

# TROJAN HORSES: USING CURRENT U.S. INTELLIGENCE RESOURCES TO SUCCESSFULLY INFILTRATE ISLAMIST TERROR GROUPS

JAMES O'BRIEN

*Fighting the War on Terror will continue to require many organizational, strategic and tactical changes, including new methods of covert action that can be effectively employed against closed, fanatical terrorist groups like al Qaeda. This paper argues that the United States should attempt to use Western terrorist organizations to penetrate Islamic extremist groups. The paper examines the feasibility of using derivatives of the Irish Republican Army and Russian organized crime as "trojan horses" capable of approaching and identifying Islamic terrorists in the market for documents, weapons, and other illicit materials and/or services. The paper concludes that, while there are many risks and difficulties in applying this tactic, it is superior to other options and has viable success potential.*

## INTRODUCTION

The United States has declared war on terrorists. To fight this war effectively requires reliable intelligence. However, a critical gap exists in U.S. intelligence capabilities that will continue to place the United States at a significant disadvantage, namely, the inability to infiltrate Islamic extremist terror groups. During the Cold War, CIA operatives

---

**James O'Brien** is currently enrolled at the International Security Studies Program at the Fletcher School of Law and Diplomacy, Tufts University, as a Jack Kent Cooke Foundation Graduate Scholar. His specific interests are Iranian backed terror groups and Tehran's exportation of radical Shi'ism.

focused on “turning” agents of the Soviet Union (and other communist bloc countries) to gain access to the inner circles of the enemy. This approach is not likely to be as effective today: there is very little leverage that an operative can hold over a fundamentalist willing to commit self immolation in the name of jihad. The tight-knit structure of Muslim

***There is very little leverage that an operative can hold over a fundamentalist willing to commit self immolation in the name of jihad.***

terror groups makes turning agents even more far-fetched. In addition, the decentralized structure of organizations such as al Qaeda reduces the quantity and quality of information a turned agent may be able to provide. Nevertheless, the direct penetration of terror groups by U.S. operatives will have to be secured in order to achieve

the goal of credible intelligence collection. Although long-term solutions have been proposed—and these solutions should be pursued—the length of time necessary to effectively implement these changes endangers the lives of millions.

Once U.S. intelligence operatives become well prepared for the task of penetrating terror groups, these operatives are still likely to face obstacles to deep infiltration. Such obstacles include family or clan-based recruiting mechanisms, cultural peculiarities that differ among localities and communities that epitomize “six-degrees-of-separation.” Such obstacles may prove fatal to countless operatives, and even if penetration is achieved, it may take years to cultivate the trust necessary to gain access to the inner circles of a terror group’s hierarchy. This is assuming that the operatives will not have to carry out an act that shows proof of commitment – such as a suicide mission. The decentralized structure of terror groups further complicates leadership infiltration because many of the members of an extremist cell will often have limited actionable intelligence on a terror group’s senior leadership beyond their immediate supervisor. To deal with the Islamic terrorist threat and a recognized human intelligence (HUMINT) deficiency, this paper examines two questions: (1) *What can U.S. intelligence do to gain access to the terrorist hierarchy?* and (2) *What tools can the United States employ from its current arsenal that can achieve intelligence objectives rapidly?* The proposed answer: *Instead of working to penetrate terror groups directly, U.S. counter-terrorism operatives should penetrate the groups that either provide, or have the*

---

*means to provide, services to Islamic extremist groups.* The U.S. intelligence community can exploit this vulnerable *backdoor* of terrorist organizations, namely, their dependency on criminal elements to facilitate their terrorist needs. The U.S. intelligence community has a proven track record of penetrating two organizations that have close ties to such terror groups—the Irish Republican Army (Provisional and Real) and Russian organized crime. By using these organizations as *trojan horses*, the United States may be able to achieve key terrorist monitoring objectives, including terrorist identification and insight into planned attacks.

## STATEMENT OF THE PROBLEM

The fact that a HUMINT deficiency exists for the United States is not news. Consider the following testimony provided by Bruce Hoffman, Vice President of External Affairs Washington Director of the RAND Institute to the U.S. House of Representatives Permanent Select Committee on Intelligence:

It is not surprising therefore that America's HUMINT (human intelligence) assets have proven so anemic given a military orientation that ineluctably feeds on technological intelligence such as MASINT (measurement and signature intelligence), ELINT (electronic intelligence) and SIGINT (signals intelligence) collected by spy satellites orbiting the planet. Given the emergence of formidable, transnational, non-state adversaries, and the lethally destructive threats that they clearly pose, this balance is no longer appropriate. Moreover, our own HUMINT deficiencies, which forced us to rely on information provided or forthcoming from liaison services, has clearly been shown to be wanting in the wake of the failure of any of our allies to provide warning of the September 11th operations.<sup>a</sup>

U.S. hyper-dependence on high-tech for intelligence gathering has been derided in many post-9/11 articles dealing with the subject, including *The 9/11 Commission Report*. Over the past five decades, the U.S. intelligence community has simply supplanted operatives with satellites and other forms of electronic eavesdropping. This is a reflection of the Cold War environment within which U.S. intelligence matured.

<sup>b</sup> Initially seen as a positive development, the ability to see the enemy from space enabled the United States the type of oversight necessary

in a bipolar world order governed by mutually assured destruction. As the world reverted to a multifaceted political environment, the security environment changed with it, diminishing the positive returns once gained by multi-billion dollar imagery and sensory equipment. The nature of the threat today is no longer large conventional militaries and fixed missile facilities that produce enormous signatures; the threat is small, mobile and very human. Thus, the recent increased emphasis on HUMINT as a primary component of any comprehensive intelligence reform is not only a reflection of a recognized operational deficiency, but also a reflection of the new type of threat facing the United States: terrorism perpetrated by Islamic extremists.

This new enemy has learned how to evade high-tech methods of information gathering. *The 9/11 Commission Report* describes an operation that was conducted by rather ordinary people, albeit fanatical, but

not particularly skilled. The terrorists were assisted by a host of other ordinary people in many countries, including within the United States. The weapons used were unsophisticated but effective: box cutters and pocketknives. From start to finish, with the exception of the flight school training, the al Qaeda 9/11 strikes were a decidedly low-tech operation.<sup>c</sup> The lesson learned from 9/11 is that future terrorist attacks will be conducted in ways that raise few suspicions, carried out by individuals who have the ability to thrive under the radar. The emphasis of counterterrorism, therefore, should be placed on stopping terrorist operatives from achieving success, while simultane-

ously working to take down the networks that employ them. The first step will be identifying the enemy. *The 9/11 Commission Report* states that "...the enemy is not just 'terrorism,' some generic evil. This vagueness blurs the strategy. The catastrophic threat at this moment in history is more specific. It is the threat posed by *Islamist* terrorism-especially the al Qaeda network, its affiliates, and its ideology."<sup>d</sup> The 9/11 Commission's definition of "*Islamist* terrorism" as "the catastrophic threat at this

---

***The recent increased emphasis on HUMINT as a primary component of any comprehensive intelligence reform is not only a reflection of a recognized operational deficiency, but also a reflection of the new type of threat facing the United States: terrorism perpetrated by Islamic extremists.***

moment in history” provides U.S. security strategists with an identity. However, the designation of so specific a threat also provides an instant challenge to the U.S. security community, especially as it relates to the intelligence sector. The combined dynamics of an Islamist threat and a recognized HUMINT deficiency challenges the intelligence community to fix an inadequacy while working within a tightly confined demographic space. This will prove to be a daunting task.

Professor Richard Betts, Director of the Institute of War and Peace Studies at Columbia University, notes the following about human intelligence and the role of cultural diversity in the United States:

Despite our huge and educated population, the base of Americans on which to draw is small: there are very few genuinely bilingual, bicultural Americans capable of operating like natives in exotic reaches of the Middle East, Central and South Asia, or other places that shelter the bin Ladens of the world.<sup>e</sup>

Having a diverse population is not sufficient for the task of broadening U.S. HUMINT capabilities. Muslim terrorist group penetration, if it occurs at all, is conducted by either recruiting or “turning” proxies, or by utilizing allied foreign operatives.<sup>f</sup> Unfortunately, some “allies” are less reliable than others. Saudi Arabia is a case in point: while vocalizing support for the United States, key figures within the Saudi government assist anti-Western terrorist groups in a variety of ways.<sup>g</sup> Consequently, while U.S. policymakers are emphasizing the need for rapid intelligence overhaul to close the HUMINT deficit, the United States is fighting a War on Terror with other countries’ unreliable eyes.

***While U.S. policymakers are emphasizing the need for rapid intelligence overhaul to close the HUMINT deficit, the United States is fighting a War on Terror with other countries’ unreliable eyes.***

Nevertheless, it is easier to recognize HUMINT deficiencies than to fix them. This is especially true when reconstituting sectors spread over several agencies that have been allowed to corrode. There is no quick fix in resolving this deficiency. This reality is recognized by both policy advisors and policy-makers, who propose long-term investments in intelligence reform. A 2002 Congressional Research Service report exemplifies this mindset:

First is a renewed emphasis on human agents. Signals intelligence and imagery satellites have their uses in the counterterrorism mission, but intelligence to counter terrorism depends more on human intelligence (HUMINT) such as spies and informers. Any renewed emphasis on human intelligence necessarily will involve a willingness to accept risks of complicated and dangerous missions, and likely ties to disreputable individuals who may be in positions to provide valuable information. *Time and patience will be needed to train analysts in difficult skills and languages.*<sup>h</sup>

Unfortunately, the “time and patience” necessary to develop these operatives is not a luxury the United States can afford. *The 9/11 Commission Report* describes the rapid nature and lack of warning that defines the current security environment:

National security used to be considered by studying foreign frontiers, weighing opposing groups of states, and measuring industrial might.... Threats emerged slowly, often visibly, as weapons were forged, armies conscripted, and units trained and moved into place....

Now threats can emerge quickly. An organization like al Qaeda, headquartered in a country on the other side of the earth, in a region so poor that electricity or telephones were scarce, could nonetheless scheme to wield weapons of unprecedented destructive power in the largest cities of the United States.<sup>i</sup>

Furthermore, even if the United States succeeds in developing the types of intelligence operatives with the skill sets desired for an effective war against Islamic extremists, the capacity to penetrate these groups will likely never be fully achieved. The problem is that Islamic terrorist groups are highly insulated from outside intrusion because of their family-based and/or clan-based recruitment policies: “Ethnically based terrorist groups recruit new members personally known to them, people whose backgrounds are known and who often have family ties to the organization. Intelligence penetration of organizations recruited this way is extremely difficult.”<sup>j</sup> Even those organizations that do not recruit exclusively through family ties, such as al Qaeda, still employ a severe level of vetting that places an operative’s survival in jeopardy. Regional dialects, local cultural sensitivities and “six-degrees-of-separation” within small populations all work against an operative attempting to secure a terrorist leader’s trust. Recognizing these difficulties, Rich-

---

ard Betts summarizes this operational reality: “More and better spies will help, but no one should expect breakthroughs if we get them. It is close to impossible to penetrate small, disciplined, alien organizations like Osama bin Laden’s al Qaeda, and especially hard to find reliable U.S. citizens who have even a remote chance of trying.”<sup>k</sup> Nevertheless, the intelligence community should pursue HUMINT reform that will develop operatives with penetration potential, but accessing the inner circles of terror groups may take years to materialize, or may even be impossible. For example, if the operative is accepted by a terror group, he may be isolated or removed from the organization’s hierarchy, leaving the operative uninformed as to what other groups within the same organization are planning, including the cell within which he may be operating.<sup>l</sup>

Therefore, recognizing the U.S. HUMINT deficiency, the lengthy process of comprehensive reform, the unpredictable nature of terrorism as a constant imminent threat, and the insulated structure of terrorist groups, the United States will need to employ creative methods to collect information without jeopardizing long-term intelligence reform. Bruce Hoffman suggests “some new, ‘out-of-the-box’ thinking that would go beyond simple bureaucratic fixes.”<sup>m</sup> One possibility is taking a backdoor approach to penetrating various fundamentalist terrorist organizations.

*The “Achilles heel” of terror groups is their dependence on criminal or other interconnected terrorist groups to provide certain services to them, specifically weapons and drug smuggling.*

## **SOLUTION PROPOSED: WORK WITH THE TOOLS WE HAVE**

### **THE BACKDOOR**

One backdoor ripe for exploitation is the dependence of Islamic extremists on illicit activities and services to fund, train, and/or facilitate their operations.<sup>n</sup> The “Achilles heel” of terror groups is their dependence on criminal or other interconnected terrorist groups to provide certain services to them, specifically weapons and drug smuggling. The United States should exploit this dependence and has the capacity to do

so. This backdoor should be envisioned just as the name connotes: an alternative entrance that is easier to sneak into than the front door. In the world of computer programming, a backdoor is “an undocumented way of gaining access to a program, online service or an entire computer system. The backdoor is written by the programmer who creates the code for the program. It is often only known by the programmer. A backdoor is a potential security risk.”<sup>o</sup> When hackers discover backdoors in software programs, they exploit them. The U.S. intelligence community should adopt the hackers’ approach; infiltration agents should be looking for similar types of alternative access routes.

Like the fabled ruse used by the Greeks to breach the walls of ancient Troy, a “trojan horse” refers to a programming technique employed by computer hackers to breach otherwise secure software programs. A trojan horse is defined as “a destructive program that masquerades as a benign application. Unlike viruses, trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of trojan horses is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.”<sup>p</sup> Similarly, in order to gain backdoor access to the hierarchy of Islamic terror groups, especially Al Qaeda, this paper recommends using a trojan horse approach by manipulating the terror groups’ reliance on outside organizations. The organizations that should be carefully considered as potential trojan horses are the Irish Republican Army (IRA)—Provisional (PIRA) and/or the Real (RIRA)<sup>q</sup>—and/or Russian organized crime.

### **TROJAN HORSES**

The IRA and Russian organized crime enjoy close ties to fundamentalist terror groups, although for different reasons. At one time, the IRA was the world’s premier proliferator of terror; it provided training, weapons/weapons expertise, money, and even services to terror groups as diverse as Hamas, Euzkadi Ta Askatasuna (ETA),<sup>r</sup> and the Fuerzas Armadas Revolucionarias de Colombia (FARC).<sup>s</sup> The IRA has also enjoyed the protection of terrorist proliferators such as Libyan leader Muammar Qadhafi<sup>t</sup> and Cuban dictator Fidel Castro.<sup>u</sup> Although the IRA has most often been moderated by political considerations, recent trends in its activities indicate that ideological considerations no longer hold the

---

same weight they once held prior to signing the ceasefire known as the “Good Friday Peace Accords.”

Russian organized crime, in contrast, has not broken from its primary ideology: greed. As a result, elements of opportunistic Russian organized crime members have sold weapons to terrorist organizations throughout the world. Whereas the IRA has won the support of terror groups through years of anti-British violence and open support for the Palestinian cause, Russian organized crime has earned its reputation through a cold-blooded business ethic that does not discriminate where profit is involved. Thus, both organizations share positive relations with terror groups that the United States is targeting.

The fact that violent Islamic extremist groups enjoy good working relations with organizations such as the IRA and Russian organized crime should be seen as an opportunity to deal with the intelligence penetration problem. U.S. intelligence and law enforcement agencies have a proven track record infiltrating these organizations. Rather than waiting to develop a HUMINT program that can produce capable operatives—a timeframe that may prove too costly—the United States can use an existing capacity it already has to penetrate and monitor extremist pockets. Both the IRA and Russian organized crime offer a critical commodity and a credible motivation to terrorist groups. The commodity: confirmed weapons smuggling capabilities into the United States and Great Britain that would be highly attractive to terrorist groups seeking to “rival the events of September 11.”<sup>v</sup> Their credible motivation: money. The United States should use the trojan horse approach to exploit these motivations. *By hiding behind a criminal façade, Islamic extremists may unwittingly welcome U.S. Intelligence operatives into their inner circles.*

## STRUCTURE

This paper will cover two proposed trojan horses: the IRA and Russian organized crime. Beginning with the IRA, it will first present this group’s global reach and international credentials prior to and after

the Good Friday Peace Accords. This paper will illustrate the degenerative impact of the ceasefire on the IRA, especially the disintegration of discipline within the rank-and-file members due in part to a loss of funding. It will analyze the impact of these factors upon the various factions of the IRA and chart the organizations' increasing turn toward organized criminal behavior. This paper will then consider the credentials that the IRA currently possesses to make a convincing trojan horse: the documented erosion of restraint by low-level IRA operatives now serving themselves due to a loss of cash subsidies since the ceasefire. Completing this section, this paper will present examples of U.S. and British penetration into the two principle branches of the IRA—the PIRA and the RIRA—and how the U.S. intelligence community can exploit this penetration.

The next section will deal with Russian organized crime. It will present its global reach and reputation, followed by previous examples of interaction between Russian organized crime and Islamic terror groups. This will be followed by a brief synopsis on U.S. law enforcement's proven capability to penetrate Russian organized crime. An envisioned scenario for utilizing a Russian organized crime cover will complete this section.

The conclusion of this paper will provide an analysis of the policy prescription. The pros and cons of employing a trojan horse tactic will be weighed. The viability of such a tactic will be assessed, and likewise the problems inherent in such an ambitious scheme will have to be addressed: *What might go wrong? What issues may arise in agency coordination? What are the risks to the operatives involved?*

## **PROPOSED TROJAN HORSE #1: THE IRISH REPUBLICAN ARMY**

### **CURRENT STATE OF THE IRA**

The Provisional Irish Republican Army (PIRA), and their more violent offshoot, the Real IRA (RIRA), have been two of the most active terrorist groups within the current trend of terrorist group interconnectivity.<sup>w</sup> Examples of PIRA and/or RIRA complicity in propagating terrorist tactics include the recent increase in urban operations by the FARC,<sup>x</sup> the presence and subsequent arrest of an IRA explosives expert

---

in the West Bank,<sup>y</sup> and over two hundred IRA- designed pipe bomb booby-traps designed to kill Israeli troops in evacuated Jenin refugee camps.<sup>z</sup> Illustrating their impact on modern terror beyond the operational level, the Council on Foreign Relations attributes the advent of a cell structure to the IRA, stating the following: “The group honed the ‘cell’ structure that Osama bin Laden’s al-Qaeda network has also adopted.”<sup>aa</sup> Furthermore, the IRA has enjoyed ties to terrorist sponsor states such as Libya, Syria and Cuba; all of which have had established relations with anti-American terrorist organizations. The global reach and credibility of the IRA enables its members to access organizations that have long since precluded most westerners. From Euskadi Ta Askatasuna (ETA) to the Palestinian Liberation Organization (PLO), the IRA enjoys immense respect. (This is especially true of the PIRA, which has built a cooperative reputation for itself over the past thirty-some years.)

***The global reach and credibility of the IRA enables its members to access organizations that have long since precluded most westerners.***

Still, it should be noted that the PIRA is not the same organization it had been prior to signing the Good Friday Peace Accords in April 1998. Since 1969, when attempts at securing Irish-Catholic civil rights in Northern Ireland erupted into bloodshed, the PIRA has been at the forefront of the political violence.<sup>ab</sup> The PIRA has been the face of Irish terrorism for three decades, despite periodic challenges from more violent groups such as the Irish National Liberation Army (INLA). Beginning in the early 1990s, PIRA experienced a decline in activity. This may be partially due to the fact that its political face, Sinn Fein, gained some genuine political clout with the election of its president, Gerry Adams, to the Irish parliament in 1988 and his return to parliament in 1997 and 2001. In fact, for the better part of the 1990s, the PIRA was quieter than in previous decades. Although the group is still active, the PIRA has suffered a steady decline since 1991 due to three major factors:

1. The loss of Soviet subsidies in the early 1990s forced the PIRA to engage in crimes, such as bank robberies, narcotics distribution and racketeering, as a way of generating revenue. The PIRA, which once enjoyed strict discipline in the ranks, has since found itself undermined by the activities of less cautious mavericks.<sup>ac</sup>

2. The Good Friday Peace Accords created a rift between more violent members within the organization and those in support of a peace deal, the result being the formation of three IRAs: PIRA, RIRA and the Continuity IRA (CIRA).<sup>ad,ae</sup> The CIRA is comprised of extremely violent but disorganized former members of the PIRA, and does not threaten the existence of the latter. On the other hand, the RIRA has been a significant challenge to the PIRA and—of the three groups—has unleashed the most violence. It is also highly efficient and well organized, having been formed by an experienced core of the PIRA's militant wing.<sup>af</sup> The RIRA quickly proved its propensity for violence in Omagh on 15 August 1998, killing 29 people and injuring 220 in one incident that defied previous terror bombing protocols and evinced an increased level of lethality.<sup>ag</sup> The RIRA has recently absorbed the CIRA into an alliance that will probably be permanent, especially with respect to the increased level of lethality and involvement in international organized crime.<sup>ah</sup>

3. 9/11 Attacks: The PIRA has experienced a significant drop in financial support from Irish-Americans, a critical source of funding.<sup>ai</sup> This loss may be attributed to a combination of factors, including a newfound sympathy for the effects of terrorism. Another factor is very strong British support for the United States in the War on Terror.

The most damaging of the three circumstances mentioned above to the PIRA is its separation from the RIRA/CIRA. The schism has had an enormous impact on the organization's ability to earn money and maintain discipline. The earnings of the PIRA have been cut by almost half according to some estimates,<sup>aj</sup> including subsidies for PIRA volunteers.<sup>ak</sup> This financial fact, combined with the inactivity of PIRA gunmen on home territory, has caused some members of the organization to engage in criminal activity outside of the leadership umbrella.<sup>al</sup> Such unsanctioned activity has taken a political toll on the once disciplined PIRA. The following case exemplifies this point:

July 1999: While the PIRA was issuing rhetorical support for the current cease-fire, PIRA operatives were caught smuggling weapons from the United States. This action may have been unauthorized by the PIRA hierarchy. A combined Irish, British and U.S. intelligence/law enforcement task force seized a PIRA weapons shipment originating in Philadelphia and Ft. Lauderdale, and shipped from New York to Ireland, undermining PIRA political and moral credibility. This ac-

---

tion immediately placed the PIRA commitment to the peace process in question. It also served to alienate pro-republican [i.e. pro-unified Ireland] U.S. politicians who had bargained their political clout in good faith to seek equitable bargaining status and concessions for the PIRA with the British.<sup>am</sup>

Despite this and other embarrassing incidents involving PIRA members in Great Britain and other places, the organization still enjoys international support from various sectors. The RIRA has also inherited this support. The problem, however, is that such a dissolution of discipline among trained killers, sitting idle with no service subsidies coming in, has caused a significant number of PIRA members to either defect to the more active RIRA, or to go after independent opportunities on the international criminal market.<sup>an</sup> The leverage most often used by these operatives is their historical IRA connections. Many of these trained killers have international contacts, expert smuggling capabilities, and a cold capacity for violence. Whether they are operating under the PIRA or RIRA banner, or as independents, their recent reach has been impressive based on what we know. Consider the following examples:

#### **EXAMPLE 1: PIRA CONNECTIONS TO THE FARC**

In August 2001, three PIRA operatives, James Monaghan, Niall Connolly and Martin McCauley, were arrested in Colombia for allegedly assisting the FARC in developing a new mortar

device and training FARC terrorists to increase their level of lethality in urban areas. All three men were relatively high-ranking members of the PIRA organization. Of the three, James Monaghan is the most dangerous: he is the explosives engineer who developed the Mark 1 and the improved Mark 18 Barracks Buster mortar.<sup>ao</sup> In developing the Mark 1, Monaghan received Libyan support, thus tying him to both Middle Eastern terrorist organizations and the state sponsors who have funded these groups in the past. *In developing the Mark 1, Monaghan received Libyan support, thus tying him to both Middle Eastern terrorist organizations and the state sponsors who have funded these groups in the past.*

Monaghan's mortars, in the hands of the FARC, immediately had a deadly impact in Colombia.<sup>ap</sup> Furthermore, it is quite possible that he shared this technology with Palestinian terror groups, as evidenced by the increased lethality of Palestinian attacks on Israeli

troops using a mortar system and tactics linkable to Monaghan and/or the IRA.<sup>aq</sup> Furthermore, Monaghan has an incredible ability to technologically adapt his inventions in order to circumvent counter-terrorism methods.<sup>ar</sup> Such disseminated adaptation techniques have the potential to further intensify the lethal capabilities of his mortars in the hands of terrorist operatives. One of the other two IRA members arrested with Monaghan in 1999, Niall Connolly, had been Sinn Fein's "official" envoy to Cuba since 1996.<sup>as</sup> Gerry Adams, speaking on behalf of PIRA and Sinn Fein, denied any knowledge of these three men's activities. However, it is highly unlikely that Sinn Fein and/or the PIRA were unaware of their involvement in Colombia. Pointing out an operational fact about the PIRA, testimony given by an IRA expert to the U.K. House of Commons noted the following in relation to Adam's denial: "... [the] PIRA is very much akin in organizational terms to a mafia-type structure of organized crime. One sees a great deal of discipline."<sup>at</sup> In fact, the U.S. Congress recognizes that the IRA has been engaged in Colombia for some time: "The available evidence strongly indicates that involvement of the IRA in Colombia extends beyond the three members who were captured and that it has had a presence in that country for at least 3 years."<sup>au</sup> The men were eventually released due to a lack of evidence, although political pressure from pro-republican U.S. politicians may have played a role in their release. The U.S. government contends that the three PIRA operatives received \$2 million for their training of FARC operatives.<sup>av</sup>

#### **EXAMPLE 2: RIRA—ORGANIZED CRIME OR TERROR GROUP?**

The 2000 arrest of three RIRA members securing heavy weapons in Croatia and Slovenia<sup>aw</sup> is consistent with a pattern of activity that indicates the RIRA is becoming more of an organized crime group and using political terrorism to mask its true motive: profit. Consider the following testimony of Jonathan Winner, former U.S. Deputy Assistant Secretary of State, International Law Enforcement:

Many terrorist groups have also been linked to other criminal activities, including smuggling and counterfeiting operations. For instance, the Real IRA is active in smuggling assorted goods into Great Britain. In recent years the Real IRA established close links to British criminal groups to sell converted diesel fuel on the black market. Moreover the Real IRA established tobacco-smuggling operational links to east Euro-

---

pean mafia, and oversees counterfeit operations that produce pirated copies of compact discs and videocassettes. When these illicit profits are coupled with the millions of dollars raised by Irish communities in the United States, the Real IRA can easily afford to recruit new members, construct bomb-making facilities, procure light weaponry, and maintain close contact with other terrorist groups, especially in the Americas.<sup>ax</sup>

A report by the U.S. Government's Federal Research Division makes a similar suggestion: "Tamara Makarenko<sup>ay</sup> points out that, once a group enters category three [fighters-turned-felons], *'instability is sustained for the sole purpose of profit-seeking.'* As an example, Makarenko suggests that the splinter RIRA's ongoing terrorist activities, done in the name of continuing the cause deserted by the parent organization's peace efforts, actually aim to preserve the environment of instability that protects the group's criminal activities."<sup>az</sup> The fact that the RIRA has been relatively quiet in terms of anti-British aggression in the past few years<sup>ba</sup> and that these few attacks have been small in comparison to their 1998 Omagh attack may corroborate this supposition. This hypothesis is further strengthened by the fact that the RIRA has been building an arsenal of considerable firepower<sup>bb</sup> since their inception and yet they seldom use these weapons. If the assumption is correct, and the RIRA is using political terrorism to hide criminal enterprises, it would mean that a terrorist group once governed by political goals—and therefore less likely to engage in activities that would undercut civilian sympathy for the organization—would now be governed by profit. Thus, a very real potential exists for other terror groups to buy access to weapons and smuggling routes currently used by the RIRA.

These two examples chart a slide toward criminal behavior that is undermining political credibility, but not marketability, at least in the eyes of other terrorist organizations. The fact that international terror groups and organized crime syndicates are utilizing the services of IRA operatives, be they PIRA or RIRA, should worry security planners. All it would take to sneak a major weapon of mass destruction (WMD) into the United Kingdom are a few profit-oriented IRA members with in-depth smuggling knowledge and Islamic fundamentalist contacts willing to pay the right price. Ironically, it is this same slide toward criminal behavior that grants security planners the best opportunity

***By marketing this same capacity to smuggle a WMD into the United Kingdom, U.S. and/or British operatives could, for the right price, also gain access to the inner circle of a terror group, without having to take on the cover of “fellow” Islamic extremists.***

for penetrating Islamic terror groups. By marketing this same capacity to smuggle a WMD into the United Kingdom, U.S. and/or British operatives could, for the right price, also gain access to the inner circle of a terror group, without having to take on the cover of “fellow” Islamic extremists. Rather, U.S. and British operatives can act as undercover IRA operatives—a capacity in which they already are experienced. For this reason, the PIRA or RIRA would make an excellent candidate for the trojan horse strategy.

#### **IRA SUSCEPTIBILITY TO PENETRATION: *THE McKEVITT TAKEDOWN***

Despite a tradition of caution and discipline on the part of Irish paramilitaries, the British intelligence services have successfully penetrated all three branches of the IRA, mainly because the British Force Research Unit has honed its infiltration skills over the past few decades. Also, the recent disintegration of IRA internal discipline post-ceasefire may make the IRA groups more porous. Although such a statement cannot be quantified, the recent takedown of RIRA chief, Michael McKevitt, underscores a definite weakness on the part of current IRA operations.

The August 2003 conviction of Real IRA chief, Michael McKevitt, was facilitated by the cooperation of the U.S. FBI, Britain’s MI5 and Irish Special Police. It exploited the RIRA’s susceptibility to infiltration by U.S. operatives in large part due to the RIRA’s reliance on Irish-American sympathizers and financial necessity. This susceptibility was especially true in the early years of the RIRA’s formation, when the organization was competing with the PIRA over funds from sympathetic U.S. donors. The problem for the RIRA, and especially McKevitt, was that “his real expertise lay in handling and hiding weapons,” not fundraising.<sup>bc</sup> As a result, McKevitt was willing to engage in talks with people with whom the PIRA would previously never have made contact due to a perfected vetting process. This early weakness led to McKevitt connecting with David Rupert, an American businessman from Pennsylvania, and a FBI informer.

---

The Rupert penetration of the RIRA is a great example of U.S.–U.K. cooperation.<sup>bd</sup> Coached by MI5, and funded by the FBI, Rupert opened a bar in Dundalk, County Louth, Ireland, near the border with Northern Ireland. The location of the bar was guided by MI5. Between October 1998 and August 2000, Rupert gained the trust of the RIRA,<sup>be</sup> and eventually McKevitt himself. Such cooperation in infiltration played to U.S. strengths, while simultaneously allowing the United States to learn from the British, who have become adept at penetrating the IRA over the past thirty-some years fighting their own war on terror.

The lessons that the United States should take away from the McKevitt takedown, which was a law enforcement structured penetration<sup>bf</sup> as opposed to a military type of intelligence-gathering mission,<sup>bg</sup> are the following:

(1) HUMINT does not have to go deep into an organization to gain quality information. By standing on the periphery, the intelligence community can gather greater amounts of data with less time to prepare. Rupert was never an RIRA member; he was an outsider who gave the RIRA a good reason to trust him—money.

(2) The United States *does* have human assets it can use; it is not helpless in penetrating foreign terror organizations, but it must be creative with its covers. Rupert is neither Irish-born *nor* an Irish-American. The key to Rupert's penetration relied solely on a credible cover story, not a fake accent or even a top-notch Gaelic language school.

***There is an increased potential for the proliferation of terrorism when one organization engages in criminal activity.***

(3) The RIRA is cash dependent, and this was the weakness exploited by U.S. and British intelligence agencies. This weakness can exist even for al Qaeda. Periphery covers should be considered in ways that exploit such weaknesses.

## **HOW THE IRA CAN HELP PENETRATE ISLAMIC TERROR GROUPS**

As previously quoted in this paper, there is an increased potential for the proliferation of terrorism when one organization engages in criminal activity:

Many terrorist groups have also been linked to other criminal activities, including smuggling and counterfeiting operations... When these illicit profits are coupled with the millions of dollars raised by Irish communities in the United States, the Real IRA can easily afford to recruit new members, construct bomb-making facilities, procure light weaponry, and maintain close contact with other terrorist groups...<sup>bh</sup>

The U.S. intelligence community should be seeking to exploit these contacts “with other terrorist groups.” Although at the present there is no concrete evidence that any form of the IRA has connected directly with al Qaeda, the *ability* to connect to al Qaeda, or some other similarly motivated group, is established. Like Rupert’s McKeivitt, al Qaeda needs something badly: to strike a major Western state in an enormous way. Any faction of the IRA can facilitate this through established smuggling networks. The IRA’s ability to offer up Great Britain would undoubtedly perk a few ears. Furthermore, the IRA, especially the two factions not involved in the peace process, the RIRA or the CIRA, would come with credibility on multiple levels that al Qaeda leaders can appreciate. First, a desire to hurt the British people has been established by the IRA, and especially by the RIRA after Omagh. Although the leadership of the IRA (specifically the PIRA) would preach constraint to avoid constituent backlash, it could be sold to a fundamentalist that a rank-and-file member of any of these Irish paramilitary organizations may not appreciate the politics of such a decision and perceive the IRA leadership as becoming “soft.” Secondly, criminal activities have supplanted ideological constraints with profit motives, and lastly, the leadership has lost its credibility through either imprisonment (RIRA) or appeasement (PIRA). Feeding on these motivations, the following scenario could be envisioned: *Rogue IRA operatives wish to seek a deal with al Qaeda. For €5 million, relocation, and protection, these operatives will get a large WMD device into Great Britain and deliver it to Islamic terrorists. The conditions can be small and reasonable: money upfront, fellow IRA members cannot be made aware of the deal, and fair warning before the attack in order to have time to leave the city and enjoy the money.* Such a scenario is not that far-fetched. In fact, this may be what took place between ETA members and al Qaeda in order to facilitate the 11 March 2004 Madrid attacks. In this case, the rogue IRA operatives would be members of a joint U.S.-British intelligence team. Furthermore, this scenario could even be implemented *with only one such undercover operative.*

---

The merits and problems of such idea scenario will be scrutinized in the final section of this paper.

## **PROPOSED TROJAN HORSE #2: RUSSIAN ORGANIZED CRIME**

### **THE OPPORTUNISTIC FORMER COMMUNISTS**

The term “Russian” organized crime is a misnomer. The first problem with the term is that there is very little “Russian” involved in this criminal phenomenon. Speaking at a 1998 Congressional hearing on the subject of international crime, then-FBI Director Louis Freeh gave the following description of what is sometimes known as the “Russian *mafija*”:

Russian Federation Ministry of Interior (MVD), Organized Crime Control Department officials report the existence of over 8,000 Russian/Eastern European/Eurasian criminal groups. There are allegedly over 150 ethnic-oriented criminal groups, including the Chechens, Georgians, Armenians and Russian-ethnic Koreans, of which 25 are active in the United States. Russian authorities also report the existence of some 750-800 so-called “Thieves-in-law,” the Godfathers of the “Russian Mafia.”<sup>bi</sup>

The second problem with the term Russian organized crime is that it is hardly “organized” in the traditional sense of the term. The U.S. Department of Justice’s National Institute for Justice International provides the following operational definition and description of Russian organized crime:

[The] structure does not look like either what is commonly understood to be the structure of organized crime or a mafia in the conventional sense of those terms. The networks are neither highly centralized nor dominated by a small number of individuals. Those individuals who do have particular influence seem to occupy their positions on the basis of their personal characteristics...This means that the networks lack...continuing structures...

On the other hand, it is clear that these structures are not simply small groups of criminals essentially acting independently of one another... Instead, there is broad connectivity among most of the actors. They may not be directly connected to a large number of others, but they are indirectly connected to many. This allows the networks a great

deal of flexibility in the organization of their offenses, which means they can be responsive to the opportunities for illegal undertakings that develop. Given such an opportunity, a member of these large networks can access partners who are either generalists or specialists, can raise capital, and can access other needed resources. In this sense, the structure is very functional. The fluid nature of the structure may also explain the high level of internal violence that the network seems to experience. The lack of a more hierarchical structure means that no one can effectively control the use of violence or mediate disputes. In addition, the lack of more formal subgroupings weakens loyalty to past partners: many of the murders, for example, seem to involve disputes between individuals who once worked together.<sup>bj</sup>

***Italian Mafiosi would not be likely to engage in activity with al Qaeda, regardless of how much money was offered, because it would solicit the full weight of U.S. law enforcement agencies and spell the end of their associated enterprises.***

Russian organized crime (hereafter referred to as ROC) is therefore neither ethnically Russian nor a unified body. The only apparent unifier is that it is heavily composed of former Soviet intelligence officers (KGB) and Special Forces (*Spetsnaz*), making the operational capacity of these groups highly efficient and lethal.<sup>bk</sup> Consequently, the potential problems that ROC poses are numerous for those engaged in the War on Terror for the following set of reasons:

#### **UNENCUMBERED**

A lack of accountability to any centralized figure makes any member of any one of the ROC groups free to pursue profitable endeavors without reprisals from a more strategically focused “boss.” What this means is that a maverick ROC associate does not have to consider the consequences of an action on the overall organization, such an Italian Mafia member would. There is no moderator for the behavior of a single actor or small set of actors. Italian Mafiosi would not be likely to engage in activity with al Qaeda, regardless of how much money was offered, because it would solicit the full weight of U.S. law enforcement agencies and spell the end of their associated enterprises. This same type of consideration would not exist for an ROC affiliate.

---

## GLOBAL

The transnational character of such organizations, both operationally and structurally, makes it more likely to engage in profitable alliances with groups operating within environments from which ROC members originate. This may be why al Qaeda has had almost free reign throughout the Caucasus: it is both lawless and easy to secure materials from ready providers, namely, ROC affiliates. Rohan Gunaratna describes this in his book *Inside Al Qaeda: Global Network of Terror*. “According to a European intelligence agency, al Qaeda assisted Al Ansar Mujahidin<sup>bl</sup> in weapons trafficking via Russian, Ukrainian and Chechen criminals. During the first Chechen war, Ukraine, notably Odessa, was a prime transit point for Mujahidin fighters and weapons smuggling.”<sup>bm</sup> The ability to operate with impunity across a broad geographic range, including expatriate communities like those found in the United States, makes ROC groups especially dangerous and far reaching. The broad cultural and geographic spectrum which affiliates enjoy enables bases from which to launch more ambitious endeavors in places such as Latin America, and even East Asia.<sup>bn</sup> This ability to traverse the globe while maintaining strong presences in lawless regions should be attractive to Islamic terror groups seeking ways to smuggle operatives, weapons, or cash from one continent to the next.

*The broad cultural and geographic spectrum which affiliates enjoy enables bases from which to launch more ambitious endeavors in places such as Latin America, and even East Asia.*

## INTELLIGENT

Many ROC affiliates are highly educated and savvy individuals. Although street-thugs exist within the ranks, the types of crimes in which ROC affiliates normally engage are more often sophisticated white-collar crimes than the lowbrow jobs indicative of other criminal enterprises. A May 2000 FBI *Law Enforcement Bulletin* describes the types of typical ROC crimes: “Some experts predict that white-collar crime will serve as the benchmark for ROC in the United States... The more sophisticated ROC fraud schemes include fuel scams, healthcare fraud, bank fraud, and stock market manipulation. In these and other schemes, ROC members have demonstrated an aptitude for circumventing or exploit-

ing the bureaucracy, rules, and procedures of government agencies, financial institutions, insurance companies, and other businesses.”<sup>bo</sup>

## **WELL CONNECTED**

ROC members, because of their composition and former Soviet credentials, enjoy unrivalled government contacts. In his 1998 Congressional testimony, Colonel Stanislav Lunev (former Glavnoye Razvedovatel’noye Upravlenie – GRU)<sup>bp</sup> was asked why he decided to defect to the United States in 1992, *after* the Cold War. He gave the following reason which provides insight into ROC access to high-level government officials: “And actually, I couldn’t provide anymore—to continue to provide anymore my very special services for government, which existence, legal existence is under really great suspension, and government which was penetrated by Russian organized crime groups, by Russian Mafia so deeply that it was possible a few years ago to say officially that Russian Federation just now is a criminal state.”<sup>bq</sup> Not only have these connections been verified through a number of other sources, but they have also created direct security problems. The weapons caches that have been pilfered by connected former military ROC have made their way into a variety of transnational terrorist and organized crime groups.<sup>br</sup>

An unencumbered, global, intelligent and well-connected group of criminals can be an asset for any organization seeking to commit illegal acts—especially mass murder. However, it is precisely because of the “potential problems” cited above that ROC is a potential asset to the U.S. intelligence community. Its disorganized structure, ruthlessness and Soviet composition all play into U.S. intelligence strengths.

## **ROC SUSCEPTIBILITY TO PENETRATION**

U.S. law enforcement has had some success penetrating ROC groups; the problem has mainly been jurisdictional disputes between numerous agencies operating in the ROC-saturated New York area. The New York Police Department (NYPD), New York State Organized Crime Task Force (NYOC-TF), and the New York District Attorney’s Office (NYDA) have cooperated with each other with some success. Unfortunately, coordination at the federal level has not been as fluid. The New York field office of the FBI has reportedly worked separately from the New York offices of the DEA, BCIS (formerly INS) and the IRS.<sup>bs</sup> As late as 1999

---

there was no cooperation between the local New York law enforcement agencies and the FBI in dealing with Russian organized crime.

The problem for all of these law enforcement agencies is the disjointed nature of ROC. Within ROC, stereotypical “Godfathers” are rare in the Italian-Mafia sense of the word. This makes it difficult to climb a ladder of convictions up through a hierarchy like they have done with the Italian Mafia. With each low-level mobster arrested, the potential to turn that Italian organized crime figure on his immediate boss is available. If this occurs, which it often does, the next in command will be apprehended, turned and so on. This enables a climb-the-ladder approach toward taking down the entire organization. This approach cannot be applied to ROC, because there is no boss in the true sense of the word. Still, monitoring ROC activity is facilitated by a combination of penetration and utilization of an occasional informant. The key to penetration is offering a profitable *skill* through a liaison, such as the ability to crack computer bank codes. If the undercover agent can establish trust by offering the ROC a profitable opportunity then penetration can be achieved. Once accomplished, the doors are open as wide as that particular group can open them.

### **HOW RUSSIAN ORGANIZED CRIME CAN HELP PENETRATE ISLAMIC TERROR GROUPS**

Despite the risks on the domestic side of penetrating ROC, the international counterterrorism benefits that such a penetration may yield are worthwhile. The benefit lies in its non-existent structure. Disorganization reduces the ability of other groups to challenge the legitimacy of an actor claiming to have criminal connections. Although such connections would have to be established, the skill-set that U.S. intelligence brings to the table will greatly determine the speed by which operatives are accepted by other ROC members. The Soviet composition of ROC allows U.S. intelligence agencies to tap an enormous pool of HUMINT strength:

*Disorganization reduces the ability of other groups to challenge the legitimacy of an actor claiming to have criminal connections.*

former Cold War-era Soviet experts, spies, and linguists. As for the ruthlessness of ROC, this figures into the critical credibility game that will need to be played in order to win the confidence of Islamic extremists. ROC members are notoriously opportunistic, even profiting in Chech-

nya at the expense of their own country. An investigator at the New York District Attorney's Office described Russian mobsters in the following way: "These guys love money. They'll do anything for it. You name it, if it makes them money, they're gonna' do it."<sup>bt</sup> Establishing trust will be a matter of cash. It is not difficult to envision an ROC affiliate selling unfettered access to a U.S. port for the right price. Furthermore, ROC members are already serving the needs of al Qaeda in other ways. The scenario envisioned would be as follows: *U.S. intelligence operatives pose as members of an ROC group based out of the New York area, offering a combination of services for a steep price. These services can include a host of logistical services including terrorist smuggling, weapons smuggling, or cash transfers to sleepers. For al Qaeda, this would be a constant flow of supplies and personnel into the United States. For the Russian organized crime members, this would be just another (perhaps bigger) business deal.* Clearly, both the merits and problems of such an idea require scrutiny, but the potential opportunity is far too great to overlook.

## CONCEPT ANALYSIS AND CONCLUSION

### EMPLOYING THE CONCEPT

Consider the following FBI press release from August 2003:

F.B.I.: 13 August 2003: NEWARK, N.J. - A British arms dealer appeared in U.S. District Court today, on charges that he tried to complete the sale of a shoulder-fired missile, with the understanding that it was going to be used to shoot down an American commercial airliner, the U.S. Attorney's Office and Justice Department announced today.

Two other defendants were arrested. Both of them helped in a planned money transfer that was part of the transaction. One of those two individuals arrived in the U.S. to allegedly arrange for a \$500,000 down payment [sic] from a government cooperating witness for 50 more shoulder-fired missiles.<sup>bu</sup>

The "British arms dealer" mentioned above could easily have been a U.S. intelligence operative working in the other direction. The problem is not coming up with a credible service to initiate contact with terrorist operatives, rather designing a credible cover so that they will

---

trust you. In other words, a number of services would likely spark Islamic terror groups' interest, such as smuggling a WMD into a U.S. port, but the same terrorists would likely ask, "Why is he offering us this great deal?" Trust will have to be secured. There are two ways to achieve this trust: it can be built or it can come ready-made. Building the trust will undoubtedly take time. As previously stated, the problems inherent in deploying operatives capable of directly infiltrating Islamic terror groups are numerous: dialects, cultural mannerisms, introductions, etc. The issue of proof of commitment will also come up. In its best form, proof of commitment may be some form of criminal act, such as a robbery for the purpose of funding. In its worst form, proof of commitment may include a suicide operation. Based on what we know about previous Islamic terror operations and the guarded nature of their planning process, the U.S. intelligence operative may not know he is involved in a suicide operation until it is too late. In all, the flaws inherent in terror group infiltration are numerous, dangerous, and may yield little or no benefits. Islamic terror group infiltration should seek to circumvent these inherent problems. Finding ready-made trust may be the solution.

Finding ready-made trust, as this paper advocates, is using organizations that are easier to penetrate, that fit well with U.S. HUMINT strengths, and have established (or very likely can establish) connections to Islamic terror groups. This paper suggests the IRA and Russian organized crime for the reasons explained above. It should be noted that, although the cases presented for the purpose of this paper have involved law enforcement penetration of the two groups suggested, infiltration can also take a more military approach toward gathering intelligence for the War on Terror. In other words, collection should be viewed as long-term monitoring focusing on disrupting terror operations, not as a short- or medium-term gathering of evidence for building a criminal case. Trojan horses should provide insight into planning, weapons procurement, location and identification of Islamic terrorists.

***A number of services would likely spark Islamic terror groups' interest, such as smuggling a WMD into a U.S. port, but the same terrorists would likely ask, "Why is he offering us this great deal?"***

Once identified, the nature of the threat should determine the level of force and speed of deployment.

Despite the potential benefits, there are some significant questions regarding utilizing trojan horses that should be addressed. The most important question is: *Can it work?*

### **CAN IT WORK?**

The answer is maybe. Although penetrating the IRA or ROC can be achieved, making the next step, i.e. connecting to Islamic terror groups, may prove difficult. The first problem is contacting Islamic extremists.

*Collection should be viewed as long-term monitoring focusing on disrupting terror operations, not as a short- or medium-term gathering of evidence for building a criminal case.*

How does a new member of the IRA or ROC become the first to make such a bold suggestion? Such a recommendation by a newly affiliated member may make the intelligence operative seem too risky, if not outright crazy. The suggestion could label the operative as a liability. Among such groups, liabilities are dealt with in several ways: at best they are ostracized; at worst, they are assassinated. Thus, making the initial suggestion to sell an Islamic terror group a commodity would have to be done in a way that does not endanger the operative's life or relationship with the group. However, assuming that the operative is able to get members on board for such a scheme, the next step, contacting the terror groups to make such an offer may prove more difficult.

The task of contacting Islamic extremist groups presents a multidimensional problem. First, trust will have to be secured. Islamic extremists are highly suspect of Western motives. Rhetoric from the Middle East sees the hand of the CIA in almost everything, and this distrust will have to be overcome. The next problem will be dealing with the low-level Islamic operatives who are likely to serve as the first point of contact. These low-level terror operatives may not appreciate the deal being offered. An easy Western target may seem more immediately satisfying to one of these low-level terrorists than some long-term plan that may never take off. The third problem is that there is no guarantee that the terror group's leadership will ever become immediately involved in the negotiations. Proxies or representatives will undoubtedly be used at the outset, but getting higher-ranking members to become involved

---

will be tricky. At any time, a suggestion of direct leadership involvement may immediately raise suspicion, destroying both the initial trust of the operative as well as any future use of the trojan horse as a cover.

Assuming that such contacts are made, and leadership involvement is secured, the next set of issues involves cost-benefit analysis, timing, and consequences. How far does one go before pulling the plug on the program? If the operative is offering U.S. port access for a nuclear device, do we let the device arrive? Do we stop it in mid-shipment? At what point does the success of the intelligence gathering operation endanger the United States or Great Britain? Finally, how do governments explain to their citizens if something goes wrong to the benefit of a terror group? Example: If smuggling terrorist operatives is the request, and the operative complies, what happens if the terrorist evades those agents sent to monitor him? In such a situation, the United States or the United Kingdom would then be faced with the problem of having a dangerous terrorist within its borders, compliments of its own security apparatus.

*At any time, a suggestion of direct leadership involvement may immediately raise suspicion, destroying both the initial trust of the operative as well as any future use of the trojan horse as a cover.*

#### **WHAT FUNCTIONAL ISSUES MIGHT ARISE?**

All of these issues would have to be carefully considered and weighed before employing such a program. In some cases, the issues may be planned for and the problems avoided; but there are no guarantees, and the consequences of a mistake can cost lives. Furthermore, outside of the inherent operational questions that such a program is likely to raise, there are political, legal, jurisdictional and logistical concerns that will also arise. Which agencies should take the lead in such a program if penetration is facilitated from the domestic side, but operations are conducted overseas? Which methods of operation will have to be coordinated between British and U.S. intelligence agencies to facilitate functional cooperation? What latitude will be granted to a U.S. intelligence operative that is forced to prove his commitment with a criminal act? All of these functional issues would have to be addressed by policy experts before initiating such a program.

### **IS THERE A GENUINE TIME BENEFIT?**

The other issue is time benefit. It will first take time to infiltrate a trojan horse, before an infiltration of the Islamic terror group is initiated. (It took David Rupert three years to successfully penetrate the RIRA.) The transition time from infiltration to terror group contact will certainly take longer. The next step, facilitating the terror group's request will take longer still. The years that such a program may require, from start to finish, could exceed the benefits other programs may yield within the same possible timeframe. However, the time to penetrate a terror group is not the only issue that must be considered from the standpoint of timing, the other issue is effective communication.

What capacity will a U.S. intelligence operative have at his or her disposal to communicate any information gained? Timing is a critical issue for an effective response to a terror attack. The problem with deep cover, such as the type proposed, is keeping an open line of communication. This is a luxury not always enjoyed. The speed at which a terror attack can materialize may diminish the returns of this type of infiltration.

### **CONCLUSION**

There are many potential problems with the concept proposed, the majority of which are operational. The concept is unproven. The benefits are questionable. There are significant risks for an operative. Because the gains are impossible to verify, a cost-benefit analysis to weigh the risks-to-gains is equally impossible to determine. As a whole, the idea of utilizing trojan horses to infiltrate the Islamic terror groups' backdoor of criminal dependence is extremely risky. There simply is no way to quantifiably justify its utilization.

The problem, however, for U.S. intelligence is that *infiltration is necessary*. How else can this be achieved? The U.S. intelligence community is ill-equipped to directly infiltrate Islamic terror groups. They are fluid, often decentralized networks, comprised of family and friends, who are tested in ways that would likely shock outsiders. But direct penetration of terror groups by U.S. operatives will have to be secured in order to achieve the goal of credible intelligence collection. Changes are being made, but today this is still not possible.

---

This brings back the two initial questions: *What can U.S. intelligence do to gain access to the hierarchy?* and *What can we employ from our current arsenal that can help achieve our intelligence objectives rapidly?* The answer proposed was the manipulation of Islamic extremists' dependence on illegal activities to fund or supply their operations. This backdoor will not be easy to exploit, but it may be possible. There is no proof that the trojan horse method will work. It may seem an imperfect strategy, but there are few alternatives that are not equally flawed. Either way, infiltration will have to be achieved—quickly. The attacks of 9/11 proved the terrorists' resolve, and unfortunately there is a historic pattern that says future terrorist attacks become more dramatic and more lethal with each subsequent assault.<sup>bv</sup> Today's Islamic terror groups are exhibiting a need to exceed. If al Qaeda is trying as hard as possible to out-do the 9/11 attacks, any strategy that can potentially remedy the HUMINT deficiency should be considered. 

---

## NOTES

<sup>a</sup> Testimony of Bruce Hoffman, Vice President of External Affairs, Washington Director of the RAND Institute, U.S. House of Representatives, House Permanent Select Committee on Intelligence, Subcommittee on Terrorism and Homeland Security, 26 September 2001.

<http://intelligence.house.gov/Casestudies.aspx?Section=81>

<sup>b</sup> Amos Jordan, William Taylor and Michael Mazarr, *American National Security, 5<sup>th</sup> Edition* (Baltimore: Johns Hopkins University Press, 1999), 143–170.

<sup>c</sup> *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2004), 108–277.

<sup>d</sup> *Ibid.*, 362.

<sup>e</sup> Richard Betts, *Fixing Intelligence*, 461. Reprinted in Russell Howard and Reid Sawyer, *Terrorism and Counterterrorism: Understanding the New Security Environment* (Guilford, Connecticut: McGraw-Hill Company, 2002).

<sup>f</sup> Jeffrey Richelson, *The U.S. Intelligence Community, 4<sup>th</sup> Edition* (Boulder, Colorado: Westview Press, 1999) 262–266.

<sup>g</sup> House Resolution 5223, *National Intelligence Reform Act of 2004*, Title V, Section 504, “The United States-Saudi Arabia Relationship,” 5 October 2004, <http://thomas.loc.gov/cgi-bin/query/D?c108:1:./temp/~c108q5Yw50::>

<sup>h</sup> Richard Best, “Intelligence to Counter Terrorism: Issues for Congress,” 21 February 2002 (Washington, DC: Congressional Research Service). <http://fpc.state.gov/documents/organization/31482.pdf>

<sup>i</sup> *The 9/11 Commission Report*, 362.

<sup>j</sup> U.S. Navy, *General Military Training Manual*, Unit 1, Topic 3: Terrorism, Section 22 (1-3-22) Three Categories of Motivation, [https://www.cnet.navy.mil/cnet/gmt/gmt03/1\\_3.pdf](https://www.cnet.navy.mil/cnet/gmt/gmt03/1_3.pdf)

<sup>k</sup> Betts, 461.

<sup>l</sup> John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime and Militancy* (Santa Monica: RAND Corporation, 2001) 86-108.

<sup>m</sup> Hoffman, Footnote 1.

<sup>n</sup> Elizabeth Joyce, *Transnational Criminal Enterprise: The European Perspective*, 102, printed in Farer, Tom (editor), *Transnational Crime in the Americas* (New York: Routledge Press, 1999); Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror*, Chapter 3 (New York: Berkley Books, 2003).

<sup>o</sup> “Backdoor,” <http://www.webopedia.com/TERM/b/backdoor.html>

<sup>p</sup> “Trojan Horse,” [http://www.webopedia.com/TERM/T/Trojan\\_horse.html](http://www.webopedia.com/TERM/T/Trojan_horse.html)

<sup>q</sup> Hereafter, all manifestations of the Irish Republican Army—PIRA, RIRA, CIRA and OIRA—will be denoted collectively as “IRA” unless otherwise noted for specificity.

<sup>r</sup> Basque Fatherland and Liberty.

<sup>s</sup> The Revolutionary Armed Forces of Colombia.

<sup>t</sup> Honorable William S. Broomfield (R-MI), Extension of remarks, U.S. House of Representatives, 101<sup>st</sup> Congress, *Attacks on Israel Reveals Libya’s Continuing Role in Terrorism*, 20 June 1990 <http://thomas.loc.gov/cgi-bin/query/D?r101:1:./temp/~r101ckW117::>

<sup>u</sup> U.S. House of Representatives, “International Global Terrorism: Its Links With Illicit Drugs As Illustrated by the IRA and Other Groups In Colombia,” Hearing Before The Committee On International Relations, 107<sup>th</sup> Congress, 2<sup>nd</sup> Session, 24 April 2002.

[http://commdocs.house.gov/committees/intlrel/hfa78947.000/hfa78947\\_0.HTM](http://commdocs.house.gov/committees/intlrel/hfa78947.000/hfa78947_0.HTM)

<sup>v</sup> U.S. State Department, “Patterns of Global Terrorism 2001”, 66.

<sup>w</sup> Council on Foreign Relations, “Terrorism: Questions and Answers” <http://www.terrorismanswers.com/groups/ira2.html#Q11>

<sup>x</sup> Two reports: the first originated from a United States Congressional House of Representatives Hearing and subsequent report, 24 April 2002, *International Global Terrorism: Its Links with Illicit Drugs as Illustrated by the IRA and Other Groups in Colombia*; the second corroborated the first, summarizing the findings of a United Kingdom Parliamentary inquiry from the House of Commons, 2 July 2002, *Northern Ireland Affairs Fourth Report*.

<sup>y</sup> Jill Lawless, IRA suspect nabbed on West Bank, *News Interactive*, 3 November 2004. [http://www.news.com.au/common/story\\_page/0,4057,6748942%255E1702,00.html](http://www.news.com.au/common/story_page/0,4057,6748942%255E1702,00.html). Also see State of Alaska Homeland Security and Emergency Services, *Situation Report 03-195*, <http://fc.ak-prepared.com/dailysitrep/0000D6AC-80000005/007046D4-000F6917>

<sup>z</sup> Mark Burgess, Center for Defense Information, *Globalizing Terrorism: The FARC-IRA Connection*, <http://www.cdi.org/terrorism/farc-ira-pr.cfm>

<sup>aa</sup> Council on Foreign Relations, “Terrorism: Questions and Answers”

<sup>ab</sup> The Provisional IRA was an offshoot of the Northern Irish wing of the Original IRA (OIRA). The OIRA chose to accept, and adhere to a ceasefire in 1972. This ceasefire inspired many OIRA operatives to breakaway and form the PIRA. This paper suggests 1969 instead of 1972 because the majority of PIRA operatives came from these initial years of violence. See J. Bowyer Bell, *IRA: Tactics and Targets* (Dublin: Poolbeg Press, Ltd., 1993).

<sup>ac</sup> [politics.ie.com](http://politics.ie.com), “Gerry Adams admission on IRA members involved in criminal activity - SDLP,” 18 May 2004, <http://www.politics.ie/modules.php?name=News&file=article&sid=5092>

<sup>ad</sup> This group was actually formed in 1994, but it did not gain momentum until after the *Good Friday Peace Accords*. See Glenn E. Curtis and Tara Karacan, Federal Research Division, “The Nexus Among Terrorists, Narcotics, Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe,” Library of Congress, December 2002, 4, [http://www.loc.gov/rr/frd/pdf-files/WestEurope\\_NEXUS.pdf](http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf)

<sup>ae</sup> A fourth IRA group, the Official Irish Republican Army (OIRA, a.k.a. Original IRA), was more prevalent in the early years of “The Troubles.” It split into two groups, the OIRA and the PIRA in 1970 and agreed to a ceasefire in 1972. Many former members still operate in the Republic of Ireland and they emerge on occasion. The “Originals” claim a direct lineage from the IRA that engaged the British during the fight for Irish independence at the turn of the 20<sup>th</sup> century. Although it has supported anti-British activities in the past, the few remaining OIRA have become more of an organized crime syndicate than a terrorist organization.

<sup>af</sup> Sean Boyne, "The Real IRA: After Omagh, what now?," *Jane's Defense*, 24 August 1998, [http://80-www.janes.com.ezproxy.library.tufts.edu/security/international\\_security/news/jir/jir980824\\_1\\_n.shtml](http://80-www.janes.com.ezproxy.library.tufts.edu/security/international_security/news/jir/jir980824_1_n.shtml)

<sup>ag</sup> U.S. State Department, *Patterns of Global Terrorism 2001*, 106.

<sup>ah</sup> U.S. State Department, Federal Register, "Foreign Terrorist Organization; Designation: Continuity Irish Republican Army," Public Notice 4758, 13 July 2004, Vol. 69, No. 133, <http://a257.g.akamaitech.net/7/257/2422/06jun20041800/edocket.access.gpo.gov/2004/pdf/04-15827.pdf>

<sup>ai</sup> United Kingdom Parliament, House of Commons, 2 July 2002, *Northern Ireland Affairs Fourth Report*, "The Financing of Terrorism in Northern Ireland," Question 44, <http://www.parliament.the-stationery-office.co.uk/pa/cm200102/cmselect/cmniaf/978/97802.htm>

<sup>aj</sup> *Ibid.*, Statement 33, Table 1.

<sup>ak</sup> *Ibid.*, Questions 3 & 4.

<sup>al</sup> Mark Gribben, "Peace In Ulster Breeds Organized Crime, Former Guerillas Become Wiseguys," 17 June 2003 – <http://organizedcrime.about.com/cs/irish-gangs/a/aa061803a.htm>

<sup>am</sup> United Kingdom Parliament, House of Commons, 2 July 2002, Statements 66-81.

<sup>an</sup> Glenn E. Curtis and Tara Karacan, "The Nexus Among Terrorists, Narcotics, Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe" (Washington, DC: Library of Congress, 2002) [http://www.loc.gov/rr/frd/pdf-files/WestEurope\\_NEXUS.pdf](http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf)

<sup>ao</sup> Mark Burgess, "Globalizing Terrorism: The FARC-IRA Connection," *Center for Defense Information*, 5 June 2002.

<sup>ap</sup> Global News Wire, The Financial Times, *Provo device found as FARC blast kills 20*, 9 February 2003, [http://80-web.lexis-lexis.com.ezproxy.library.tufts.edu/universe/document?\\_m=c894148ac95a635fd5616eea3d18cbfe&\\_docnum=5&wchp=dGLbVzb-zSkVA&\\_md5=7e84ad765f778e414078f9fa2c1b8ac6](http://80-web.lexis-lexis.com.ezproxy.library.tufts.edu/universe/document?_m=c894148ac95a635fd5616eea3d18cbfe&_docnum=5&wchp=dGLbVzb-zSkVA&_md5=7e84ad765f778e414078f9fa2c1b8ac6)

<sup>aq</sup> Rachel Ehrenfeld, National Review Online, *IRA+PLO=Terror*, 21 August 2002 – <http://www.nationalreview.com/comment/comment-ehrenfeld082102.asp>

<sup>ar</sup> Mark Burgess, Center for Defense Information, *Globalizing Terrorism: The FARC-IRA Connection*, 5 June 2002.

<sup>as</sup> Niall Stanage, "Victims of the Irish blame game: The 'Colombia Three' case shows that sinister forces are still at work," *The Guardian*, 8 August 2003, [http://80-web.lexis-nexis.com.ezproxy.library.tufts.edu/universe/document?\\_m=40b087c6df6f361a0ec24eecb204d1c8&\\_docnum=4&wchp=dGLbVzb-zSkVA&\\_md5=c1304c76932d78b34a4ae85ca1368806](http://80-web.lexis-nexis.com.ezproxy.library.tufts.edu/universe/document?_m=40b087c6df6f361a0ec24eecb204d1c8&_docnum=4&wchp=dGLbVzb-zSkVA&_md5=c1304c76932d78b34a4ae85ca1368806)

<sup>at</sup> United Kingdom Parliament, House of Commons, 2 July 2002, Question 130, "Mr. Veness."

<sup>au</sup> U.S. House of Representatives Hearing and subsequent report, "International Global Terrorism: Its Links with Illicit Drugs as Illustrated by the IRA and Other Groups in Colombia," 24 April 2002, Statement of Rep. Peter King (R-NY), <http://www.911investigations.net/IMG/pdf/doc-1027.pdf> or [http://commdocs.house.gov/committees/intlrel/hfa78947.000/hfa78947\\_0.HTM](http://commdocs.house.gov/committees/intlrel/hfa78947.000/hfa78947_0.HTM)

<sup>av</sup> *Ibid.*

<sup>aw</sup> U.S. State Department of State, *Patterns of Global Terrorism 2001*, 106.

---

<sup>ax</sup> Jonathan M. Winner, Former US Deputy Assistant Secretary of State, “Congressional Testimony of US Senate Committee on Governmental Affairs,” *Terrorism Financing*, 31 July 2003, [http://80-web.lexis-nexis.com.ezproxy.library.tufts.edu/congcomp/document?\\_m=79d8326d99a1f69087234d30eec3bbba&\\_docnum=8&wchp=dGLbVtz-zSkSA&\\_md5=70cdb70820d3b858bb6d047f4b3d2b0d](http://80-web.lexis-nexis.com.ezproxy.library.tufts.edu/congcomp/document?_m=79d8326d99a1f69087234d30eec3bbba&_docnum=8&wchp=dGLbVtz-zSkSA&_md5=70cdb70820d3b858bb6d047f4b3d2b0d)

<sup>ay</sup> University of St. Andrews Professor, major contributor to Systematic Transnational Crime Theory. See Monica Den Boer, Groupement D’Etudes et de Recherches, *9/11 and the Europeanization of Anti-Terrorism Policy: A Critical Assessment*, Policy Paper No. 6, September 2003, <http://www.notre-europe.asso.fr/IMG/pdf/Polycypaper6.pdf> (Paper is in English)

<sup>az</sup> Curtis and Karacan, 24. [http://www.loc.gov/rr/frd/pdf-files/WestEurope\\_NEXUS.pdf](http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf)

<sup>ba</sup> The last attack by the RIRA was on a police station in County Tyrone, 21 October 2002.

<sup>bb</sup> U.S. State Department, *Patterns of Global Terrorism 2003*, 133.

<sup>bc</sup> BBC News, *Body Blow to the Real IRA*, 6 August 2003, [http://news.bbc.co.uk/1/hi/northern\\_ireland/3127355.stm](http://news.bbc.co.uk/1/hi/northern_ireland/3127355.stm)

<sup>bd</sup> CNN.com/World, *How US Trucker Spied on Real IRA*, 7 August 2003. <http://edition.cnn.com/2003/WORLD/europe/08/07/ireland.mckevitt.informer/index.html>

<sup>be</sup> Rupert was initially instructed to gain the confidence of the CIRA, but when that organization proved to be insignificant due to disorganization, the FBI and MI5 redirected Rupert toward the RIRA.

<sup>bf</sup> Penetration for the purpose of building a criminal case that will stand up in a court of law.

<sup>bg</sup> Information collection for the purpose of identifying targets, obtaining mission information, weapons locations, etc.

<sup>bh</sup> Congressional Testimony of Jonathan M. Winner, Former US Deputy Assistant Secretary of State, US Senate Committee on Governmental Affairs, *Terrorism Financing*, 31 July 2003, [http://80-web.lexis-nexis.com.ezproxy.library.tufts.edu/congcomp/document?\\_m=79d8326d99a1f69087234d30eec3bbba&\\_docnum=8&wchp=dGLbVtz-zSkSA&\\_md5=70cdb70820d3b858bb6d047f4b3d2b0d](http://80-web.lexis-nexis.com.ezproxy.library.tufts.edu/congcomp/document?_m=79d8326d99a1f69087234d30eec3bbba&_docnum=8&wchp=dGLbVtz-zSkSA&_md5=70cdb70820d3b858bb6d047f4b3d2b0d)

<sup>bi</sup> Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation, U.S. Senate Committee on Appropriations, Subcommittee on Foreign Operations, 21 April 1998, [http://www.fas.org/irp/congress/1998\\_hr/s980421-lf.htm](http://www.fas.org/irp/congress/1998_hr/s980421-lf.htm)

<sup>bj</sup> James O. Finckenauer, International Center National Institute of Justice, *Russian Organized Crime in the United States*, <http://www.ojp.usdoj.gov/nij/international/russian.html>

<sup>bk</sup> Testimony of Colonel Stanislav Lunev, United States House of Representatives, Committee on National Security, Military Research and Development Subcommittee, 4 August 1998, *United States/Russian National Security Issues*, [http://commdocs.house.gov/committees/security/has216010.000/has216010\\_1.HTM](http://commdocs.house.gov/committees/security/has216010.000/has216010_1.HTM)

<sup>bl</sup> Chechen rebels. Gunarantna states that this particular group is the most feared of the three main bodies of Chechen fighters.

<sup>bm</sup> Gunarantna, 180.

<sup>bn</sup> These were quickly suppressed by the Chinese Triads, which did not appreciate the presence of Russian Mafia members in their respective territories. See Bruce Michael Bagley, School of International Studies, University of Miami, *Globalization and Transnational Organized Crime: The Russian Mafia in Latin America and the Caribbean*, 31 October 2001, 4–5. [http://www.mamacoca.org/feb2002/abs\\_bagley\\_globalization\\_organized\\_crime\\_en.html](http://www.mamacoca.org/feb2002/abs_bagley_globalization_organized_crime_en.html)

<sup>bo</sup> Scott O’Neal, “Russian Organized Crime,” *FBI Law Enforcement Bulletin*, May 2000, Vol.69, No. 5, 4, <http://www.fbi.gov/publications/leb/2000/may00leb.pdf>

<sup>bp</sup> Main Intelligence Agency, former Soviet Union.

<sup>bq</sup> Testimony of Colonel Stanislav Lunev, United States House of Representatives, Committee on National Security, Military Research and Development Subcommittee, 4 August 1998, *United States/Russian National Security Issues*, [http://commdocs.house.gov/committees/security/has216010.000/has216010\\_1.HTM](http://commdocs.house.gov/committees/security/has216010.000/has216010_1.HTM)

<sup>br</sup> David Slatter, *Darkness at Dawn: The rise of the Russian criminal state* (Yale University Press, 2003).

<sup>bs</sup> Robert Friedman, *Red Mafiya: How the Russian Mob has invaded America*, 112–113. (New York: Berkley Books, 2002).

<sup>bt</sup> Interview of George Annarella, NYDA Office, 13 October 2004

<sup>bu</sup> Quote taken from U.S. Department of Justice, FBI National Press Office, 13 August 2003, <http://www.fbi.gov/pressrel/pressrel03/igla081303.htm>

<sup>bv</sup> Bruce Hoffmann, *Inside Terrorism*, 201 (London: Columbia University Press, 1998).

---