the network from pursuit by the counterinsurgents, the function of clandestine arts or tradecraft kept the signature so low that even experts like Hoffman did not realize the magnitude of the insurgency and its internal coordination.

Therefore, just as important as understanding clandestine cellular networks' organizational compartmentalization, it is imperative to understand the functional compartmentalization as well. To facilitate the functional compartmentalization, clandestine techniques or tradecraft are used for the following: to conduct indirect or impersonal communications in order to *functionally* compartmentalize the organization; to minimize the signature of person-to-person communications, or "personal communications;" to conduct counter-surveillance; to reconnect the network when key leaders are detained or killed; to clandestinely recruit new members in order to purposefully grow the organization or replace losses; to hide key individuals using safe houses; to provide security for locations, such as meeting places and safe-houses; and lastly, to facilitate clandestine skill training between the superior and subordinates.[139]

Impersonal Communications

Impersonal communications, also known as cut-outs, functionally compartmentalize the networks as an additional precaution to the organizational forms of compartmentalization explained in the previous chapter.[140] Impersonal communications, as the name implies, is anything other than face-to-face contact between two members of the organization.[141] Impersonal communication is a method of ensuring that two individuals never come in direct contact, and thus cannot be physically linked to one another.[142] Impersonal contact includes passive and active methods, the difference being in the type of signature produced.[143] Passive methods include mail or dead-drops, live drops, and clandestine codes or signals hidden within different types of media.[144] Active methods include short or long-range radios, phone, and Internet, all which emit signals that can be more readily detected by technologically capable counterinsurgents.[145]

Passive measures are used to minimize signature in high-threat environments. Couriers are the most secure means of transmitting messages or moving items, such as weapons, between two individuals.[146] The key requirement for couriers are their ability to move some distance, including through counterinsurgent population-control measures, such as checkpoints, without arousing suspicion.[147] Women and children may be used as couriers to decrease suspicion and the chance of search if moving sensitive items or written information.[148] Although couriers are one of the most secure methods, they and their messages can be intercepted, as was the case with the letter sent from al-Qaeda's Ayman al-Zawahiri to Abu Musab Zarqawi in Iraq that exposed a rift between the al-Qaeda core leadership and Zarqawi over Zarqawi's tactics against the Shi'a in Iraq.[149]

The second method of impersonal communication is the mail drop, also known as a letter drop or dead drop.[150] In this method, one member of the network places a message or item at a certain location, the drop site, which for larger items could be a cache. The deliverer then alerts the receiver, through other clandestine means, to pick up the item, resulting in no personal contact between individuals.[151] French counterinsurgency practitioner Roger Trinquier provides a description of the Algerian underground use of mail drops: "Carefully kept apart from other elements of the organization, the network was broken down into a number of quite distinct and compartmented branches, in communication only with the network chief through a system of letter boxes."[152] Although mail or letter drop describes the idea of leaving a letter or package in the Western mindset, and at times may include literally using the post office, this wording also symbolized that some unconventional locations may act as "mail boxes." Orlov provides some examples of the use of unconventional hiding places:

> Hiding places, such as a hollow in a tree…or a deep crack in a wall…or a hole bored in a public monument, take the place of mailing addresses….A special system of 'indicators' is used to orient each agent as to the specific hiding place where a message is awaiting him….The 'indicator' consists of a number or a symbol written on a wall, a park bench, or somewhere inside a railway station, post office, or public telephone booth.[153]

Thus the "item" is dropped off by one individual and then hours or days later, when the other individual sees the "indicator," he can recover the item, place an "indicator" signaling that he has retrieved the item, and thus ensures that both parties know the status of the communication while maintaining the anonymity.[154]

The third method of passive communication is the so-called "live drop."[155] The difference between a dead drop and live drop is that there is a person at the drop site that secures the item being passed between members.[156] This person is the cut-out, passing the item to the other member when they come to the location after being alerted that the item has been left with the live drop through some indicator or signal. As Prikhodko explains,

> When communicating by means of a live drop there is no personal contact….Operational materials from [deliverer]…are passed through a special person who more frequently than not is the proprietor of a small private business (book shops, antique dealers, [drug stores], etc.). The [receiver] visits the live drop…only after a

> special signal. The proprietor of the live drop places the signal after receiving the items.[157]

The danger of this method is that if the individual that is the live drop is discovered, he has a direct link to the other member and may provide information that can lead to the interdiction of the other member, but only if he has enough information on the other members, such as names, addresses, or acquaintances. If not, then the "live drop" method works as an effective cut-out.

Clandestine codes are the fourth method and can be used across different types of media to alert other cell members or pass information passively.[158] In print media, this could include ads or announcements in newspapers in which the information in the ad is a code that the other cell members understand.[159] In World War II, the Allies extensively used the nightly British Broadcast Corporation overseas radio broadcasts to the resistance forces in Europe to pass information clandestinely on resupply drops and operational directives. These included the messages that only had meaning for the intended receiver, based on a code word intermingled in the broadcast, such as a forewarning of an impending parachute resupply drop to the resistance on a certain drop zone.[160] This same theory causes intelligence agencies to conduct in-depth analysis of broadcasts by al-Qaeda core leadership to see if there are any hidden messages.[161] Finally, code words can be innocuously inserted into emails or telephone conversations that for example could provide warning of security forces approaching or execution orders to conduct operations against pre-approved targets.[162] Regardless of the means, it is the passage of information while maintaining a low signature that makes these very difficult to counter.

Active methods of impersonal communications—short- and long-range radio, Internet, landline, and cell phone—provide a much faster means of communications that has to be weighed against the increased risk of detection and interdiction by technologically-sophisticated counterinsurgents.[163] Short- and long-range radio transmissions have largely been replaced by phone. However, radios may be the only method of rapid communication in areas where there is no phone coverage. Radios may also be necessary if the instant passage of messages is required, such as an early warning alert of counterinsurgency forces moving into the area. Telephones, both landline and cell, have a role in impersonal communication, with the disadvantage of producing a signal which a security force could monitor. Phones can also be combined with passive measures, such as code words.[164] The Internet has opened a new clandestine playing field, but like other active measures, there are still dangers due to an electronic signal. Thus, instead of being a revolutionary adaptation, like the information age network theorists posit, the Internet provides the ability to disseminate information and ideology quickly and is another tool for communicating, but it comes with associated risks. The same clandestine techniques presented here have also been adapted to the cyberspace, including using cyber dead drops.[165] However, like other active measures, there are dangers due to the electronic signatures that can be detected by the counterinsurgents.[166] For example, Jihadists have attempted to clandestinely hide their webpage by piggybacking on other non-nefarious websites, often without the webmaster's knowledge, but they have been discovered in some cases.[167] Despite the strengths of active methods, such as rapid communications and long-distance reach, they significantly increase the danger for the insurgent due to the signals emitted that may be detectable by a technologically-advanced adversary.[168]

Personal Communications

Meetings between members of a cell or network, who would normally be separated by one of the methods of compartmentalization, greatly increase the vulnerability of the two members.[169] However, despite the risks, there may be times when a clandestine leader needs to meet in person with his subordinates, instead of using an impersonal means, to gain better situational awareness, train the subordinate, assess the subordinate, or when the clandestine recruiting process explained below requires personal communications with potential recruits.[170] As I. E. Prikhodko explains from the perspective of an intelligence officer working with his subordinate agent,

> Only by personal contact can the case officer study the agent better, analyse [sic] his motives, check on and control his activities, and finally—and this is of great importance—instruct the agent, train him in new methods and in professional [clandestine] skills, develop him, and exert an influence on him through personal example.[171]

Due to the vulnerability, meetings must be thoroughly planned including: identifying a meeting location, planning the routes of both individuals to and from the meeting location, establishing security to counter surveillance during the individuals' movements to the location, as well as having security around the location to give early warning and a plan if the meeting fails to take place.[172] As Swiss insurgency expert H. von Dach Bern notes, "meetings of [underground] members must be prepared at least as carefully as a raid, for they constitute a 'special type' of operation."[173]

Counter Surveillance

Surveillance is the observation of a person or place to gain or confirm intelligence information, conducted by foot, vehicle, aerial, cyber, mechanical, and from a fixed location.[174] This section will describe the counter surveillance techniques practiced by the insurgent to defeat the counterinsurgent's attempts at surveillance.[175] Counter surveillance methods are those taken by the individual members for three purposes: to keep from being surveilled while conducting insurgent-related activities; to determine if under surveillance; and to thwart active and passive surveillance in order not to expose other members, operations, or physical infrastructure of the network, such as safe houses or caches.[176] During the Cold War, surveillance was a mix of stationary, foot, and vehicle surveillance.[177] These types of surveillance techniques can be used against cells and networks operating outside zones of conflicts where the threat to the surveillance team is minimal. However, due to the difficulty of counterinsurgent elements safely conducting foot or vehicle surveillance in a high-threat counterinsurgency environment, today's insurgents have to contend more with aerial surveillance, both manned and unmanned, as well as other types of intelligence-collection platforms. During the hunt for Abu Musab Zarqawi in Iraq, for example, an aerial-surveillance platform followed Zarqawi's spiritual advisor as he conducted a counter surveillance operation in which he quickly switched vehicles.[178] However, the aerial-surveillance package watched this counter surveillance maneuver and followed the spiritual advisor to where he met with Zarqawi, a fatal application of counter surveillance technique, leading to both of their deaths. Regardless of the types of surveillance employed by the counterinsurgents, low- or high-technology, the same basic counter surveillance principles apply.

The best method of counter surveillance is to keep from being detected in the first place. As DA PAM 550-104 noted in 1966,

> A former underground leader has suggested that while it is difficult to completely escape modern surveillance methods, there are many ways to mislead the surveillants. The underground member, wishing to minimize risks and chance factors, attempts to be as inconspicuous as possible and refrains from activities which might bring attention or notoriety. He strives to make his activities conform with the normal behavior and everyday activities of the society in which he lives.[179]

Having cover stories that provide a good reason for being in an area is one of the best methods of countering surveillance. For example, a clandestine network could use a delivery company driver as a courier, or could move large items, such as weapons, hiding them within the shipment, delivering the information and items as the driver makes his daily or weekly rounds within an urban area.[180] Along the same lines, a larger shipping company may ship items to numerous locations within a country or even across borders, giving the clandestine network long-range operational reach to support larger networks spread out over geographic regions or even into sanctuary areas in neighboring countries. The possibilities are endless.[181]

Soviet clandestine operations expert I.E. Prikhodko refers to these measures as "counter-surveillance check routes which afford the most favourable [sic] opportunities for the detection of surveillance."[182] As Prikhodko explains, these check routes provide the clandestine operator a method of determining if they are under surveillance through a combination of traveling by different means (car, bus, train) and through different areas (urban, rural, congested, and sparsely populated) that would expose any surveillance package by forcing them to betray their activity.[183] If no surveillance is detected after a certain period of time using the check route, the clandestine operator can be reasonably sure that he is not being followed.[184] This technique is used by both the leader and his subordinates if they are to meet, or conduct any other type of activity that may compromise other members or infrastructure if surveilled. This technique could also be used to move to and from safe sites, caches, or dead drop locations. If surveillance is detected, then the clandestine operator cancels the meeting or other planned activities so as not to expose the other elements of the network or he attempts to lose the surveillance and continue the operation.[185]

Emergency Methods for Re-connecting the Network

Cellular or compartmentalized networks are by their nature resilient to attacks that kill or capture single individuals, to include key leaders, facilitators, or specially-skilled individuals, who have superiors and subordinates. These individuals will be referred to as nodes for clarity in this section. By compartmentalizing the organization, the damage done by counterinsurgent operations is minimized and allows for the re-connection of the network above and below the lost node. In this case, when a node is removed, emergency clandestine communications measures must have been pre-arranged by the leader prior to his death or capture, to ensure that his subordinate and superior can link up.[186] This prearranged method is developed in such a fashion that the instructions do not lead to the compromise of either party.[187] Thus, the reconnection procedure must be systematic and clandestine principles applied throughout. Without some type of secure and clandestine mechanism to reconnect the network, the network can be successfully fractured, and would be indicative of poor clandestine practice.[188] In some cases, a network can reconnect if the members know each other well, but again, this ability is indicative of an insecure network that is operating more on luck than on any type of set clandestine procedures.[189]

In a well-structured clandestine cellular network, emergency communication methods are established throughout the organization from the higher level to the lower levels, as the organization grows, minimizing the threat of fracture.[190] The reconnection process can take place in four ways:

- Top down—the lost node's superior to subordinate
- Bottom-up—subordinate to superior
- Through a third party or intermediary, using a process similar to a live drop, providing a method for anyone in the organization to regain contact with the core network
- Through common knowledge of the other network members outside the individual's normal cellular chain of command, which happens in networks that are made up of individuals that know each other well[191]

Regardless of the method, the superior and subordinates may not know each other, and thus have to rely on pre-arranged recognition signals, codes, and specific actions when they meet.[192]

The first method is used when the higher level leader, the superior of the killed or captured node, makes contact with the subordinate through a pre-arranged method, such as a phone call and code word, or a visible signal, much like the one described by Orlov for marking a dead drop.[193] The superior establishes the special marking in a pre-designated location after the node has been removed. The subordinate knows that when he sees this emergency signal, he is to carry out the previously agreed upon action given to him by his former leader—such as calling a certain number and using a code name—going to a certain location at a specific time to meet someone.[194] Once the two elements have linked up, the superior can provide the subordinate with further instructions on what to do and how to maintain contact. The superior may elect to promote the subordinate to replace the lost node, replace the lost node with someone else, or fill the role himself. Regardless of the method, a superior practicing good clandestine technique will immediately establish a new form of cut-out to protect the superior and subordinate once the meeting is complete.[195]

In the second method, the subordinate contacts the superior.[196] This method would be most likely used if the leader of the subordinate was captured, and the subordinate was worried that his leader may provide information leading to the subordinate's arrest. This may force the subordinate to flee the operational area, nullifying any attempt by the superior to use pre-arranged signals in the old area of operation. In this case, another set of pre-arranged emergency procedures would be used, where the subordinate established an emergency signal at a pre-designated location to alert the superior. As before, this would lead to the link up of the two elements, and the reconnection.

The third method, much like the live-drop described above, would be a location, such as a business, provided to all the members of a network, to go in case of lost contact.[197] A code word or code name would then be used to alert the owner or workers of the need for the individual to get in touch with a network leader.[198] Once the subordinate initiates the code word, he is given further instructions on how the superior would contact them to affect the link up. This method is risky for the location owner and workers since it acts as a funnel for multiple individuals to use to get in contact with network leaders. The individuals working at the location could be detained in an attempt to get them to provide information on the superior's location. This was the main method of the Allied evasion networks during World War II, where pilots were given a location to go to in order to get funneled into the network, but the Axis was able to infiltrate numerous agents acting as Allied pilots to fully expose these networks.[199] If the superior has established a solid cutout between the location and himself, then he, theoretically, is protected. The superior can further protect himself by controlling the location of the meeting site and by establishing inner and outer security to observe if the subordinate is under surveillance prior to committing to the meeting.

In many cases, the superior and the subordinates do not know each other, which requires further application of clandestine methods during the actual physical link-up to ensure positive identification. It is the physical act of contact with an unknown subordinate that puts the superior at greatest risk.[200] He has to assume that the subordinate may have been detained, turned by the counterinsurgents, or perhaps provided them with the re-contact plan, and they have inserted an infiltrator, taking advantage of the lack of direct knowledge of the individual.[201] Due to this threat, the link-up is one of the most dangerous acts, and thus requires further application of clandestine methods.[202] It would be easy to meet at a pre-designated isolated location; however, this would make counterinsurgent surveillance easier if the subordinate was in fact working for them. Instead, the superior wants to blend in and use the human terrain to his advantage.

To do this he will establish a meeting location, likely in a very public place, such as a restaurant or market, with numerous escape routes.[203] The location would also provide an environment in which his inner and outer security elements could also blend into, or maybe even be part of the chosen environment, such as storeowners, sellers, and buyers in the market, or other jobs that are natural for the surroundings, in order to identify counterinsurgent surveillance. If the superior has indirect contact with the subordinate and can pass messages, he may provide detailed instructions, describing the exact route to take and providing a set of signals for recognition, emergency abort, and safe signals, as well as an alternate meeting plan if there is a reason the meeting cannot be carried out.[204] These instructions may also be passed through dead or live drops as well. If conducted correctly, the inner and outer security should be able to identify surveillance or determine if the subordinate is "clean." If they discover surveillance is following the subordinate, then the meeting is cancelled, and the superior escapes.[205] If not, then the superior and subordinate meet after exchanging recognition signals and code words to verify identities, and then they can begin the process of reestablishing the network.

The final method happens in poorly compartmentalized networks and in networks built on pre-existing friendships, acquaintances, or groups, such as clans and tribes. In these cases, it is possible for individuals to re-link into the network through known individuals. This technique, with numerous links that bypass any cut-outs, such as members of one cell that interact with other cells, is indicative of a network with poor compartmentalization and clandestine practices, and could generally be categorized as an unsecure network that is operating at a very high risk. Sherri Greene Ottis' *Heroes: Downed Airmen and the French Underground* describes this method being used by some evasion line networks in WWII to return downed pilots to allied control.[206] In some cases it worked, mostly out of luck, but for the most part, it led to the destruction of multiple escape lines in World War II throughout occupied Europe.

It should also be noted that regardless of the method of reconnection, once the link-up is successful, the superior will determine how best to reestablish the intermediate node. This will be done either through promoting the subordinate of the lost node, bringing in an outside individual that had not been previously part of the network, or simply by the superior taking over the role himself.[207] The course of action is likely determined prior to the meeting so that the superior only has to expose himself once during this emergency reconnection. If he can reestablish the cut-out simultaneously, then once the two depart, the network is generally safe again. If either individual is picked up leaving the site, they will not know the whereabouts of the other one. With the cut-out reestablished and the new reconnection instructions and clandestine communications instructions passed to the subordinate, the network can once again reconnect if one of the individuals is captured or killed by security forces soon after the face-to-face meeting.[208]

Clandestine Recruiting

Although there is a perception that clandestine networks are largely made up of trusted and known friends and family members, reality throws this logic into a spin.[209] For an insurgency to be successful, it must increase in size and control.[210] While family and friends provide an added sense of security through loyalty bonds, and may well make up the members of the core group, few insurgent movements can be successful only having the support of their close friends or family, including tribes and clans. They must branch out and increase their popular support in order to affect large political change. To do this, the organization must grow with purpose in order to gain access to the population for resources, to replace losses, and to gain access to areas to target counterinsurgent forces. Thus, unlike information-age networks that grow randomly or without any control mechanism, such as the Internet or social networks, clandestine networks grow with purpose—identifying low-risk individuals that bring skills, resources, intelligence, or access to targeted areas.[211] These individuals go through a process of clandestine recruiting.[212] Unlike the strong links between trusted individuals that have developed trust relationships prior to partaking in nefarious activities, clandestine recruiting is largely a method for recruiting unknown individuals or acquaintances of others, a form of social networking, and thus a weak link to the clandestine recruiter.[213] Generally, the recruiter is a network member that is purposefully gaining more links. The recruiter may or may not be a network leader, recruiting his subordinates directly. He could be a member of the core network who has the right kind of background or natural talent for recruiting, who recruits new members based on organizational needs, and then passes the recruit off to a network leader for actual operational control.[214] This may in fact protect the network if the recruiting effort goes bad and a potential recruit turns in the recruiter. In this case, having good cut-outs between the network and the recruiter further protects the network.

The key for the clandestine recruiter is to never let on that he is recruiting for the insurgency until he has used his skills to identify, assess, and possibly test the candidate for recruitment. He must be reasonably certain that the recruit will accept his recruitment offer when finally approached.[215] The recruiter is looking for a recruit who has a personality for clandestine work; the right motivation, trustworthiness, and loyalty; special skills or military background; access to a specific target location, population, intelligence, or resource of importance to the insurgency; and has the proper background—ideological, ethnic, or religious—to support the core movement's agenda.

The key for the clandestine recruiter is to never let on that he is recruiting for the insurgency until he has used his skills to identify, assess, and possibly test the candidate for recruitment.

In some cases, if there is doubt about the recruit's willingness to work with the insurgency, the recruiter may have embarrassing background information to blackmail the recruit or he may simply gain compliance through coercion and threats to kill the recruit or members of the recruit's family if he does not cooperate.[216] If the person declines the offer to work with the insurgents, then the same methods of blackmail or coercion can be used to keep them from going to the counterinsurgents.

Another purposeful growth model, other than recruiting, includes insurgent leaders marrying into families, tribes, or clans, to gain instant rapport, loyalty, commitment, and access to the resources of the group, much like the monarchies of old, where the sons and daughters would be married to link kingdoms or countries.[217] This technique depends on the cultural and societal norms, but may effectively unite groups quickly. This is a favorite technique of al-Qaeda to try to quickly gain the trust and backing of tribes, as was evident in al-Anbar in the year leading up to the "Anbar Awakening."[218]

Safe Houses

Safe houses are used as part of core members' daily pattern of hiding from counterinsurgent forces, or if members are under pressure of pursuit by counterinsurgents and "need to go underground."[219] Safe houses are locations that should not draw attention, nor be readily connected to any pattern of insurgency or criminal activities.[220] These locations give the user a place to hide or stay that has a built-in but invisible inner and outer security ring to provide early warning and protection.[221] Key leaders may use a series of safe houses daily to allow them to change location regularly to thwart attempts by counterinsurgency forces to interdict them. They generally move based on either early warning or within the amount of time they believe it would take for the counterinsurgents to gather intelligence, develop a plan, get approval, and conduct the operation. This may cause them to move every few hours or days, depending on the perceived threats, the capability of their early warning, and how good an escape plan they have. It is not uncommon to hear of insurgent leaders who move every few hours each day to make sure that they are not captured.[222] If the counterinsurgents conduct operations against the safe house, but miss the insurgent leader, then the insurgent leader knows that he cannot reuse that safe house location without an increase in risk since the house may be under surveillance, or the informant that provided the information that drove the counterinsurgents to raid the location may still be active.

As shown in Figure 6, safe houses are maintained by a subordinate leader as part of an operational support network.[223] The person that maintains the safe house is not involved in any other organizational functions so as not to draw attention and jeopardize the safe house.[224] The leader uses the safe house or safe location as randomly as possible so as not to provide the counterinsurgent with a distinguishable pattern amongst several safe houses.[225] At each location, a system of emergency signals would alert the user whether the location is safe or not. For example, safe signals may be the "predesignated [sic] placement of shutters; flower pots; arrangement of curtains; open or closed windows; or clothes hanging on clothes lines."[226] Changes to these pre-designated signals would alert the leader that the site was not safe. The leader may also establish a personal evasion network or line, also depicted in Figure 2, in which he establishes all the safe houses, safe-house keepers, and movement plans himself so no one else in his organization knows.[227] This gives the network leader the ability to escape if the rest of his organization is detained. The evasion may be interstate, or extend over borders into sanctuary areas or other international locations.[228]

Security at a Location

Security at any location, such as meeting sites, safe houses, and dead drops, provides a means of early warning to give the network members an opportunity to escape or not approach the location.[229] To conduct this type of operation, the member responsible for establishing the location must have good communications with the members conducting security in order to get near real-time warning of impending danger. Two security rings are established—inner and outer.[230] Inner security is responsible with immediate security around the site, and may be armed to disrupt any counterinsurgent operations that penetrate the outer security without being detected in order to give the underground members time to escape. Outer security observes likely routes into the location that the counterinsurgents may use. A system for communicating must be established, and may include cell or telephones, short-range radio, signals, or runners.[231] There should also be an agreement on actions of the security elements and the individuals at the location, whether to fight, flee, or if the security elements will fight the counterinsurgents to give the key network members a chance to escape.[232]

In some cases, the security elements may simply be passive, watching key counterinsurgency locations such as bases or airfields, or the security elements may be individuals infiltrated onto one of these installations—such as cooks, maintenance personnel, laundry facility workers, contractors, or even interpreters— that provide a form of outer-ring early warning, but within the enemy camp.[233] This passive security measure could include overhearing conversations between soldiers about upcoming missions or information found in the trash. In the case of locally hired interpreters, they may even be directly briefed on upcoming missions against the network that they actually work for, thus providing the ultimate security and situational awareness for the network leaders. If the interpreter deems the threat to be immediate, then he can risk calling the network leader direct with the warning. In the case of infiltrators whose duty does not allow for daily movements on and off the counterinsurgent installation, such as the interpreter who may have ongoing operations or strange hours due to ongoing operations, or the information is not time sensitive, then another clandestine communication method can be used. For example, other local-hires purposefully infiltrated onto the installation by the network leaders with regular daily schedules may be the courier between the network leaders and interpreter or other intelligence gatherers. In this case, they may use a dead or live-drop procedure to pass the information, or the courier may use the same method to pass instructions from the leaders to the agent.

Other passive outer-ring security techniques may include recruiting business owners whose businesses sit astride likely counterinsurgent routes, or even outside the gates of counterinsurgent installations. The movie *Blackhawk Down* also provides an example of outer security, where a young boy is paid to sit and watch over the airfield. He then phones the cell leader to report activity, in the case of the movie, the over flight of a large helicopter assault force departing the airfield.[234] Passive security can consist of anyone who does not draw the counterinsurgents' attention.

Clandestine Skills Training

New and old members must be continually trained and tested on the clandestine methods above to make sure they are not violating the clandestine procedures of the network.[235] As Prikhodko explains,

> Clandestinity in agent operations is directly dependent on the indoctrination...keeping in mind the main objective: to offer assistance, to show how to fulfil [sic] his assigned task better and more securely, [and] to help correct mistakes he has committed or eliminate inherent shortcomings.[236]

However, the best training is risky due to the fact that the leader and subordinate must meet in person until the leader is confident that his subordinate is trained.[237] This training can take place in any secure location and may include any of the functional skills described above, as well as operational skills required by the individual, such as the employment of new weapons systems.[238] As Prikhodko notes, "The [network, branch, or cell leader's] task is to train [subordinates] properly and to transfer [them] to impersonal forms of communications in good time."[239]

If the insurgency is receiving external support and is directly working with intelligence or special operations personnel from the external supporter, personnel may undergo specialized training in tradecraft and other clandestine operational capabilities. During the Cold War, communist insurgent leaders received extensive training by communist regimes, especially the Soviets, such as the courses taught at the Lenin School.[240] The ability of nation-states and non-state actors to provide this type of in-depth training continues today, but much more covertly, to provide plausible deniability, such as the training provided by Iran to Iraqi Shi'a insurgents.[241] This training may be conducted simply during a personal meeting between the underground member and the external support representative locally or could include training outside the country of conflict, such as in sanctuaries or other locations chosen by the external supporter. Person-to-person training, as noted above, increases the risk of all parties involved, but training at external sites provides the opportunity for intense training to be conducted while not under pressure from the counterinsurgents.

The last method is training conducted almost as independent study, including reading historic literature, manuals produced by the insurgent organization, or online references. Obviously, this is the least preferred method for training individuals in the organization. The Internet provides a balance, with the ability to provide video, and rapidly disseminate new tactics, techniques, and procedures, but still far from perfect. Without controlled or precision distribution to desired individuals, the counterinsurgent can view and learn from these as well. The medium for distribution may also not reach isolated individuals. Stratfor's Fred Burton correctly identifies the problems with this type of training in tradecraft,

> While some basic [clandestine] skills and concepts…can be learned in a classroom or over the Internet, taking that information and applying it to a real-world situation, particularly in a hostile environment, can be exceedingly difficult. The application often requires subtle and complex skills that are difficult to master simply by reading about them: The behaviors of polished tradecraft are not intuitive and in fact frequently run counter to human nature. That is why intelligence and security professionals require in-depth training and many hours of practical experience in the field.[242]

Thus, freedom of movement is paramount for clandestine leaders to gain access to their network members, especially new members, and provide clandestine training if they expect their subordinates to survive.

This is one reason why prior to transitioning from the latent and incipient phase to other phases of an insurgency, the core group attempts to establish an extensive clandestine cellular network, to include training subordinates, before counterinsurgent operations and population control measures can be implemented. This requirement for personal contact for training provides counterinsurgents with an exploitable weakness of clandestine networks—the requirement for freedom of movement. Without freedom of movement, the result of population-control measures that isolate the population from the insurgents, the insurgent leaders are unable to replace, further develop, or grow a clandestinely competent network that has a chance for long-term survival. This explains why the periphery or edge elements, the "low-hanging fruit" of the clandestine organization, may receive little or no clandestine training since these elements can be replaced more easily and with less risk to the network than it would take to train them to be proficient.[243]

Considerations for Elements at the Edge of the Clandestine Organization (Cells and individuals)

Unlike other parts of the clandestine cellular network, the edge elements are generally poorly-trained individuals hired specifically to carry out attacks on the counterinsurgents. By their very nature, these are the highest-risk operations carried out by the clandestine network. If the skills required to conduct these attacks are minimal, then the hiring of less skilled, but more abundant individuals is preferred. The training these individuals or cells receive on clandestine arts will depend solely on how easy they are to replace. The harder to replace, the more time the network leadership will spend to train them to minimize their signature and provide them with some level of protection.

These types of cells and individuals are the true “low-hanging fruit” of a clandestine cellular network and likely consist of individuals that are hired to carry out direct attacks or intelligence collection against the counterinsurgent force. In most cases, these cells consist of individuals that are formed by a cell leader who may or may not have training or experience in clandestine operations. Generally, the cell leader is the only individual that links to the main network through a cut-out, while the rest of the cell communicates amongst themselves. These individuals may simply be in need of money, desire to regain honor by fighting the counterinsurgent directly, or they are not competent enough for higher levels of responsibility within the organization.[244] They are hired to participate with the recognition by the network leadership that they will likely not survive long against competent counterinsurgents. Even with little training, they will cause some disruption in the counterinsurgent activities, but can be quickly replaced by other individuals with similar needs (money, regain honor, et cetera) if or when interdicted.

The only thing that matters to the leader is that there is a solid cut-out between the cell and the clandestine organization. If the leader can replace a cell simply by paying a group of individuals to attack the counterinsurgent force, he can repeat this process indefinitely. There is no incentive to waste time and risk his exposure trying to link-up to train the group in clandestine arts or to expose himself to try to physically reconnect the cell to the network if the cell is interdicted.[245] This is especially pertinent when the cell is responsible for engaging the enemy, either directly with small-arms fire, or indirectly with an explosive device, and thus becomes a priority target of the counterinsurgent.

This attention these edge organizations draw from the counterinsurgent serves an additional purpose, intentionally or not. Simply based on requirements for force protection, the local counterinsurgent force will have the local cells and individuals on their high priority target lists for interdiction.

If the cell is very proficient, then the counterinsurgent may become solely focused on capturing or killing the cell. The proclivity of U.S. and the West counternetwork operations to focus on these kinetic elements of the insurgency provides the true clandestine organization with a built in "security buffer." Thus, the counterinsurgent is focused on the most kinetically active elements of the insurgency, and therefore is unable to focus on the non-kinetic elements of the clandestine cellular network that are of greater danger to the overall COIN effort. In effect, these less-trained and sophisticated elements end up being the primary target of the counterinsurgent.[246] This provides the clandestine cellular network with time and space to provide support to other elements that are achieving the tactical, operational, and strategic objectives of the movement.

Lastly, there is little requirement for emergency reconnection of edge elements when they are interdicted. Even if a cell member manages to evade capture and escapes from or is released by the counterinsurgents, the clandestine leaders must decide if it is worth the risk to reincorporate the individual. Before the leadership conducts procedures for emergency reconnect, the leaders of the clandestine network must trust the individual enough to reincorporate them into the organization. Since these elements are easier to replace, the leadership may decide that the risks for re-incorporating an individual that may be under control or surveillance of the counterinsurgent are too great. In this case, this individual will not be reincorporated or even contacted.

Section Summary

This section described how clandestine networks use function—clandestine art or tradecraft—to minimize signature and thus detection by counterinsurgent forces. The form in this case is functional compartmentalization, which complements the organizational and structural compartmentalization described earlier. Functional compartmentalization refers to the actions of the network members to reduce the signature of the interactions between members. This is done to "hide" the network from the counterinsurgents in order to protect the clandestine cellular network from effective counternetwork operations.

This section analyzed historic examples of different types of clandestine interactions to provide the reader with a deeper understanding of the types of actions that take place in clandestine cellular networks including personal and impersonal communications, how networks reconnect when nodes are removed through counternetwork operations, counter surveillance, and recruiting. This section also discussed how insurgents learn and how they risk the interdiction of the less-trained elements along the edge or periphery of the actual clandestine network to attack the counterinsurgent.

Thus, this section's explanation of functional compartmentalization and signature reduction, along with the previous section on organizational and structural compartmentalization together provide the resilience of the clandestine cellular network. Through both the form and function, the clandestine cellular network is able to ensure its survival, the ultimate logic of the clandestine cellular network.