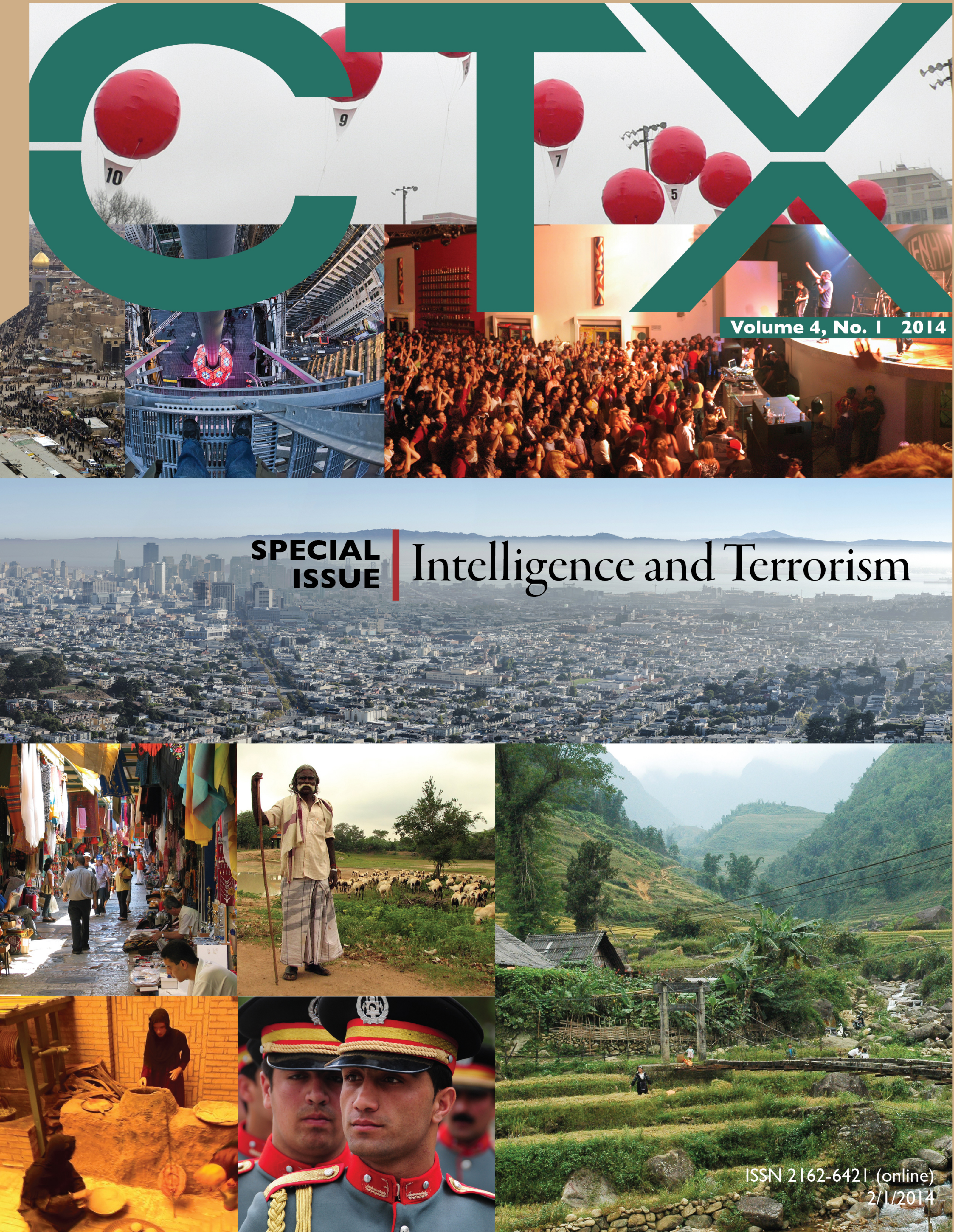
CTX

Volume 4, No. 1 2014



SPECIAL ISSUE | Intelligence and Terrorism

ISSN 2162-6421 (online)
2/1/2014

From the Editors

Welcome to this special issue of *CTX*, "Intelligence and Terrorism." The articles and roundtable discussions gathered in this issue came out of a workshop that took place at the Naval Postgraduate School (NPS) in Monterey, California, in August 2013. We wish to thank the Combating Terrorism Fellowship Program (CTFP) for sponsoring the workshop and for its continuing support for *CTX*.

No matter which strategy we choose to deal with terrorism, the more we know about the terrorists, the more likely we are to achieve our objectives. While intelligence presumably is important in all of our strategic endeavors, experience has found it to be particularly important in the case of terrorism. Terrorists hide, and if we are to deal effectively with them, they must be found. Broadly understood, intelligence is what does the finding. As both an activity—the collection and analysis of information—and a product—the final intelligence report—the purpose of intelligence is to inform the decisions of policymakers and operational leaders. As the current information technology revolution has rolled on, it has affected both the gathering and uses of intelligence and the terrorists themselves, who are now among the principal targets of intelligence work. For that reason, it is worthwhile to consider the current relationship between intelligence and terrorism.

The August meeting gathered together a small group of military, police, and civilian officers with experience in intelligence and in combating terrorism. This group included senior officers with decades of experience as well as some students currently enrolled in the CTFP curriculum. Participants came from the United States, Europe, the Middle East, and South and East Asia. Over the course of a day and a half, they discussed the ways in which terrorism has changed, current intelligence requirements, roles and missions among intelligence agencies, and intelligence sharing. Reflecting the diversity of their backgrounds and operational experience, the participants offered a variety of views about all of these topics. For example, some declared that terrorism has changed in fundamental ways over the past two decades, while others, despite acknowledging some differences, argued that the fundamentals of terrorism have remained the same. There was broad agreement on the issue of requirements, but less on roles and missions because the division of labor depends so heavily on the circumstances within each country. Several senior officers offered some hard-earned wisdom on how to establish effective intelligence sharing. The three-part conversation presented in this issue raises a number of important questions about intelligence and terrorism and suggests a variety of ways to answer them.

In addition to this meeting, *CTX* commissioned four articles on the role of information technology at the nexus of intelligence and terrorism. Dorothy Denning leads off with an exploration of the potential roles that social media and social networks can play in large-scale searches for objects and individuals. John Mitra, a CTFP alumnus, discusses the uses and limitations of modern technology in India's campaign against Maoist insurgents, who are a decidedly low-tech opponent. James Walsh then considers how access to "big data" through new technological data-mining techniques may affect intelligence sharing among governments.

The final article, by Erik Dahl, is not about information technology. It is a case study of a foiled terrorist plot. In recounting this case, Dahl touches on themes raised in the workshop's conversations, in particular the difficulties posed by intelligence work that may end up in court. The case also displays the confluence of luck and skill that is good intelligence work and offers an illuminating portrait of what it is like to work with a confidential source. Dahl's article provides a fitting conclusion to this special issue.

For those of you who are interested in delving further into the ideas presented in this issue, we have included an annotated bibliography, which provides some suggestions for further reading and offers a variety of views pertaining to intelligence and terrorism.

The Combating Terrorism Archive Project (CTAP) interview also is a special one this time, comprising two complementary pieces. In early December, director Peter Berg came to Monterey for a special screening of his new film *Lone Survivor* for students, faculty, and staff of NPS's Defense Analysis department. The film is based on the book of the same title by former Navy SEAL Marcus Luttrell. A brief interview with Mr. Berg, which followed the screening, is presented first, followed by a subsequent roundtable discussion of the film with three Special Forces officers who attended the screening.

The U.S. television series *The Wire* is the topic of this issue's Moving Image column. MAJ Matthew Upperman describes the ways in which this often bleak depiction of inner-city Baltimore can offer lessons to the Special Forces and intelligence communities. For The Written Word, MAJ Anthony Keller reviews the book *The Way of the Knife,* a nonfiction account of the working relationship between the Central Intelligence Agency and U.S. Joint Special Operations Command both before and after 9/11. Finally, be sure to look at the latest offerings from the Joint Special Operations University (JSOU) in the Publications Announcements.

> In peace there's nothing so becomes a man
> As modest stillness and humility:
> But when the blast of war blows in our ears,
> Then imitate the action of the tiger.
> —*Henry V* (3.1.1), by William Shakespeare

DAVID TUCKER

Guest Editor
Professor, Department of Defense Analysis
U.S. Naval Postgraduate School

ELIZABETH SKINNER

Managing Editor, *CTX*
CTXEditor@globalecco.org

Special Issue: Intelligence and Terrorism

About the Contributors

Dr. David Tucker, guest editor of this special issue of *CTX*, is an associate professor of Defense Analysis at the U.S. Naval Postgraduate School (NPS) in Monterey, California, where he teaches courses on terrorism and intelligence. From 1991 to 1998, he worked at the Pentagon, in the Office of Special Operations and Low-Intensity Conflict, on a variety of defense and intelligence issues. He joined NPS in 1998, where he has taught in both the Defense Analysis department and the Center for Homeland Defense and Security. His publications include *Illuminating the Dark Arts of War: Terrorism, Sabotage, and Subversion in Homeland Security and the New Conflict* (Continuum, 2012) and *The End of Intelligence: Espionage and State Power in the Information Age* (Stanford University Press, forthcoming in Spring 2014). He earned his PhD from Claremont Graduate University.

Peter Berg is an actor, writer, and director. His latest feature film, *Lone Survivor,* was released in December 2013. Mr. Berg earned his BA in drama from Macalester College in St. Paul, Minnesota, in 1984. After moving to Hollywood, he acted in a number of TV series and feature films before turning to screenwriting. His first major writing and directing success was *Friday Night Lights* (2004), which was turned into an award-winning TV series of the same name.

Major Patrick Collins is a U.S. Army Special Forces officer with 12 years of experience and multiple deployments in the Central Command (CENTCOM) and Pacific Command (PACOM) areas of responsibility. He previously served as Special Forces Detachment commander, Special Forces Company executive officer, and Mobility Commodity chief at Headquarters, U.S. Army Special Operations Command. MAJ Collins is currently earning his master's degree in Defense Analysis at NPS.

Dr. Erik J. Dahl is an assistant professor of National Security Affairs at NPS, where he is on the faculty of both the National Security Affairs department and the Center for Homeland Defense and Security. Dr. Dahl is the author of *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Georgetown University Press, October 2013) and a number of journal articles. He earned his PhD from the Fletcher School at Tufts University. Dr. Dahl retired from the U.S. Navy in 2002 after serving 21 years as an intelligence officer.

Dr. Dorothy E. Denning is a Distinguished Professor of Defense Analysis at NPS, where her focus has been mainly in the area of cyber security and cyber conflict. She earned her doctorate from Purdue University, which later named her a Distinguished Science Alumnus. Dr. Denning is the author of *Cryptography and Data Security* (Addison-Wesley, 1982) and *Information Warfare and Security* (Addison-Wesley, 1998). She has received numerous awards, including the Ada Lovelace Award, the National Computer Systems Security Award, and the Harold F. Tipton Lifetime Achievement Award. In October 2012, she was selected to the inaugural class of the National Cyber Security Hall of Fame.

Major Anthony A. Keller, U.S. Army Infantry, is currently studying in the Defense Analysis curriculum at NPS. He has served in Stryker and Air Assault units and the 75th Ranger Regiment as an infantry platoon leader, a Ranger rifle platoon leader, an infantry company commander, and a Ranger company commander.

D. M. "John" Mitra is the joint director of the National Crime Records Bureau, India. He has held many posts in the Madhya Pradesh Police and the Indian federal government, including superintendent of police in three districts; deputy inspector general of the Special Armed Force, Administration, and Home Guards; and Additional Director General of Railways, Complaints, and Narcotics. Mr. Mitra recently contributed a field study for a research project on the impact of developmental initiatives in Maoist-affected areas. Mr. Mitra earned a BSc in physics (with honors) from Ravenshaw College, Odisha, India, and an MS in Defense Analysis from NPS.

Commander Brian O'Lavin graduated from the U.S. Naval Academy in 1996 with a BS in systems engineering. In 2009, he graduated from the U.S. Naval War College with an MA in national security and strategic studies. He is currently working toward his PhD in security studies at NPS. In 1996, CDR O'Lavin graduated from Basic Underwater Demolition and SEAL training. As a SEAL, he has deployed to European Command (EUCOM), PACOM, and CENTCOM.

Lieutenant Colonel Gabor Santa is a member of the 34th Special Forces Battalion, Hungarian Army. In Iraq in 2007, he was the assistant team leader of the Hungarian Military Assistant and Liaison team, NTM-I. Two of his three deployments to Afghanistan were as a member of the Hungarian SOF: in 2008, LTC Santa was a partnering officer in the International Security Assistance Force SOF Headquarters, and in 2012, he served as Hungarian SOF Special Operations Task Unit liaison officer. He is currently studying at NPS.

Major Matthew Upperman is a U.S. Army military intelligence officer who is currently assigned to the 7th Special Forces Group (Airborne). He recently earned an MS in Defense Analysis from NPS. MAJ Upperman has a combined 36 months of deployment time to Iraq, Afghanistan, and the Philippines in support of Operation Iraqi Freedom and Operation Enduring Freedom.

Dr. James Igoe Walsh is a professor of political science at the University of North Carolina at Charlotte. He is the author of two books, including *The International Politics of Intelligence Sharing* (Columbia University Press, 2010), and a number of articles in academic journals. He is currently writing a book on the political consequences of the use of drones and similar technologies in counterterrorism and counterinsurgency campaigns, and was recently awarded a grant from the Department of Defense's Minerva Research Initiative to analyze how armed groups finance their activities and the consequences for military conflict.

COVER PHOTO

See image credits, page 103.

DISCLAIMER

This journal is not an official DoD publication. The views expressed or implied within are those of the contributors and do not necessarily reflect the views of any governmental or nongovernmental organization or agency of the United States of America or any other country.

TERMS OF COPYRIGHT

A Roundtable Conversation on Intelligence and Terrorism
Part One: The Changing Nature of Terrorism[1]

MODERATOR: Has terrorism changed in any ways that have changed intelligence requirements, or the way in which the business of gathering information about terrorists and their organizations has to be done?

The participants in this conversation were guaranteed anonymity to encourage a frank discussion of sensitive issues. Their opinions are their own and do not reflect the official policy or positions of the U.S. government or any other government, agency, or official entity.

The icons at the beginning of paragraphs are assigned to individual speakers.

● I believe there is a fundamental change in the objectives of terrorists and what they are after. Back in the days when we were chasing after state-sponsored terrorist groups, most of the groups had rather specific and somewhat limited objectives. This was true of the Baader-Meinhof Gang, for example. They started out with a very specific objective, which was to destroy the American presence in Germany because of the gang's opposition to the American role in Vietnam. The difference today is that we are dealing with people whose objectives are millennial, global, and perhaps not even clear to themselves in many cases. I was involved in a project that looked at Libyans and others coming through Syria into Iraq. The real thing that bothered me was the number of people who just wanted to commit suicide. That was their stated goal. They wanted to go to Iraq to get killed in a terrorist bombing and take out people with them. In Bosnia and Croatia, we had information on hundreds of Arab and Asian volunteers who were being expelled from Bosnia. What was amazing was their absolute lack of any kind of central direction in life. They were generally young men or men who were failures in one capacity or another, estranged from their families in almost all cases, complaining about not getting their share of the family inheritance, and with a desire to kill. Why? They didn't even know. That is the only real change I have seen. The rest of it to me is just tactics.

The difference today is that we are dealing with people whose objectives are millennial, global, and perhaps not even clear to themselves in many cases.

◆ I agree completely. There are two periods of terrorism. The first period was tied to Middle Eastern problems, roughly from the end of the 1960s to the end of the 1980s. The groups were more or less organized, were tied with states, and shared the goals of those states. Then in France at the beginning of the 1990s, we saw the change to a kind of global terrorism. The GIA [Armed Islamic Group] in Algeria at this time was backed by the anti-Soviet mujahedeen in Afghanistan and trained in Afghanistan. The GIA published a magazine in London [al Ansar], and the GIA was supported by the people in Afghanistan and Pakistan as a good example to follow. From the beginning of the 1990s, we saw people going to Bosnia from France, who came back to France with weapons and materials and wanted to take action in France. Later we also had people going to Pakistan, most of the time through London because the pipeline was well organized by the Islamists there, and then we see Chechnya and so on. And these are largely self-recruited people.

But for intelligence, there is no change of methods. It is a problem of discovering these people. They come from our population, are born in our countries, are upset about their social status, as you say. The problem is to have enough resources to discover these people. Most of them don't know what they want. That's true. But security, intelligence, and law enforcement services cannot solve that problem. We do our best to arrest people, to prevent actions, but the solution will come from society.

Most of them don't know what they want. That's true. But security, intelligence, and law enforcement services cannot solve that problem.

✕ Yes, I broadly agree with most of what the previous speakers have said, but I do think there are some fundamental differences between the terrorism that we are engaging with today and previous forms of terrorism, in the following respects. First, the terrorism that we experienced in the 1970s, 1980s, and to a certain extent the very early 1990s was in general linked to some form of nationalist agenda. When people talk about the changes in scale since the 1990s, as the previous speakers have, I think that is absolutely right because what we now have is a nearly global rejectionist philosophy that has been embraced by a broad sector within the Muslim communities in a number of different countries. It has also tapped into the personal disgruntlement and alienation that those individuals have felt as a result of whatever socioeconomic or political conditions may exist in individual countries. I think that is fundamentally different from what came before, because now a young man of Pakistani ethnic origin in the UK, who has never been to Pakistan, all of a sudden can feel an emotional engagement with events that are taking place on the other side of the world. At the same time, this can fuel a personal sense of grievance that this individual may have.

Afghan resistance fighters return to a village destroyed by Soviet forces, 1986

The second area where I think there is a fundamental difference today is that, whereas previously a lot of the terrorism that we had to fight was state sponsored or state supported in some way, that no longer exists. For instance, the IRA [Irish Republican Army] was supported by the Libyan regime [of Moammar Qaddafi] in a number of different ways. A lot of the Palestinian extremist organizations in the 1970s and 1980s had support from various countries in the Middle East. In fact, their operational headquarters were based in those countries and derived significant amounts of support in terms of personnel, materiel, financing, and so on. The disappearance of state support makes a big difference. The approach the intelligence community took for tackling those forms of terrorism was to target the intelligence services of those countries and engage at the political level with them. For instance, if you were trying to tackle the PFLP–GC [Popular Front for the Liberation of Palestine–General Command], then you knew that you had to try to penetrate the Syrian services. There were fixed points where you knew you could stop the operational activity. That no

We are dealing with a transnational terrorist problem that forces us to engage in a completely different way. It is about trying to find terrorists hidden among populations.

longer exists. What we are dealing with is a transnational terrorist problem that forces us to engage in a completely different way. It is about trying to find terrorists hidden among populations. The problem is compounded by the fact that the terrorists are in countries that are at best fragile or, at worst, completely dysfunctional. Therefore, again, one of the tools that we were able to use in the past no longer exists. In the past, we could try to either penetrate a country's intelligence services to get a better idea of the level of support that they were providing to certain terrorist organizations, or engage with those intelligence services in order to co-opt them into helping us fight the terrorist problem. That is no longer a useful approach.

◠ Hasn't religion been one of the changes that has taken place in terrorism? When I think of the first stage of terrorism from the late 1960s through the 1980s, when I think of plane hijackings, for example, and those sorts of things, the purpose wasn't necessarily to kill large numbers of people. There were specific goals, maybe to broker the release of prisoners someplace. With al Qaeda and the terrorism that we saw developing in the early to mid-1990s to the present day, advancing religious purposes was at least a kind of guiding purpose or aim—for example, the establishment of a worldwide Caliphate or shari'a law here and there. So I am wondering if others see that as a significant change in terrorism.

★ I would say religion may be the motivation of the individual terrorist, but not necessarily the motive of those who are directing the movement. Osama bin Laden had a very clear goal in mind, and that was to get rid of the Saudi monarchy. The method that he chose was to harness the disillusionment or the religious grievances of thousands of people around the Middle East. But I would say that he was not a religious leader. Bin Laden and people like him, Abu Nidal and others going back generations, are just very clever public manipulators of people, and they will take on whatever cloak they need to get other people to do what they want them to do. They don't risk their own lives. The real question is what is driving terrorism, what guides it, what directs it, what manipulates it—that may be something very different.

Religion may be the motivation of the individual terrorist, but not necessarily the motive of those who are directing the movement.

+ But does the motivation matter? I mean, in this sense, if you talk about religious motivation, would that change the way people organize? Would it change the way they think about targets? Would it change the things that terrorists do if they have a religious motivation as opposed to a nationalist motivation? Would that change any of those things?

The difference is that they are ready to die. The people who went to Iraq wanted to be killed.

◆ The difference is, as we said before, that they are ready to die. As somebody mentioned, the people who went to Iraq wanted to be killed. I remember a case where we had put a family on telephone taps. The son was in Iraq, and he telephoned every day, and he said, "One day if I don't come back to you, it means that I will be in heaven."

⧓ If the question is about fundamental changes in terrorism, I would mention a couple of things. One is the rise of suicide terrorism attacks, which were not common before the 1980s and have become more common. The other one is that the rise of the internet allows groups to communicate with their target audience in a less mediated way. They can generate propaganda and distribute it more directly to people of interest. So that may influence their ability to recruit supporters and do other things. Of course, it was a lot more difficult before maybe 10 or 15 years ago. The internet is new, but even earlier, students put cassette tapes together and sent them to Iran, and that is what built Ayatollah Ruhollah Khomeini's popularity.

✕ I don't think the form of international terrorism that al Qaeda represents today is fundamentally different. The brilliance of the al Qaeda narrative taps into the sense of grievance that so many young Muslims apparently feel across any number of countries, and that is fundamentally different. Furthermore, I think now that we are in the internet age, for instance, the barriers to entry for terrorism are very low. That is also fundamentally different from before. Previously, just going about training yourself was much more complicated. Now we see any number of self-starters who are able to go online and find out what the best way of making a bomb might be, and away they go. I think the barriers to entry from the cyberterrorist perspective are even lower. That has made a fundamental difference in terms of the philosophy, if you can call it that, that motivates young men and some women to commit terrorism. The barriers to entry for terrorism are now so low that the internet creates a fundamentally different situation for us all to confront.

The barriers to entry for terrorism are now so low that the internet creates a fundamentally different situation for us all to confront.

MODERATOR: May I ask you if you see those changes you were mentioning as fundamentally organizational issues? In other words, the original groups recruited people. They trained people, to one degree or another. So there were specific organizations—you mentioned the PFLP–GC. And that meant each of those organizations had a context, a state sponsor perhaps or a geographic location, and that determined how you went about targeting them and trying to deal with them. So would it be fair to say that the difference, the fundamental change, is an organizational change, so that you no longer have to be part of a group to learn how to make a bomb, and that group no longer has to maintain expertise and try to pass it on to new recruits? Again, from the viewpoint of intelligence, it may be much more difficult now to target or to think about how you target the people who are involved.

✕ Yes, that's true. I think there are three aspects to this. First, the narrative has tapped into a sense of grievance among many people. Just consider the example of the recent murder of Drummer Lee Rigby in London.[2] Only one of the two men had some connection to groups and individuals who were known to the intelligence community as being potentially of terrorist interest. That demonstrates that there are potentially any number of young terrorists within our communities. Second, you don't need to go anywhere to get the training. The consequence is that targeting individuals becomes much more difficult. The third element is that it is very easy to commit a terrorist act. You can go to a shop and buy a kitchen knife. If you run amok in a shopping mall and stab lots of people, that in itself would be a very frightening event, which will have a disproportionate impact on a government. Why? Strategically, I am afraid, the death of one soldier on the streets of London makes absolutely no difference whatsoever to government policy, to national security. But the psychological impact that this one act has is grossly disproportionate.

■ I want to bring the conversation back to the idea of the historical perspective of terrorism and the relevance of religion. Religion has always been one of the prime motivating factors of terrorism. Beginning back in the first century BC, we could be a group of Roman centurions discussing the assassins of the Sicarii in Jerusalem for all that it matters. Even the issue of suicide terrorism is not necessarily new. It is simply a recurrence of the cycle that we are seeing. We see different methods, we see greater effect, but it is not something new. I am speaking from a law enforcement perspective in the sense that, as we investigate these domestic cases, we are not really seeing anything new. We are just seeing new ways that terrorists are trying to implement these methods.

✕ I think that is wrong, because you have to ask, "What is the endgame?" If you asked your PFLP–GC or Abu Nidal terrorist, "What is your endgame?" they would have said that the endgame is either the end of Israel and the creation of a Palestinian state, or that a Palestinian state and Israel had to live in some form of coexistence. There was an endgame. If you asked the young Nigerians who killed Drummer Rigby, "What is your endgame? What do you hope to achieve? Was there any deal that we could have done with you before you committed this act that would have made you not do this?" I think they would have struggled to respond. I think they would have eventually come up with, "You need to get out of Afghanistan. You have got to stop killing Muslims." There was no positive endgame that they could have identified that would have enabled us to have any kind of rational engagement. I think that is why the phenomenon today is fundamentally different.

If you asked the young Nigerians who killed Drummer Rigby, "What is your endgame? What do you hope to achieve?" I think they would have struggled to respond.

▲ Maybe, but look at Hamas. A lot of their leadership came over from socialist movements that failed at the end of the Soviet Union. So they were looking for a new organizational tool.

✕ But a new organizational tool to achieve what?

▲ A very limited goal: a Palestinian state.

✕ Yes, and as a goal, you could have a discussion with them about that. I am sure that people a lot more clever than myself can draw up an interesting graph that indicates the number of terrorist attacks conducted against the state of Israel while there were ongoing discussions between the Israelis and the Palestinians brokered by the United States. There is a correlation, isn't there, between the possibility of the creation of a Palestinian state and the level of terrorism in that part of the world? Whereas there is no correlation, from our perspective, when it comes to terrorist acts that are conducted in the UK and elsewhere, with whatever outcome or endgame might be intended. There is no discussion. There is no stated end state other than Osama bin

The debate we are having is whether al Qaeda represents the future or is a one-off exception to the norm of terrorism that has existed for thousands of years.

Laden's desire to return to some golden age of the Caliphate, which in reality never existed.

▼ It seems as if we are talking about al Qaeda as the new terrorism, right? We are obsessed with that for good reasons, but then the debate seems to be whether al Qaeda is the future as a dispersed network, using the internet, with religious millennial goals. Are they the future, or are they the aberration? Are they the abnormality and groups like Hamas, Hezbollah, and, until a few years ago, the LTTE [Liberation Tigers of Tamil Eelam], the Taliban, the norm? Some of these groups still have state sponsors. You have a lot of those groups that are still out there, but you also have groups like al Qaeda, or at least affiliates or people connected to them, killing people on the streets of London. So I think the debate we are having is whether al Qaeda represents the future or is a one-off exception to the norm of terrorism that has existed for thousands of years. That is what we are really coming back to. I don't know what the answer is. I think 10 years from now or 20 years from now, maybe we will know, but I think that is where we are at right now.

◆ The young people who live in our country, they are asocial people who have a problem with society. They know nothing about religion. Absolutely nothing. With Sunni Islam—tell me if I am wrong—anybody can preach. In France, there was a young preacher. He pushed more than 20 people to go to Iraq after the American operation. He was not trained, but he was preaching very fervently, and all those young people were waiting for that because they want to fight society. I repeat—they don't know anything about religion. They see only black and white. They are white, and the society is black. So they want revenge. They want to do something. This is more a social than political problem.

You were mentioning earlier the problem of the traditional organizations, such as Abu Nidal, Hezbollah, and so on. You think it was easier to penetrate them? I don't think so. Who has ever penetrated Hezbollah? I think nobody. When they put bombs in Paris in 1995 and 1996, it took a month to get information, and we did so only because one of the people we arrested before was tempted by the reward of one million francs and wanted revenge against the organization. So it is not as easy as that. I think the real problem, which has not changed, is that you need to have a system. We must develop more sources because it is more difficult to detect the terrorist within society. It is a question of organization, international cooperation, national cooperation, and resources, more than the fact that terrorists have changed or not changed.

● I used to keep in my office in Beirut a picture of a soccer team, 11- and 12-year-old kids, who were in a sporting club. Among that group were Hassan Izz-Al-Din, Imad Mugniyah, one of the Nasrallah brothers—you don't penetrate an organization like that. These kids grew up together, and it would be like trying to penetrate Tony Soprano's gang. You can gather intelligence from the outside, you can gather intelligence electronically or using various means, but you don't penetrate the core group. Nobody ever penetrated Hezbollah because they all grew up together. They all know each other.

Nobody ever penetrated Hezbollah because they all grew up together. They all know each other.

✕ I think the important question from my perspective is this. When we pull out of Afghanistan, and if there is some success in the negotiations between Israel and the Palestinians, would that decrease the likelihood of support for al Qaeda within the Muslim communities in our countries? Ostensibly, two of the greatest motivating factors that promote the idea of violence among young men within our Muslim communities will be eliminated.

■ It's a rhetorical symbol, though, for al Qaeda, right? They didn't fly those planes into buildings in Tel Aviv. The Israeli-Palestinian conflict is just a rhetorical symbol to rally people. They have a few limited goals related to politics, primarily in Saudi Arabia, and then by extension in the region.

✕ That is my point. There is no endgame for a lot of these people. There is no goal, there is no negotiated outcome.

◆ If we take away the goalless quality of the violence, does that return us to the situation we had with the IRA and PKK [Kurdistan Workers' Party] and all the other groups that we are familiar with?

⬮ The Mahdist movement in the Sudan lasted for 100 years after the Mahdi died. It just kept up because there were certain people who were disaffected, who were always willing to do something. But the Mahdi was long dead.

● You raised the question of Palestinians. I argue that the Palestinian problem is the root of all the terrorist organizations. Solving the Palestinian and Israeli problem will not end terrorism, but it will affect it very much, and it will help our narratives in countering terrorism. The terrorists don't care about the Palestinians. They are now in Syria fighting the regime that is against Israel. But they still have the narrative that they are fighting against Israel. So the narrative is supporting them a lot if we consider recruitment, especially in the Middle East, Yemen, and Saudi Arabia—the governments that have good relationships with the West. [The people they target for recruitment] feel that there is no hope, that their governments cannot deal with Western governments. They arrive at the point that they have to do something. That is when the recruiters, the smart people that you mentioned, take the chance and tell them, "Okay, now you know what? You have to do something. This is your duty and honor, and you have to go." That is how these people are recruited. That narrative is behind the terrorists. We are just waiting for them to pop up to try to fight them and will continue doing the same thing, no matter how techniques and our technology to kill them and target them develop. You are targeting a man, not the ideas and the narratives behind the man.

Syria now is full of terrorist organizations. Before the Arab Spring, no terrorist groups were found in Syria, just some Palestinian groups.

Graffiti depicting Hassan Nasrallah (leader of Hezbollah)

★ But we have to pay attention to the environment that is around the terrorist organization. In my opinion, the Israeli-Arab conflict is not the main issue now in the Arab world or the Muslim world, because the people watching the news are watching Syria. They are watching Egypt, they are watching Libya. Most of them do not know that there are negotiations between Israelis and Palestinians. So the change in the environment will decrease or increase the numbers of organizations and groups. Syria now is full of terrorist organizations. Before the Arab Spring, no terrorist groups were found in Syria, just some Palestinian groups. So this changed environment will increase terrorism in the Arab world.

◆ That is exactly what countries in Europe are concerned about: the consequences of the Arab Spring. If you have a huge Muslim community [in your country], 100 people are concerned by this Syrian fighting and will go to Syria, through Jordan or Lebanon. According to past experience, a lot of the people we have arrested came from Bosnia; they went through Chechnya. The jihadis were from Iraq before, and now they are from Afghanistan or Pakistan's tribal areas. They have learned how to bomb, and they come back with the will to commit terrorist attacks. In our country, for instance, where the majority of the Muslim community is Arab, the Palestinian problem remains a very important problem. When you go into a mosque, the people that give *zakat*, they give money for the Palestinian cause.

♥ Most of the things you are saying apply to India. But the fundamental difference is that the funds that used to come to the terrorists because of state sponsorship have dried up. When those funds were there, it attracted the wrong kind of people. Criminals actually got into terrorism because it was an easy way to make money. You get money from the sponsors, but they can't keep track of how you spend it. Then, in the name of terrorism, you can loot banks and all of that and make money. So attracting the wrong kind of people meant that the movement was going in a downward direction. It was losing the narrative and the popular support it was trying to gain. Now, the terrorists are not flush with funds, but they don't need that much money to make these IEDs they use. They want to make news; they have to make news. The more people they kill, the better. Even just making a blast without killing someone can make national news.

They want to make news; they have to make news. The more people they kill, the better.

Now when it comes to the future, if we can manage to stop the state sponsorship and control, then that kind of organized terrorism, with particular objectives, is going to decline because they need some kind of organization for that. But then you will have individuals to deal with. Some two or three people can decide what to do. They have the internet from anywhere and can decide what to do. It is hard to track them. We can't do much, except that we have to handle the border and what is coming in both from a state and from a non-state actor abroad. But inside India, they don't use modern communications. You don't have lines to tap, or other things like social networking from which you can try to guess who is what, and how it is working.

✕ I wouldn't necessarily subscribe completely to the view that state sponsorship is no longer an issue. There are still links between, for instance, Iran and some of the terrorism that takes place in both Iraq and Afghanistan. I think in Iraq, we only truly became aware of the extent of the problem that we

In Iraq, we only truly became aware of the extent of the problem that we faced among some of the Shi'a groups by actually discovering both Iranian and Hezbollah links.

faced among some of the Shi'a groups by actually discovering both Iranian and Hezbollah links supporting those groups. So, I wouldn't preclude the fact that we are going to have to carry on [targeting states and their intelligence services]. But not by any stretch of the imagination is targeting state sponsors the only solution.

MODERATOR: May I put you on the spot? You worked against the Puerto Rican Nationalists and against the Abu Nidal group in Puerto Rico, but also more recently against the ALF/ELF [Animal Liberation Front/Earth Liberation Front]. From the viewpoint of law enforcement, do you see any fundamental changes in those groups, how they operated, or how it was necessary to operate against them? I ask because the environmental group is often cited as an example of the new kind of terrorism we face, networked, leaderless, and so on.

■ Except that it is not really. It still fundamentally involves small cells, clandestine activity. It is no different trying to penetrate a group like that than it was trying to penetrate a cell structure of the Abu Nidal organization that existed in Puerto Rico in 1984. If you are going to develop human intelligence, you have to target people who show the greatest vulnerabilities for recruitment, which is exactly what happened in regard to the clandestine cell known as The Family that was conducting a number of environmentally motivated arsons in the Pacific Northwest [of the United States]. If you are going to try to penetrate a clandestine cell of suspected terrorists, you are going to try to target those who have the most vulnerabilities, the weakest sense of self, and exploit those vulnerabilities. Now, that takes a very strong development of intelligence about the individuals in the group. But it is basic law enforcement work that you are doing in trying to target them.

◆ May I add something? The difference between what we faced in the past and what we have to face now is that, in the previous case, the people involved rarely lived in the country they were targeting. They came from the outside. Sometimes they had some accomplices inside, but they were state sponsored. So the intelligence service was enough to work against them, and the intelligence service members were specialists. Now, with the new type of terrorism coming from the population, we have to mobilize all the services on the ground. You see? Everybody must be concerned—police, educators, prisons, social organizations, everything—in order to find the terrorist.

■ But that is a European-centric problem because it has always been that way in the United States, in the sense that homegrown terrorism is an American phenomenon, and it has been since the United States was founded.

+ But teachers in high schools in the United States don't think of themselves as intelligence collectors.

■ They do in regard to gangs, though.

+ But the suggestion is that we need to turn all of the social institutions—doctors, teachers, all of them—into collectors of information.

There is a focus now on these organizations, and getting the people who work in them to understand that they are part of the solution in a way that would have never occurred to them before.

◆ Also the religious leaders. In France, for instance, we believe that the Muslim authorities should help because they are moderates. They don't do it because it is too complicated for them. I think in Great Britain, it is different.

✕ That is absolutely right. We have found ourselves in a situation where the lead government department for the prevention strategy, which is basically tackling the causes of radicalization, is the Department for Communities and Local Government. Now, that department 10 or 15 years ago would never, ever have imagined that it would be part of the UK counterterrorism strategy. It has required from our perspective a fundamental rethinking. Unless you mobilize all of these people, the chances of the intelligence or the law enforcement community ever being able to identify potential terrorists is that much more difficult.

▲ In the United States, there are significant restrictions on law enforcement getting access to education records and medical records, so it is very difficult.

✕ It is the same in Britain. I think what we are saying is that there is a focus now on these organizations, and getting the people who work in them to understand that they are part of the solution in a way that would have never occurred to them before.

★ Terrorism is not a onetime incident. Leaders have to have a strategy and the means to carry it out. It is hard to change objectives. If you change the objectives as a leader, people in the organization will question you. When you are questioned as a leader, you will lose your support. It means the end of your organization. So, it is hard to change objectives. If the intelligence community focuses on the objectives or the goals of the terrorist organizations, then it slowly will be able to define the ways and means of the terrorist organizations. If not—if you focus on the ways—most probably you will not get the target. The Armenian Secret Army for the Liberation of Armenia, for example, may reappear for the one hundredth anniversary of the 1915 Armenian incidents. It will emerge again with the same name or another one, but from the same ethnic group, and try to accomplish the same goals. So, if we can define the goals of the terrorist organizations or if we focus on those as an intelligence community, most probably we would get the target, and we will accomplish our goals.

If the intelligence community focuses on the objectives of the terrorist organizations, then it slowly will be able to define the ways and means of the terrorist organizations.

As for the goals, I ask myself, "Does a terrorist organization have a religion or not?" I don't think so. There are lots of organizations, not only al Qaeda or Hamas. For example, the Red Army Faction didn't have a religion. Maybe the members of terrorist groups have a religion, but the terrorist organization itself, I think, doesn't have a religion. We should also consider some organizations recruiting members of various religions. For instance, the PKK. As far as I know, there are Zoroastrian, Christian, and Muslim members of the PKK.

▼ In India, we have some homegrown terrorism, but sponsored and trained from outside. Earlier they had to go outside the country for training. That was a chance for you to notice that somebody was missing, and if you had the support of the community, as a law enforcement agency, you should be able to know [somebody was missing]. It was a failure on the ground if you couldn't get that intelligence in time. But if your penetration into certain areas is limited, you might not notice somebody going out. It is a huge country. But going across the border has decreased now because these guys don't actually train in handling guns and all; they just know how to make IEDs. That is good enough to make a terrorist attack.

These guys don't actually train in handling guns and all; they just know how to make IEDs. That is good enough to make a terrorist attack.

As for religion, you have to distinguish between religion as a motivation and knowledge of religion and how religious someone is. Those are different things. The biggest motivation, or the satisfaction, that a suicide bomber has is that he is immediately going to heaven. If that solace is missing, you don't find a suicide bomber there. Our terrorists have all been linked to religion, and madrassas have been used for instilling that feeling that Islam is under threat unless you do something, and Allah is there with you. These guys, they don't understand the Qur'an or any of that. But they know this equation: I am fighting jihad here; I go [to heaven], so I don't care.

★ But there are cases where terrorists have a conscience and they give up detonating the bomb, and they believe in the same religion [as those who carry out attacks]…

🗨 Yes, yes, it is like people going and trying to commit a suicide attack, and at the last minute, they call their parents, who stop them from committing suicide. So that happens. We are human beings; the determination may not be as strong in some as in others. But religion has played a role in generating this feeling of injustice. Not only in India but all over the world. They keep targeting Israel, the United States. Of course, in madrassas, there are people who will help you in identifying and noticing what is happening. There are activities like Tablighi Jamaat [Society for Spreading Faith] in which people go around talking about Islam. There is nothing wrong with that. It is a constructive approach. But then, there may be one person planted there, who tries to locate recruits for terrorist activities. The community is the way you know about such things, because intelligence services cannot plant somebody everywhere. We had a sponsored attack in Mumbai, the biggest attack we have had.[3] They were all outsiders, they came from Pakistan…

There may be one person planted there, who tries to locate recruits for terrorist activities. The community is the way you know about such things.

◆ Yes, Lashkar-e-Taiba.

🗨 Yes, and they are still in Pakistan. Nobody has done anything with them. There is state sponsorship, some kind of involvement by the state to handle them, and some linkages at the lower level of operations. That is still going on. But this new phenomenon is something we need to watch out for because it is a more difficult, more challenging thing for law enforcement because you don't have linkages to tap on. You have to totally depend on this social interpretation to guess which person [is involved]; otherwise, he looks like a simple, ordinary person. How do you [identify potential recruits] when even the parents and the close family cannot guess that this boy is in that small group, a peer group, that is into this kind of activity? So to get at them is very difficult.

⧗ I would like to make a comment on the fundamental change in terrorism. At the end of the Cold War, it is true that state-sponsored, state-supported terrorism declined, but we should not forget countries like North Korea. They are still supporting terrorism, setting up cells in South Korea and in Japan as well. They are apparently very quiet now. But in a crisis, I don't think they will

We should not forget countries like North Korea. They are still supporting terrorism, setting up cells in South Korea and in Japan as well.

launch a missile attack. They will use terrorism. Second, I think that amateur terrorism based on religion will become very popular. I am not an expert on al Qaeda, but the comparison some like to make between al Qaeda and kamikazes is not true. The motivation is completely different. The typical kamikaze suicide was pressured by the organization. The pilots were not happy at all. But al Qaeda members feel very happy. Also, in 1995, Aum Shinrikyo was the first terrorist group that used chemical weapons. They were very intelligent young people. So it is very difficult for the police to find the candidate for a terrorist organization. This is a very big problem these days.

★ But if you talk about religion and terrorism, the number of religious people is much greater than the number who engage in terrorism.

💬 Yes, yes, India has a population that is 14 percent Muslim [about 176 million people]. It is the second biggest Muslim country, in that sense. You can imagine that if the percentage of people wanting to do terrorism was a little more, India would be in big trouble.

★ So terrorism is not just a religious or Islamic phenomenon.

⬢ I would like to add something to the picture. I am puzzled by the conversation. Take Anders Breivik.[4] Put aside all the stuff about motivation. The interesting thing is how he did it. I learned in our discussion that you need a motivator. There has to be somebody behind you. But as far as we know, that guy was totally self-radicalized, building a fertilizer bomb of about 1,000 pounds, which he blew up in central Oslo, driving up to a remote island and killing 69 youth. These guys are really hard to find. I agree so much with our British colleague here, that when you look at this case in particular, if somebody was to find out what he was doing, it would be in his school time. There was a history of some mental issues, but that is a closed chapter for security services. This could be just this guy, but it is a bad sign when in a rather transparent country like mine—transparent because if I go and buy fertilizer, I will pop up on a list—he masterminded this from a remote farm, building a bomb, making his own police uniform, taking legal education to acquire firearms, and that is what happened. And 77 people were killed.

Take Anders Breivik. Put aside all the stuff about motivation. The interesting thing is how he did it.

◆ The Breivik example brings out what the problem is because [even if we knew about the mental problems] there is no way to predict. In other words, somebody can engage in all sorts of activity that is perfectly legal and then it goes beyond that, but there is no way to predict or even to anticipate what would be the event that pushes somebody over that line. ❖

NOTES

[1] This discussion was edited for length and clarity. Every effort was made to ensure that the meaning and intention of the participants were not altered in any way. The ideas and opinions of all participants are theirs alone and do not represent the official positions of the U.S. Naval Postgraduate School, the U.S. Department of Defense, the U.S. government, or any other government or official entity.

[2] Drummer (Private) Lee Rigby, a British soldier who had served in Afghanistan, was murdered on a London street by two men who called themselves soldiers of Allah. See "Two Guilty of Lee Rigby Murder," *BBC News*, 19 December 2013: http://www.bbc.co.uk/news/uk-25450555

[3] For more information, see the *Guardian*'s collection of articles on the Mumbai attacks: http://www.theguardian.com/world/mumbai-terror-attacks

[4] For more on the Breivik massacre, see David Blair, "Anders Behring Breivik's Norway Shooting Spree Relived in Chilling Detail," *Telegraph*, 20 April 2012: http://www.telegraph.co.uk/news/worldnews/europe/norway/9217315/Anders-Behring-Breiviks-Norway-shooting-spree-relived-in-chilling-detail.html

A Roundtable Conversation on Intelligence and Terrorism Part Two: Requirements and Roles and Missions

Intelligence Requirements

MODERATOR: I would like to talk about roles and missions based on the various points that were brought up in the previous discussion on the changing character of terrorism. As a transition to that, could we talk a bit about intelligence requirements for terrorism, keeping in mind all the varieties that we have talked about? We talked about organizations, and dispersed organizations like al Qaeda, and individuals who suddenly pop up. Is it possible to talk about a set of requirements for collecting intelligence on terrorism, or does that depend on the particulars of the problem we confront?

Dick Cheney used the term *sleeper cells*, and all of a sudden everybody in the American intelligence community was looking for something that doesn't exist.

⬮ The problem [with trying to identify requirements in the abstract like this] is that the intelligence community reacts to what our leaders decide are the problems. Dick Cheney used the term *sleeper cells,* and all of a sudden everybody in the American intelligence community was looking for something that doesn't exist.

+ But we, in this room, don't have to respond to Dick Cheney…

⬮ But the political leaders decide what is important, and we do respond to them, and it's very difficult to try to explain to political leaders what this stuff is all about.

✕ It is possible to define terrorist requirements. I don't think, actually, that intelligence requirements have changed, even if we posit the possibility that the form of terrorism has evolved in a changing environment. I think the intelligence requirements have remained constant. Whether it has become more difficult to meet those requirements is a different issue.

MODERATOR: And how would you describe those requirements?

✕ Well, I think they have always been who, what, when, where, why, how. Globally, those are the questions. Increasingly we become fixated with the "why" to try and work out how on earth we are going to stop it in the future. But I think the perception is that those are the key questions.

In some communities, we train trash collectors, garbagemen, to watch for indications of bad activity and then call the cops.

⧓ In the U.S. case, since 9/11 we have seen two different approaches to looking at what we need for intelligence to counter terrorism. One is the international connections that national-level [intelligence] organizations go after. At the same time, in the U.S. and probably in most other countries, we are developing domestic, local law enforcement intelligence structures that aren't as well understood, and that gets back to the point about whether or not high school teachers are collecting intelligence. In the United States, we have programs of suspicious activity reporting that we are trying to grow. In some communities, we train trash collectors, garbagemen, to watch for indications of bad activity and then call the cops or [an emergency number]. That is an area that I think is more important when we are trying to prevent homegrown and domestic terrorism and the "lone wolf" sorts of things.[1] What clues law enforcement on to those individuals, in my experience, is a tip from a neighbor or somebody who talks to somebody else. We don't seem to get the sort of intelligence that actually prevents attacks within the United States so much from international connections.

A significant amount of terrorism is mitigated as a result of pocket litter that is collected in Afghanistan that reveals a phone number in Seattle.

■ You don't hear about them because it is classified. I can tell you from the inside looking out, having experienced that, that there is a significant amount of terrorism that is mitigated—maybe not prevented, but at least mitigated—as a result of pocket litter that is collected in Afghanistan that reveals a phone number in Seattle that sends an FBI agent out to talk to somebody. So we now know who you are, and we are going to begin an investigation on who is in your network.

◆ I think a state must have a permanent intelligence system with enough resources. The work requires mid- and long-term investment, including in [electronic surveillance]. Political leaders usually want immediate results, certainly in case of attacks, and they don't understand that [investigating] these things often takes time. The problem is that we can't succeed every time. We have to take this into consideration, and the politicians don't understand that. They don't want to understand that. The important thing is to make politicians give us the possibility to build a system, inside and outside, and to put all the resources together to do the maximum. Another thing, you were mentioning the [surveillance] work in the United States. Things have changed, mostly because of 9/11. I remember the first attack against the World Trade Center in 1993. It was made by a cell living in the United States, the Blind Sheikh[2] and some affiliated with him. When we talked to our friends in the FBI and said, "You have to put a telephone tap on them," at that time, Congress was absolutely against it. Of course, we can be accused of bugging only Muslims, but it is not the case. We also look at the extreme right. It is sometimes difficult. We recently arrested a friend of [Anders Breivik]. He had plenty of weapons, but we had nothing against him, so we had to release him. So we must keep an eye on everything, but we must concentrate much more on the main threat. I think this is fundamental.

The important thing is to make politicians give us the possibility to build a system, inside and outside, and to put all the resources together to do the maximum.

MODERATOR: When you were saying who, what, when, where, and why—is the assumption there that the principal purpose is to capture somebody before they commit the act or target people who may be involved in supporting those acts? Someone said earlier that is a losing game, so to speak. If we think about the way we have been describing this—lots of information out there, self-radicalized people—are those requirements sufficient, or are they really the only thing that intelligence can provide? There may be other things that need to be done or that we need to know, but is it simply not the business of intelligence?

✕ Crikey,[3] where do I start? I think those requirements remain valid because if they weren't, what would you be admitting? You would be admitting that actually the task is so impossible that there is no point in even trying to identify the perpetrators before they commit an act. I think that would be an admission of failure that none of us would be prepared to make. So I think those requirements remain valid. I think that is still the primary responsibility of both the intelligence community and law enforcement, the whole of the state apparatus, to do everything that it possibly can to identify those individuals who may be thinking of committing a terrorist act before they get to that point. It may be very difficult, but we still have a responsibility to do that because our fundamental responsibility is to protect the communities in which we serve.

Roles and Missions

✕ The target community, if you want to call it that, is now so diffuse that it actually requires an integrated approach that is very different from what we were doing 10 or 15 years ago. I think that takes us into the area that you wanted to explore, which is, what are the respective roles and responsibilities of intelligence services and the law enforcement community?

The target community, if you want to call it that, is now so diffuse that it actually requires an integrated approach that is very different from what we were doing 10 or 15 years ago.

MODERATOR: What I had in mind was the criticism made of certain elements of the U.S. military in Iraq, who focused on identifying and killing or capturing individuals. The argument made by General Flynn in his article[4] was that the environment, the surroundings, so to speak, were ignored. If you think about the need for a high school teacher to be a collector of information, as someone who knows the environment, the social relationships, it seems to me there is an analogy with the kind of argument that General Flynn made. His criticism of his own intelligence service in Afghanistan was that it was missing perhaps the most important part of what it should be collecting on. Then the question becomes, If that is true, how do you collect all of that other stuff, the kind of stuff the teacher knows? Is that even a legitimate intelligence function, or do we simply say, "No, that is a policing function"? It is the same way the police might deal with a group of kids who are stealing cars or something. We don't think of that in terms of intelligence.

✕ We are now taking a quantum leap from a generic discussion of the problem to some very specific areas. This takes us into the whole realm of intelligence providing the forward screen that enables us to identify potential targets that are going to attack us domestically, and also the role of intelligence in supporting expeditionary campaigns in places like Iraq and Afghanistan. I think those are two very different areas. I think on occasion, unfortunately, they have been seen as one and the same thing, which would be a mistake. You are also addressing issues that take us into the examination of the different approaches required to conduct a counterterrorist campaign or a counterinsurgency campaign. Again, I think those have been confused. Certainly they were confused in Iraq. I don't think the term *counterinsurgency* ever passed the lips of most of the U.S. generals I talked to until long after 2005. It was an absolute refusal to recognize what was going on, on the ground. But if you want to start trying to delineate the various intelligence approaches that are required in places like Iraq and Afghanistan, then I would be happy to try to start you off on that.

I don't think the term *counterinsurgency* ever passed the lips of most of the U.S. generals I talked to until long after 2005.

MODERATOR: I thought when you were talking about requirements [who, what, when, where, why, how], you might have been putting more emphasis on counterterrorism. I don't know if we want to continue to use those terms [*counterinsurgency* and *counterterrorism*] because I don't know if they are necessarily very helpful. But if, as others have said, the environment—what causes people to get involved in terrorism, or what contributes to people doing those kinds of activities—is important, then there is presumably information out there that we should know or could know that would help us affect that environment. The other view would be to say no, what we are going to do is try to go after the individuals before they commit the act, to prevent them from carrying out the attack. I don't mean to say those are mutually exclusive approaches; they probably have to be combined. I think other people here have suggested that. But they suggest to me different kinds of requirements and maybe even different kinds of intelligence functions.

You have to find these people. You have to neutralize these people. So you have to have both policies: prevention inside and attacking outside.

◆ I think it is important; it is a duty to prevent. In my country, we have special legislation: we are allowed to arrest people even before they begin to do something. It is with this legislation that we have arrested more than 1,000 people and we dismantled 40 or 50 or 60 plots. The situation is different outside [one's country]. I think there is no one policy [for dealing with terrorism]. You must prevent and you must attack outside also, because the people that we face in our countries have fought in Iraq or Afghanistan and so on. Where are the people who trained them? Where are the high-value targets? Recently, France had to act in Mali because of the AQIM [Al Qaeda in the Islamic Maghreb]. You have to find these people. You have to neutralize these people. So you have to have both policies: prevention inside and attacking outside.

There is a leader of the Muslim Brotherhood, which in France is called the Union of Islamic Organizations of France. He is a very well respected man. He doesn't ask people to go to fight, to become terrorists. But he is talking to the community, and he is developing the argument that you, the Muslim population, you are the best. You are different. You will be the future, and so on. So it pushes people to feel different from the rest of the population, exactly the thing against which we are fighting.

We had completely neglected a critical element, in terms of our ability to operate securely in Afghanistan, which was understanding the environment in which we tried to operate.

✕ The way that we have prosecuted our campaigns in Iraq and Afghanistan, until relatively recently, has been very different from the way we have prosecuted the intelligence campaign domestically, in one very important respect. In the first few years, both in Afghanistan and Iraq, we weren't addressing the intelligence requirement. And, I think we confused counterterrorism with counterinsurgency. The name of the game was just going after high-value targets in both of those countries. A consequence of that, in part, was actually to fuel the sense of grievance among the local population, to actually make the operating environment both in Iraq and Afghanistan even more difficult because we were failing to win ground with the local population. I think we have become more sophisticated now, and the point that General Flynn was making when writing his report was that we had completely neglected a critical element, in terms of our ability to operate securely in Afghanistan, which was understanding the environment in which we tried to operate.[5]

You know, we hadn't actually collected what in old parlance we would call "ground truth," which is who lives where, what do they do, who do they know, how do they relate, and how do those communities work, how do they then relate to each other, etc. [We didn't collect that] because we were so focused on chasing after high-value targets. So I think we are now much more focused on the why. The question then, of course, is who is responsible for collecting the why, for collecting that mass of local information? I am not sure you can call it intelligence in strict parlance, but who [is responsible for] developing that ground truth, for developing the understanding that allows us to then operate more effectively and engage with the local communities?

▲ I agree with that. What I took from General Flynn's report was that we understood very poorly the environment we were operating in. That was the fundamental lesson.

+ If that is true, in a certain way, this actually diminishes the role of what I think of as intelligence. It seems that domestically, if we need to understand the environment, that is essentially a police function. If we are talking about [understanding the environment] overseas, it seems to be something that intelligence, as it has been traditionally practiced, is not very good at. In a combat environment like Afghanistan or Iraq, you could argue that it is primarily a military function because that is where the military ought to have the primary role.

[Understanding the environment] overseas seems to be something that intelligence, as it has been traditionally practiced, is not very good at.

Maybe [our former FBI colleague] would object to this, but in the United States, there is no national domestic intelligence service…

■ Yes, I would object…

+ But it seems to me that [understanding the domestic environment], or understanding about certain people dispersed in a population, is really a police function. That is what [our colleague] was saying about India. And that seems to be the situation in France. That's different from Iraq or Afghanistan. It seems to me that the people who are most likely to collect that [environmental] information are not traditional intelligence people carrying out traditional intelligence functions.

The people who are most likely to collect that [environmental] information are not traditional intelligence people carrying out traditional intelligence functions.

◆ In [France], it is now not the police with intelligence power; it is an intelligence service with law enforcement power. But we use the same methods to penetrate, to infiltrate, and to work on terrorism. There is also a separate external service that belongs to the Ministry of Defense, but they are completely different [from the internal services].

● In [India], police are provincially organized. Police always had an intelligence wing, and this comes from the time of British control of India. In our country, the analysis is done by the intelligence agency because they have a pan-country vision or idea of what is happening. They can put things together and make a big picture, whereas the fragmented police at the local level are looking at individuals and trying to understand why they do this, or why they have these friends, or where they were for the last three years. The big picture is given by intelligence services to the police. The police and intelligence have been working hand in hand. We have problems of sharing intelligence, but the intelligence agencies are expected to pay attention to the big picture.

✕ To go back to the example of Iraq or Afghanistan, I am not sure which organization should take the lead in producing the rich picture of that particular country that would enable us to really understand who the key players are and where the communities are, etc. To be effective in the future, there needs to be a recognition that this is something that needs to be done, and that therefore anyone who is deployed on the ground ought to be collecting and offering up that local information to be fused into some kind of countrywide report.

Clearly there is a link between strategic interests and ensuring that your nationals deployed in a particular country are as safe and secure as possible.

I think it is a very good argument that the military should take the lead. Generally speaking, the military people have the biggest footprint, and they also have the critical mass that would enable them to do this piece of work. That is not to say that there isn't a very important contribution to be made by a country's external service, be it the intelligence service, or the diplomatic service, or NGOs [nongovernmental organizations], or coalition forces. But there is a requirement to try and capture all of that information as quickly as possible and to draw on, for instance, the expertise that may exist on that country before you even deploy. So, for instance, academics, authors, again NGOs, foreign service departments, and so on. What I am not saying is that it must be the military. It might make sense for the military to do this, but in fact, there needs to be a product that enables everyone involved to understand what is going on in that country and how it works and why it works in the way that it does.

MODERATOR: In a situation like Iraq or Afghanistan, what do you understand to be the specific contribution that the intelligence service can make?

✕ I am going to reference a point that [was] made before, which I think is absolutely right: the role of the intelligence service is to help support the national policy in that country. Of course, there are exceptions to this general rule, but certainly in the United Kingdom, the role of the intelligence community is to answer intelligence requirements that flow directly from an articulation of whatever the national strategic interests may be. Those national strategic interests are then translated into various different policies. Where it becomes more complex is that there is also a role for the intelligence community to provide force protection–related intelligence. Now you can argue where that starts and where it ends. Clearly there is a link between strategic interests and ensuring that your nationals deployed in a particular country are as safe and secure as possible. There is a role for the intelligence service in that. But how you then articulate those intelligence requirements and how you then meet those requirements, I think, becomes a separate issue.

+ Are you saying that the intelligence service has a focus that is more political and strategic, and that the military will probably focus more at the tactical level? That is a traditional way of understanding the division of labor in a situation like that.

▲ In 2003 and 2004 in Iraq, the [intelligence] products that I was seeing coming from the CIA were very focused on high-value targets. The things that I was reading coming from the military had to do with broad political understandings.

✕ It depends on the specific time period you are talking about [in Iraq]…

◆ In the French case, the DGSE[6] does both [tactical and strategic intelligence]. They have their own forces and may make their own operations if necessary, but generally the problem is really how to put all of that together.

[We worked on] reports that the Iranians had a secret training camp in Bosnia. A team spent four days hiding, going through the woods, to check that out.

● In the Bosnia campaign, we had 41 nations in the "coalition of the willing," and we worked out the intelligence support with the commander of SFOR [the NATO Stabilization Force in Bosnia] almost on a weekly basis. What do you need? What are you planning to do? Where are people going to be in harm's way? Is there anything we can do to make sure that you don't run into harm? Is there anything you would like us to look at? The intelligence services played that role. Not tactical military intelligence collection; [the military] did that themselves. But [we worked on] reports, for example, that the Iranians had a secret training camp in Bosnia. A team spent four days hiding, going through the woods, to check that out, but they weren't soldiers in uniform. One of the goals that General Shinseki[7] had at the time was to reduce the potential points of conflict by reducing the presence of the soldiers among the civilian population. So the whole point was to keep it as clandestine as possible. I think you can work those things out on the ground fairly easily if you have a willingness on both sides. If you don't, then no matter what they say at the headquarters level or the national [capital] level, then it is never going to work. I do see a complementary role between the two services.

On at least a weekly basis, sometimes more frequently, we asked, "Okay, what do you need?"

MODERATOR: How would you specify that complementary role? Or are you saying that there might be some general principles that explain what those complementary roles are but it really depends more on what needs to be done in the circumstances?

● At the time [in the Balkans], we had people who concentrated on the national strategic objectives and reported on those. Then we had a small group that was assigned to support SFOR in Bosnia and Croatia. That was our job—to support General Shinseki. Other people provided the regular flow of intelligence. My job on the ground was to support his lead, not to go out and do tactical military intelligence collection or anything like that. We didn't do any reporting on the Serbs manipulating their tank parks and moving vehicles around secretly and things like that. The military was covering that. On at least a weekly basis, sometimes more frequently, we asked, "Okay, what do you need?" The commanders would say, "Well, we are going to go and inspect this factory. We believe this factory is producing such and such. Go by beforehand and make sure that we are not going to run into a hostile crowd or we are not being set up for any ambush." So we were doing a role that was complementary to and supportive of their mission.

▼ From my much more limited experience in the intelligence community, [I would say] there aren't clearly delineated roles, per se. At the higher level there are, but [intelligence] is mostly about supporting the customer. Intelligence isn't done in a vacuum. A lot of those things are worked out based on the customer and supporting whatever the customer wants.

▲ The consequence is that it is really messy and redundant and expensive because everybody has different intelligence organizations doing overlapping things. You don't have a lot of coordination to start with, not top-down coordination.

● Right, but I know exactly [what our colleague was talking about before, i.e., intelligence focused on high-value targets]. Many of us within the intelligence community were horribly disappointed by the CTC's [CIA Counterterrorism Center's][8] insistence that they were only going to deal with the top five high-value targets of the week. Many of us saw that as a total perversion of the intelligence process. There is nothing any one of us can do to change that, unfortunately.

◠ We still have to deal with nation-states, but now what can hurt us are small numbers of people, even individuals, who can do a great deal of damage, as [the] 9/11 [attacks] and subsequent attacks have shown. So one of our missions has morphed [from warning] into the notion of preventing—capturing and killing those people who can hurt us—and requirements have changed because of this. When we capture a terrorist, the very first question that people are trained to ask is, Do you know of any operations that are planned that can cause imminent damage to our country, to our allies? That is always the first question. Then you build from there. You jump from that person, going through his pocket litter and the information he has, to go immediately on to his confederates, linking to them right away and, you hope, wrapping them up in a matter of hours before they know that their colleague has been captured. That was an emphasis in Iraq and Afghanistan. It then gets to your question. The intelligence community and intelligence agencies develop certain skills at [finding high-value targets]. And you are asking the question, Is that really the right kind of specialization for the intelligence agencies, as opposed to the military? You laid out some different ways to consider Afghanistan. The environment is so complex because, yes, it is a combat zone, but the enemy that we are dealing with is not a uniformed army and doesn't have the kind of assets and physical infrastructure that armies have, so I think it does very much call for the experience and skills of intelligence agencies as well [as the military] to find, fix, locate those individuals.

One of our missions has morphed [from warning] into the notion of preventing—capturing and killing those people who can hurt us—and requirements have changed because of this.

✕ The problem that has afflicted the U.S. intelligence community, the civilian agencies, and the military is unique to the United States. Seen from the outside, certainly in Iraq and possibly in Afghanistan, a lot of tension arose out of competing interests and competing political interests. Certainly what I have witnessed is a struggle for primacy between the CIA and the DoD [Department of Defense] when it comes to who is going to take the lead on delivering intelligence. That struggle was only possible because of the scale of those two organizations. It was not a struggle, certainly, that existed within the UK community, and in my understanding, working with close allies didn't afflict our other allies. It is a problem that is very specific, I think, to the United States. In Bosnia, Kosovo, Macedonia—these were very different problems from a number of different perspectives, and it was a lot tidier to be able to distinguish who was responsible for doing what. The moment you get to something as complex, as big, as difficult, as intractable, and as messy and as dangerous as Iraq or even Afghanistan, then this neat, tidy division of responsibilities falls away very quickly.

+ Well, I think that is true. It seems to me that what was missing in Afghanistan, for example, was what, I believe, police normally gather just in the course of doing their business walking around the neighborhood—or they should. As far as I could see, neither the foreign intelligence service nor the military—again, this is a U.S. perspective—was able to do that effectively in Afghanistan. I understand the coordination problem, but it also seems to me that there is an element of information or kinds of information that we are not collecting.

What was missing in Afghanistan was what, I believe, police normally gather just in the course of doing their business walking around the neighborhood.

✕ I completely agree with you, but I think you have to go back to the reason behind our deployment to Afghanistan. We deployed to Afghanistan very specifically to destroy al Qaeda. Now to destroy al Qaeda, we had to dismantle the Taliban regime, but the reason we put boots on the ground in the first place was to destroy al Qaeda. It was not to create a new state of Afghanistan. Therefore, when we first deployed to Afghanistan, there was no requirement placed on anyone to go out and understand the communities because that wasn't relevant. So when suddenly it became really important to know and understand the community, we had already been there for many years, and the damage in some sense had already been done. So we are constantly having to play catch-up. Now the requirement is to understand the communities, but I think where General Flynn was both right and unfair was in saying, "Well, we didn't have that information." That is correct, but it is unfair because I don't think anyone was actually tasking anybody to go out and collect that information. So, from a U.S. perspective, you may argue, and I can see the sense of this, that in fact it is the primary responsibility of the military, because of their footprint in the country, to go out and collect that kind of information. But the U.S. military isn't everywhere. So how are they going to get the information they need about what is going on in Helmand before they deploy there? In Kandahar before they deploy there? The areas where the Germans are, the areas where the French are, the areas where all the close allies are? Whose responsibility is it to task those coalition allies to go and collect intelligence, and where does that information then go?

The big difference between operations like Iraq and Afghanistan and the Balkans was that in the Balkans, all we were trying to achieve was peace and stability. Fundamentally different from what we have been trying to do in Iraq and Afghanistan.

The big difference between operations like Iraq and Afghanistan and the Balkans was that in the Balkans, all we were trying to achieve was peace and stability.

MODERATOR: Your comments bring us back to the point [our colleague] made when we first began to talk about requirements. Ultimately, those requirements and what intelligence organizations do depend on what the policymakers say is the mission, or what they say they want to accomplish.

Let me add one thing about policing and intelligence. Cultural intelligence, or understanding the community, means tracking information [on activity] that is not inherently or necessarily illegal or wrong. When the U.S. intelligence community does that in Afghanistan or Iran or North Korea, Americans would say, "Sure, let's do that." When we do it domestically, that is a problem. So that is

An Afghan Border Police officer searches a man for contraband in Bets Kalay village, Kandahar province, Afghanistan.

where it may or may not be law enforcement's role; we are still trying to figure that out.

▲ Yes, you are exactly right. I am a recovering cop, so I will tell you that you just don't do that stuff in the United States. It is exactly when you start keeping track of it in some database that it becomes a problem.

▼ [In my country] as well, that is a problem. In one of our provinces, they tried to make a database. It was struck down [by the court], a big embarrassment for the government and everyone. Putting it in a database, that is the problem. But there is a need for that database because that helps you do [your job]. I don't know how we will do that.

◆ So the situation is difficult in your country. In Europe—in Britain, Germany, Holland, France—most of the domestic intelligence organizations are not police.

+ But there is an advantage to that approach because the police function is separate from the intelligence function. Normal policing is understood as a coercive force to prevent crime, and that is separated from the information collection function, so [intelligence collecting] is not as threatening.

The best strategy engages not just the police but also all of those other governmental institutions that come into daily contact with the communities.

✕ Let me say again that, in my view, based on our experience in the United Kingdom, the best strategy engages not just the police but also all of those other governmental institutions that come into daily contact with the communities. I mean teachers, health providers, etc., in the hope that, with everybody engaged in this information-gathering enterprise, a much better understanding of those communities will be developed, and potentially people who are becoming radicalized or have become radicalized will be identified much more quickly. But if you go to Afghanistan, then none of that [community] infrastructure exists there. The question, then, is, who should collect it? Well, that goes back to who has got the most boots on the ground, who is going to have the best ability to collect it, and that almost certainly is the military. But then the other people who are engaged [overseas] with those communities must not be forgotten. Their information needs to be collected and become part of the intelligence product. ❖

NOTES

[1] A "lone wolf" terrorist is someone who acts alone, without belonging to or taking orders directly from a larger organization.

[2] Omar Abdel Rahman, an Egyptian Muslim cleric (born in 1938) who came to the United States, was convicted of seditious conspiracy for terrorist plotting and is serving a life prison sentence.

[3] The exclamation *crikey* is apparently of Australian origin.

[4] Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, D.C.: Center for a New American Security, 2010): http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf

[5] Flynn, Pottinger, and Batchelor, *Fixing Intel.*

[6] Direction Générale de la Sécurité Extérieure, or General Directorate for External Security.

[7] General Eric Shinseki, U.S. Army, served as commander of SFOR from 1997 to 1998.

[8] The CTC is an office in the CIA that integrates collection and analysis, including the information provided by other intelligence and operational agencies, which send staff members to work at the CTC. In addition to analysis, the CTC directs operations. Established in the 1980s, the CTC is often cited as an example of effective interagency cooperation. For this reason, the Intelligence Reform and Terrorism Prevention Act of 2004 established a National Counterterrorism Center as part of the Office of the Director of National Intelligence.

Tags, Tweets, and Tethers

Dr. Dorothy E. Denning,
U.S. Naval Postgraduate School

Introduction[1]

On 29 January 2007, I opened my e-mail to discover that a colleague and friend, Jim Gray, was feared to be lost at sea. A noted computer scientist and Turing Award[2] winner, Gray had failed to return the day before from a solo trip aboard his 40-foot sailboat *Tenacious* to the Farallon Islands, which lie about 27 miles off the coast of San Francisco. Over the next several days, I observed a massive search effort spring into action. Not only did the U.S. Coast Guard search 40,000 square miles, but a large social network also emerged to assist in the effort. Sadly, Gray was never found, but the scale and energy put into the search itself was inspiring.

Since then, I have observed three other large-scale search operations, although none with life and death consequences. Indeed, all three were contests that offered prizes to the winners. The first of these, the Vanish competition, took place in 2009 with the goal of finding a person who intentionally tried to disappear under a new identity. The second, the Red Balloon Challenge, took place later that year with the objective of finding 10 red balloons that had been tethered to unspecified locations across the United States. Finally, the third, the Tag Challenge, took place in 2011 with the goal of finding five individuals in five cities of the world.

In all four of these cases, social networks emerged to assist with the search, leveraging communications and information technologies, especially social media, to mobilize, organize, coordinate, and share information. They are instances of what is sometimes called crowdsourcing, where a large network of people collectively performs some operation. The searches, especially the Gray search, also illustrate the concept of a "hastily formed network," where a network of people is established rapidly from different communities and works together in a shared conversation space in order to plan and execute an urgent mission.[3] Social media can provide the shared conversation space.

In all four of these cases, social networks emerged to assist with the search, leveraging communications and information technologies, especially social media.

I take a broad view of social media, including not only media such as Facebook and Twitter that explicitly keep track of social connections like "friend" and "follower," but also the group use of communication media such as e-mail, chat, and blogs. Indeed, many social networks are organized around e-mail distribution lists and chat channels.

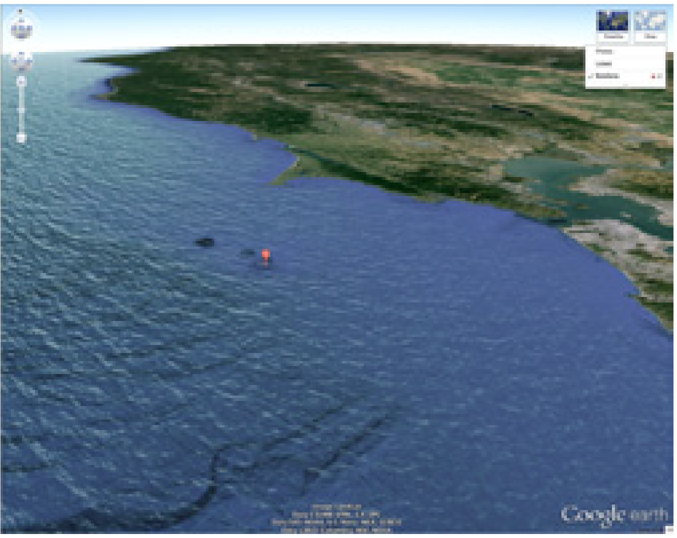
Cases of Large-Scale Search Operations

In this section, I briefly describe each of the four search operations and then draw on them to explore the role of social media in a large-scale search operation. I examine three areas where social media can contribute to a search: mobilization of persons and resources, data collection and dissemination, and verification of acquired data. For each of these areas, I offer principles for how social media and other technologies and strategies can facilitate large-scale search operations, using the four cases to illustrate.

The Search for Jim Gray

Although Gray was never found, the search operation showed how a social network could self-organize and deploy massive resources to aid the effort.

When news of Jim Gray's disappearance began to spread on 29 January 2007, a massive social network of colleagues and friends in different disciplines and industries emerged, offering funds, resources, and expertise to aid the effort. Eventually, the effort centered on acquiring and analyzing images from satellite and aerial sources, with most of the imagery coming from Digital Globe's QuickBird satellite.[4]



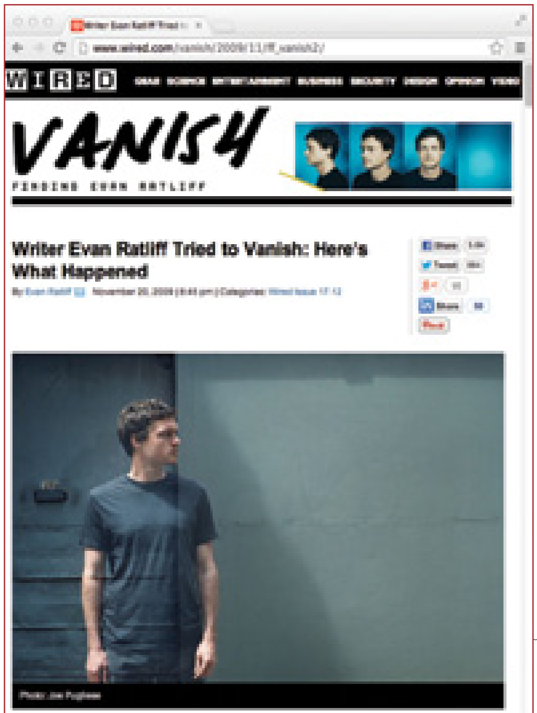
Google map of the Farallons

At the time of Gray's disappearance, Facebook had a modest 20 million users, and Twitter was less than two years old. Thus, it is not surprising that neither played a prominent role in the search. Instead, a core group of volunteers organized and coordinated their efforts through a "Friends of Jim" e-mail list and a blog called *Tenacious Search*, named after Gray's sloop. Although Gray was never found, the search operation showed how a social network could self-organize and deploy massive resources to aid the effort.[5]

Vanish Contest

The Vanish contest began on 15 August 2009, when *Wired* Magazine announced a $5,000 prize to anyone who could find author Evan Ratliff, say the password "fluke," and take his picture—all within 30 days. In cahoots with the magazine, Ratliff had vanished from his home in Northern California armed with business cards showing a fake identity, James Donald Gatz. His objective was not to go into isolation or even off the grid, but rather to see what it would be like to disappear for a month and assume a new identity.[6]

In addition to using a fake identity both online and off, Ratliff used prepaid phone cards, gift cards (paid for with cash), and cash to fund himself while in hiding. He concealed his presence on the internet by using free accounts set up with the fake identity, connecting through a computer that he set up in Las Vegas, and using the anonymity tool Tor to further obfuscate his location. But he took some risks, occasionally using his real ATM card and credit cards, or connecting directly to a website. As agreed, whenever he used his real identity,



Writer Evan Ratliff Tried to Vanish: Here's What Happened

By Evan Ratliff | November 20, 2009 | 8:45 pm | Categories: Wired Issue 17.12

Wired's editor posted the transaction information online, presumably to provide enough clues to keep searchers interested in the hunt. Had Ratliff not taken these risks, he might not have been found before the deadline. As it was, Ratliff was found in New Orleans on 8 September, a week before the clock ran out.[7]

Red Balloon Challenge

On 5 December 2009, the Defense Advanced Research Projects Agency (DARPA) ran the DARPA Network Challenge, offering a $40,000 prize to the first person to report the correct locations of 10 tethered eight-foot red balloons that had been scattered throughout the United States. The challenge was announced on 29 October during a celebration of both the 40th anniversary of the internet and the first remote login to ARPANET, giving potential contestants over one month to prepare.[8]

Although the task was considered intractable by conventional intelligence methods, an approach built around social networking seemed promising.

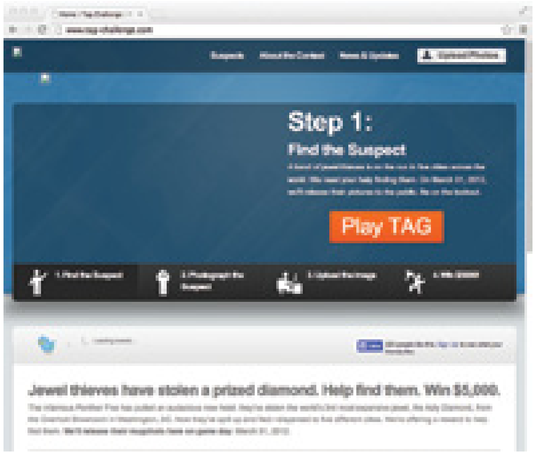
The challenge was set up as an experiment in social network mobilization. DARPA wanted to "identify distributed mobilization strategies and demonstrate how quickly a challenging geolocation problem could be solved by crowdsourcing."[9] Although the task was considered intractable by conventional intelligence methods, an approach built around social networking seemed promising. This was confirmed when a team from the Massachusetts Institute of Technology's Media Lab successfully mobilized a cross-country social network and reported the correct locations of all 10 balloons in eight hours and 52 minutes.[10]

Balloon 1, Union Square, San Francisco

A team from Mercyhurst College's Department of Intelligence Studies approached the challenge from an intelligence analyst's perspective, applying the concept of intelligence preparation of the battlefield (IPB) to predict where the balloons might be located. They mapped the locations of all DARPA-funded sites, expecting the balloons to be nearby. Their strategy also included identifying lesser-known networks they could tap into, such as law enforcement intelligence analysts and interstate truckers. However, they started late and did not correctly report any balloons.[11]

Tag Challenge

Sponsored by the U.S. State Department, the Tag Challenge took place on 31 March 2012, with the goal of determining "whether and how social media can be used to accomplish a realistic, time-sensitive, international law enforcement goal."[12] Specifically, contestants had to locate and photograph five "suspects" in five different cities of the world: Washington, D.C.; New York; London; Stockholm; and Bratislava, Slovakia. The suspects were described as jewel thieves who had "stolen a prized diamond" but were actually volunteers who had been instructed to follow a 12-hour itinerary designed to look like a normal day. The contest offered a prize of $5,000 to the first person who submitted verifiable pictures of the suspects within the allotted 12 hours for



Jewel thieves have stolen a prized diamond. Help find them. Win $5,000.

each city. Although the contest was announced two months in advance, officials waited until the day of the contest to post "mug shots" of the suspects, all wearing colorful T-shirts with the competition logo.[13]

Like the Red Balloon Challenge, the Tag Challenge tested the role of social networks and social media in a large-scale search operation. It was more difficult than its predecessor, however, spanning two continents and employing mobile targets that would be more difficult to spot than large red balloons. No team found all five suspects, but the team CrowdScanner, whose members came from five universities in the United States, United Kingdom, United Arab Emirates, and Australia, found the three suspects in Washington, New York, and Bratislava. None of the team's members resided in the target cities, but at least one had been part of the winning MIT Media Lab team in the balloon challenge.[14]

Social Network and Media Roles

This next part of the discussion turns to the role of social media in the mobilization of a large-scale search effort, in the dissemination and collection of information, and in the verification of acquired data.

Mobilization

In all four operations, social media played a key role in mobilization. However, the most successful efforts also benefited from the use of mass media, and two of these from the application of a recursive incentive structure as well. The following discussion elaborates on these findings.

In all four operations, social media played a key role in mobilization. However, the most successful efforts also benefited from the use of mass media.

Social Media Can Enhance Mobilization

Social media offer two advantages for mobilization. First, they encode existing social networks through such constructs as friends, followers, group memberships, and distribution lists, making it easy to spread information through these networks. Second, the technology facilitates the formation of new networks and the growth of existing ones.

All four operations made extensive use of social media to recruit participants in their search efforts, although the technologies they used varied somewhat. The search for Jim Gray, for example, was mobilized initially through various e-mail discussions among Gray's colleagues and friends. Recognizing the need to provide a central means of communication and coordination for everyone involved, the group set up the *Tenacious Search* blog. At first, the blog had open authorship

rights, acting as a public forum and bulletin board. After the blog attracted a large audience, however, these rights were restricted to a smaller group, while the core group of volunteers moved to a "Friends of Jim" e-mail distribution list to coordinate their search efforts. At the same time, the blog continued to support mobilization, with the blog administrator serving as a point of contact for outside persons offering tips and skills to aid the search. When the search was over, team leaders noted how "modern networked technologies enabled a group of acquaintances and strangers to quickly self-organize, coordinate, build complex working systems, and attack problems in a data-driven manner." They also recognized that "the process of coordinating diverse volunteer skills in an emerging crisis was quite difficult, and that there is significant room for improvement over standard email and blogging tools."[15]

By the time of the other three search operations, both Twitter and Facebook were more popular, and both played a role in mobilization. In the Vanish contest, the Twitter hashtag #vanish drew 600 posts a day, while the "Search for Evan Ratliff" Facebook group attracted over 1,000 members.[16] In the Red Balloon Challenge, hacker George Hotz found eight balloons, in part by leveraging his existing Twitter network of almost 50,000 followers. Another team, Nerdfighters, tapped into its network of 5,000 followers of the Brotherhood 2.0 vlog (video blog) and created a video that went viral. Several teams used Facebook's friends structure to recruit, the result being that Facebook alone brought more referrals to the official challenge website than any of the search engines, including Google.[17] The Mercyhurst team set up a Facebook group that grew to 447 members within 24 hours.[18]

In the Vanish contest, the Twitter hashtag #vanish drew 600 posts a day, while the "Search for Evan Ratliff" Facebook group attracted over 1,000 members.

Twitter and Facebook were used in the Tag Challenge as well, with the winning team creating a Twitter account and Facebook page that people could follow and like, respectively. The team thought, however, that Twitter and Facebook might have played a larger role in increasing the credibility of the teams than in actual recruitment. One team tried, but failed, to create a bandwagon effect by creating a large number of fake Twitter followers.[19]

Social Media Should Be Augmented with Mass Media

All of the operations seemed to benefit from mass media exposure. This was especially apparent in the Red Balloon Challenge, where the top two teams garnered far greater media exposure than the other teams. The winning MIT Media Lab team made *CNN Headline News* on the day of the contest, while the Georgia Tech Research Institute team, which came in second with nine balloons, leveraged mass media coverage before the event. That coverage also helped to boost the search engine ranking for their team's website. In addition, both the MIT and Georgia Tech teams enjoyed the national name recognition that came with their schools, which may have contributed to their ability to recruit volunteers to work on their behalf.[20]

In its project report, DARPA observed that "mass media was more predictable than viral transmission for the diffusion of the [challenge]."

In its project report, DARPA observed that "mass media was more predictable than viral transmission for the diffusion of the [challenge]." It noted that diffusion eventually proceeded virally, but that "the inflection was not until the final days before the balloon launch and it followed the extensive media coverage of the final week."[21]

In the Tag Challenge, the winning CrowdScanner team also leveraged mass media and tried to generate attention on blogs and news sites. It was mentioned on CNET and ZDNet, as well as by its representative universities' press teams. Organizers noted that most of their competitors focused purely on social media, and on Twitter in particular. They observed that this narrower strategy was insufficient and led some searchers to be perceived as spammers.[22]

Although not usually considered either "social media" or "mass media," public websites, which serve primarily as means of disseminating information, also played a role in the Red Balloon Challenge and the Tag Challenge, and were used by the winning teams. Nevertheless, they too appeared insufficient by themselves as a means of mobilization. The Spot Big Red team in the balloon challenge, for example, went so far as to purchase the word "challenge" from Google, so that anyone searching for the word would see a click-through ad linking to their team website. But they had no external media coverage and drew few recruits.[23]

The Harvard Business School team found no balloons, apparently because they spent too much effort on marketing rather than execution.

Of course, overall strategy also mattered. In the Red Balloon Challenge, a team from the Harvard Business School claimed almost two million "impressions," which included e-mails to their vast network of alumni, tweets and alumni re-tweets, and an ABCNews.com story featuring their team. Still, the team found no balloons, apparently because they spent too much effort on marketing rather than execution.[24]

Recursive Incentive Strategies Show Promise

The winning teams in the Red Balloon Challenge and Tag Challenge both used a recursive incentive structure to entice volunteers to work with their teams. In the Red Balloon Challenge, the $40,000 prize money was allocated in such a way that anyone who either found a balloon or was on the referral chain to the finder would be rewarded. Specifically, each balloon was worth $4,000, with the money partitioned as follows: the finder would receive $2,000, their referrer $1,000, the referrer's referrer $500, and so on, for the length of the chain. Any remaining moneys would go to charity.[25] To support their reward structure, new recruits were given an individualized referral link that they could share on social networks.[26]

A slightly different strategy was used in the Tag Challenge, but it too was designed to reward recruiters as well as finders. Here, $1,000 was allocated for each of the five suspects, with $500 for the finder and $100 for the referrer. In addition, recruiters were to receive $1 for each of the first 2,000 recruits.[27]

The second-placed Georgia Tech team said that many balloon spotters chose that team because of its plan to donate the winnings to the American Red Cross.

Although we cannot say with certainty that the recursive incentive strategy contributed to the success of the winning teams, it may have been a factor in the teams' attracting mass media publicity and then recruits. However, other teams that did not offer any direct monetary incentives at all also did well. The second-placed Georgia Tech team in the Red Balloon Challenge said that many balloon spotters chose that team because of its plan to donate the winnings to the American Red Cross.[28]

Collection and Dissemination of Information

This section describes the ways in which social media can be used both as a means of disseminating information and as a source of new information.

Social Media Can Facilitate Information Dissemination

Twitter has become a popular medium for live reporting of events, often with links to accompanying photos and videos. This use was evident in the Red Balloon Challenge, where several balloon sightings were reported on Twitter. George Hotz was able to locate four balloons just from reports on his Twitter network.

Twitter also played a prominent role in the Vanish contest, with users of the #vanish hashtag using the medium to share clues and theories. However, one frequent poster, a 16-year-old high school student named Jonathan Mäkelä, thought the conversation on Twitter was too public, because it enabled the hunted also to know what was going on. Mäkelä suggested that groups needed to go private to win; he then set up a private, password-controlled chat room for those he was sure were not Ratliff. Jeff Reifman, a former Microsoft group program manager, developed a Facebook app called Vanish Team for information and discussions about Ratliff, but most of the intelligence swap took place on Twitter or in Mäkelä's chat room.[29]

In the Tag Challenge, the winning team posted its early successes on social media. Team members also built a mobile phone app that allowed people to see photos of the suspects and submit pictures of them if they were spotted. The team found, however, that those who actually spotted the suspects submitted their photos directly through e-mail.[30]

Social Media Can Be a Source for Intelligence Data

Because so much information is disseminated through social media, the media themselves provide a source for raw intelligence data. Again, this was apparent in the contests. In the Red Balloon

Challenge, for example, the iSchools team, representing a consortium of five schools, mined publicly accessible internet sites, including Twitter feeds and competitor sites, for published reports of sightings. They found five balloons this way, but only one by drawing on their own social network.[31]

Because so much information is disseminated through social media, the media themselves provide a source for raw intelligence data.

In the Vanish competition, Jeff Reifman combed through visitors to his Vanish team, thinking (correctly) that Ratliff might be among them. This led him to the profile for a James Donald Gatz and the "jdgatz" Facebook account that Ratliff had set up with his fake identity. Reifman then found three friends of Gatz, who were willing to keep him apprised of Gatz's private posts. After Gatz made his @jdgatz Twitter feed public, Reifman also started following it. Meanwhile, Mäkelä had triangulated Ratliff's IP address to New Orleans. Once Reifman saw that @jdgatz was following three New Orleans businesses on Twitter, he looked up one, Naked Pizza, on the Web and sent off an e-mail asking for help. Naked Pizza cofounder Jeff Leach agreed and was the person to say the password "fluke" when he spotted Ratliff outside a local bookstore.[32]

Verification

In any intelligence operation, it is important to know whether acquired data is accurate. Collectors can make mistakes, and adversaries can intentionally inject bogus data. Here I discuss two ways in which social media can contribute to data verification: first, through technologies associated with social media, and second, through crowdsourced verification.

Social Media–related Technologies Can Aid Verification

Some of the technologies used with social media can facilitate verification. Tweets from cell phones can reveal the geo-locations of the phones, as can photos taken by cell phones and tagged with location coordinates. In addition, IP addresses can be mapped to at least proximate geo-locations. All of these location-based technologies can be used to verify whether claimed locations match actual locations. For example, if someone tweets that they just found a balloon in Denver and includes a link to a picture taken with their cell phone, verifiers can compare the reported location against that supplied with the tweet or the photo if that information is available.

In the Red Balloon Challenge, the MIT Media Lab team received more than 200 submissions, only 30 to 40 of which proved accurate.

In the Red Balloon Challenge, the MIT Media Lab team received more than 200 submissions, only 30 to 40 of which proved accurate. To weed out the false reports, humans reviewed the submissions. They found one bogus report where the reported location, Florida, did not match the location of the IP address associated with the submission, Los Angeles. They also found multiple bogus submissions reporting exactly the same geo-coordinates. These reports contrasted with the multiple submissions they received for actual sightings, where the reported coordinates varied slightly, owing to the spotters' being in somewhat different positions and small errors in location sensors. In addition, the photos submitted with bogus submissions tended to be fuzzier and lacked the DARPA banner. The iSchools team, which found five balloons on Twitter and other public media, gave a higher reliability assessment to tweets from established users with geo-tagged photos than to those from new accounts without followers.[33] The Mercyhurst team used their IPB analysis to rank order reported sightings, giving priority to ones in areas where they expected the balloons to be deployed. For those they decided to investigate further, they used Google Earth to identify local restaurants and stores they could call for verification.[34]

Verification Can Be Crowdsourced through Social Media

Social media can provide an efficient means for crowdsourcing the verification process. In the Red Balloon Challenge, the Nerdfighters team compiled a cell phone and address list for 2,000 persons they could dispatch for balloon verification through targeted text messages. Their entire operation was coordinated by 10 individuals using Skype. Groundspeak Geocachers drew on their network of hundreds of thousands of members to effectively dispatch verifiers, and correctly reported seven of the balloons.[35] The iSchools team dispatched verifiers from a list of pre-recruited observers, as well as people from their schools, family, and friends in the vicinities of the reported locations.[36]

The Nerdfighters team compiled a cell phone and address list for 2,000 persons they could dispatch for balloon verification through targeted text messages.

The search for Jim Gray involved farming out satellite image tiles to human analysts in order to determine areas where Gray might be found. Initially, the team used Amazon Mechanical Turk to crowdsource the review process, but eventually turned to expert analysts, who were faster and more accurate than the novices tasked by Mechanical Turk. A cluster of these analysts were colocated at The Johns Hopkins University, allowing them to collaborate and coordinate their review. Promising images were then sent to experts in marine imagery in order to determine areas worthy of dispatching people for a close-up search.[37]

Conclusions

The four search operations described here demonstrate how social media and related technologies can facilitate a large-scale search for persons and things. They can aid the processes of mobilization, information collection and sharing, and verification of data acquired, as well as communication and coordination in general. However, the search operations also drew upon other technologies, including image processing, data mining, and geo-location and mapping technologies. In addition, they made use of on-site human intelligence; in all three contests, human spotters took photos and reported or verified sightings.

Although social media can in principle support large, distributed networks lacking any centralized command and control, all four of the operations described here were led by individuals and small teams of people who debated and developed strategy, initiated actions, and coordinated contributions to the search effort. At least in these cases, the media alone were insufficient without imposing some form of organizational structure on the network, even if that structure was self-organized.

At least in these cases, the media alone were insufficient without imposing some form of organizational structure on the network, even if that structure was self-organized.

The four search operations also demonstrate that many other factors can affect the success of a search effort, including the use of mass media, name recognition, incentives, and, of course, the nature of the search to begin with. Some persons, such as Jim Gray, may never be found, and actual fugitives and intelligence targets may work much harder to hide than did Ratliff in the Vanish contest and the volunteer suspects in the Tag Challenge. Social media are not a panacea, but neither should they be overlooked or discounted.

At least one company, Crowdfynd, has been formed to exploit social media technologies to help people locate missing items. Its mobile and Web-based application leverages the power of crowdsourcing to report crimes as well as found items, and to search for missing items by location and a photo display of found items.[38] It will be interesting to see whether Crowdfynd catches on, and what else might emerge to support large-scale searches. ❖

ABOUT THE AUTHOR

Dr. Dorothy E. Denning is a Distinguished Professor in the Department of Defense Analysis at the U.S. Naval Postgraduate School.

NOTES

[1] The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government.

[2] The A.M. Turing Award is given annually by the Association for Computing Machinery to individuals who make a substantial and lasting technical contribution to the field of computing. Gray received the prize in 1998.

[3] Peter J. Denning, “Hastily Formed Networks,” *Communications of the ACM* 49, no. 4 (April 2006): 15–20: http://denninginstitute.com/pjd/PUBS/CACMcols/cacmApr06.pdf

[4] Joseph M. Hellerstein and David L. Tennenhouse, “Searching for Jim Gray: A Technical Overview,” *Communications of the ACM* 54, no. 7 (July 2011): 77–87.

[5] Ibid.

[6] Evan Ratliff, “Writer Evan Ratliff Tried to Vanish: Here’s What Happened,” *Wired* 17, no. 12 (2009): http://www.wired.com/vanish/2009/11/ff_vanish2/

[7] Ibid.

[8] ARPANET, the Advanced Research Projects Agency Network, was the original form of the internet created by the U.S. Defense Department and several universities. Defense Advanced Research Projects Agency (DARPA), “DARPA Network Challenge, Project Report,” Arlington, Va., 16 February 2010, 2: http://www.eecs.harvard.edu/cs286r/courses/fall10/papers/ProjectReport.pdf

[9] Ibid.

[10] Ibid., 9.

[11] Kristan J. Wheaton, “Lessons Learned: DARPA Balloon Challenge,” *Sources and Methods* (blog), 6 December 2009: http://sourcesandmethods.blogspot.com/2009/12/lessons-learned-darpa-balloon-challenge.html

[12] See the TAG Challenge website: http://www.tag-challenge.com/

[13] Ibid.

[14] Iyad Rahwan et al., “Global Manhunt Pushes the Limits of Social Mobilization,” *Computer* 46, no. 4 (2013): 68–75.

[15] Both quotes come from Hellerstein and Tennenhouse, “Searching for Jim Gray,” 87.

[16] Ratliff, “Writer Evan Ratliff Tried to Vanish.”

[17] DARPA, “DARPA Network Challenge,” 13.

[18] Wheaton, “Lessons Learned.”

[19] Rahwan et al., “Global Manhunt Pushes the Limits.”

[20] DARPA, “DARPA Network Challenge,” 13.

[21] Both quotes come from ibid.

[22] Rahwan et al., “Global Manhunt Pushes the Limits.”

[23] DARPA, “DARPA Network Challenge,” 12.

[24] Ibid.

[25] Ibid., 10–11.

[26] “U.S. Government Sponsors High-Stakes Balloon Hunt,” NPR, 11 December 2009: http://www.npr.org/programs/talk-of-the-nation/2009/12/11/121343437/

[27] Rahwan et al., “Global Manhunt Pushes the Limits.”

[28] “I Spy a Red Balloon: Georgia Tech Team Wins Key Insights—and a Second-Place Finish—in DARPA Network Challenge,” Georgia Tech Research Institute, n.d.: http://www.gtri.gatech.edu/casestudy/red-balloon-darpa-challenge

[29] Ratliff, “Writer Evan Ratliff Tried to Vanish.”

[30] Rahwan et al., “Global Manhunt Pushes the Limits.”

[31] John C. Tang et al., “Reflecting on the DARPA Red Balloon Challenge,” *Communications of the ACM* 54, no. 4 (April 2011): 78–85.

[32] Ratliff, “Writer Evan Ratliff Tried to Vanish.”

[33] Tang et al., “Reflecting.”

[34] Wheaton, “Lessons Learned.”

[35] DARPA, “DARPA Network Challenge,”10, 17.

[36] Tang et al., “Reflecting.”

[37] Hellerstein and Tennenhouse, “Searching for Jim Gray.”

[38] See the Crowdfynd website: https://www.crowdfynd.com/

The Relevance of Technology in the Fight against India's Maoist Insurgency

D. M. "John" Mitra, National Crime Records Bureau, India

Large areas of central India have come under the cloud of a violent struggle between government forces and Maoist insurgents. The Maoists are active in at least nine out of the 28 states of India, and are trying to spread their influence into many more states.[1] About 5,772 civilians and 2,065 members of the security forces were killed by the Maoists between 2001 and 2012. A majority of the civilians who have died in the violence were local tribal members, killed by insurgents who were enforcing Maoist hegemony over contested areas.[2]

Law and order are dealt with at the state level in India's federal structure; the national government plays primarily a supporting role in terms of providing men, matériel, and coordination to the states in their fight against the Maoists. Because the Maoist insurgency so far has been a purely indigenous, mostly localized phenomenon, each state has developed its own approach to tackling Maoist violence according to that state government's own experience and political context. In the same way, the insurgency in each state has its unique flavor, composition, and history, and uses the state-specific theater of violence to its advantage. A local group is able to start, escalate, de-escalate, or change strategy in one theater, independent of what is happening in other theaters. It can use one state as a sanctuary while waging guerrilla war in the neighboring state. Groups are also able to transfer men, matériel, and funds between the theaters according to changing needs, and to apply the experience they gained in one theater to improve their operations in other areas.

The Maoist insurgency in each state has its unique flavor, composition, and history.

Against this background, this article discusses the importance of inaccessible forested areas as initial niches for the proto-insurgencies to grow in less developed former colonies such as India. As their subsequent conduct has shown, the Maoists seem to have learned from early strategic failures in the state of Andhra Pradesh the value of sticking to inaccessible areas, even as their insurgency has matured. The article also addresses the relevance of technology, or rather the lack thereof, for counterinsurgency in these inaccessible areas.

Characteristics of India's Maoist Insurgency

The communist political movement in India has grown into many branches since it first emerged in 1920. After the Communist Party of India (CPI) began to take part in electoral democracy in 1951, some of the CPI's more radical elements broke away from the CPI in 1964 to form the CPI (Marxist). When the leadership of the CPI (Marxist) also embraced electoral politics, the more radical Maoist factions within CPI (Marxist), inspired by Mao Zedong's takeover of China, broke away to start violent uprisings in the countryside. Although these revolutionary groups have repeatedly fragmented, with some of them opting out of violent revolution to become involved in other activities such as urban trade unionism, several groups have stayed with the violent revolutionary path in remote rural areas of India. As the Indian state grew in

As the Indian state grew in strength, the Maoists were forced from the rural interior regions where they began into less accessible forested and mountainous areas.

strength and its reach extended further into the countryside, the Maoists were forced from the rural interior regions where they began into less accessible forested and mountainous areas.

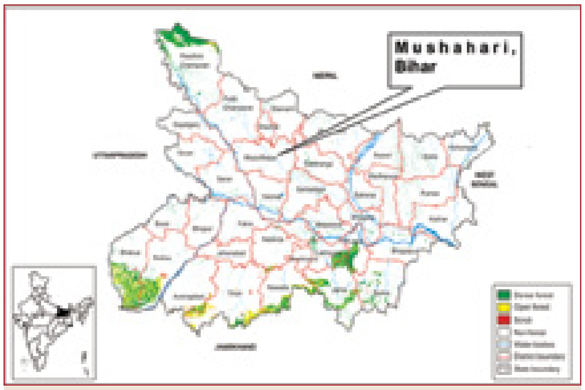
According to the U.S. government's *Guide to the Analysis of Insurgency 2012*,

> Insurgency is a protracted political-military struggle directed toward subverting or displacing the legitimacy of a constituted government or occupying power and completely or partially controlling the resources of a territory through the use of irregular military forces and illegal political organizations. The common denominator for most insurgent groups is their objective of gaining control of a population or a particular territory, including its resources. This objective differentiates insurgent groups from purely terrorist organizations.[3]

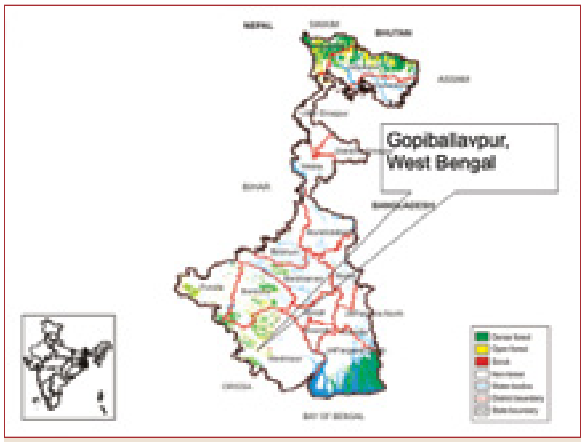
India's Maoists perfectly fit this definition of an insurgent group. This is not to say that the Maoists have not or will not resort to terrorism, given that "most insurgent groups use terrorism as a tactic in pursuit of their goal" at different stages of their growth.[4] The distinction between an insurgency and a purely terrorist organization, however, is important for understanding the way in which the Indian Maoist movement has grown since its beginning. The Maoists started as a proto-insurgency, like the majority of insurgent movements, in the rural hamlets that were most conducive for their survival, and established their dominance over those areas through armed violence.[5] The insurgents gradually expanded the territory under their control, with the ultimate objective to dismantle the local government, take over the entire target area, and bring it under some form of communist rule.

The insurgents try to impress the local population with their military power, often by wearing combat uniforms.

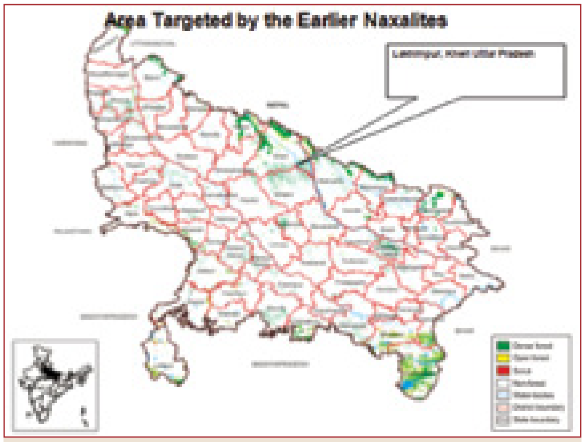
Within the areas they dominate and during armed operations, the insurgents try to impress the local population with their military power, often by wearing combat uniforms. This is unlike terrorists, who do not normally wear distinctive clothes but try to hide their identity and blend in with the local population around their hideouts. A terrorist organization usually starts with a small number of members dotted throughout a geographically large portion of the target area and tries gradually to increase its membership and activities through social contacts, media, and networking. Its terrorist activities may spread far beyond its locality and the target population. Instead of trying to establish and gradually expand its control over limited areas, a terrorist group often indulges in terrorist acts at random across the length and breadth of the target country, in order to weaken and destabilize the central or regional government and shake public confidence in the government's ability to protect its citizens. Terrorist groups grow by increasing their membership and affiliates, and by increasing the intensity and frequency of their acts. The growth and expansion of the Maoists, like most insurgent organizations, can be compared to that of cancer, which takes over an area and then gradually metastasizes in pockets, while the growth of terrorism within the borders of a state can be compared to a virus, which spreads more or less evenly throughout the body. Some insurgent organizations, however, such as the Liberation Tigers of Tamil Eelam in Sri Lanka, have followed both of these models. Maps 1 through 4 illustrate early Naxalite[6] expansion in India.



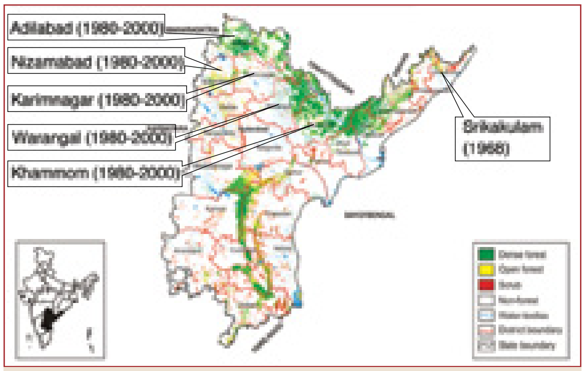
Map 1: Earlier Naxalite area of operation in Bihar



Map 2: Earlier Naxalite area of operation in West Bengal


Area Targeted by the Earlier Naxalites
Lakhimpur, Kheri Uttar Pradesh
NEPAL
MADHYA PRADESH

Map 3: Earlier Naxalite area of operation in Uttar Pradesh



Map 4: Areas of operation of Naxalites and Maoists in Andhra Pradesh

Choice of a Niche Area for the Maoists

There are many reasons why the Maoists have been forced to shift their violent operations from the rural interiors of states to more remote forested areas, as shown in maps 1 through 4. The chief reason, of course, is that the Maoists have adopted "protracted war" against the lawfully established state as their main form of revolution. This is not the case with most of the other Communist parties in India, which have adopted political mobilization as their main strategy and are active in mainstream liberal democratic politics. The preponderance of left-wing extremist violence in India is perpetrated by the Maoists, who are fugitives in the eyes of the law. The need to protect their fledgling organization from annihilation by government security forces forced the insurgents to establish themselves in inaccessible areas where state power was the weakest. After the Chinese Communist insurgency's initial setbacks in China's urban areas, in 1927 even Mao Zedong's forces famously had to take shelter in the Jinggang mountains of Jiangxi Province. As Argentine revolutionary Che Guevara prescribed, "At the outset, the essential task of the guerrilla fighter is to keep himself from being destroyed … having taken up inaccessible positions out of reach of the enemy."[7]

Size of the Organization

Guerrilla organizations have often chosen to establish themselves in terrain where small size is not a handicap but rather an advantage.

One of the many asymmetries of the struggle between a nascent insurgent organization and an established state is the difference in relative sizes. A guerrilla organization starts out as a small group and remains much smaller than the state for a long period. Therefore, guerrilla organizations have often, at least in the early stage of their development, chosen to establish themselves in terrain where small size is not a handicap but rather an advantage. Figure 1 illustrates mathematically why forestland well suits guerrillas' requirement for concealment.

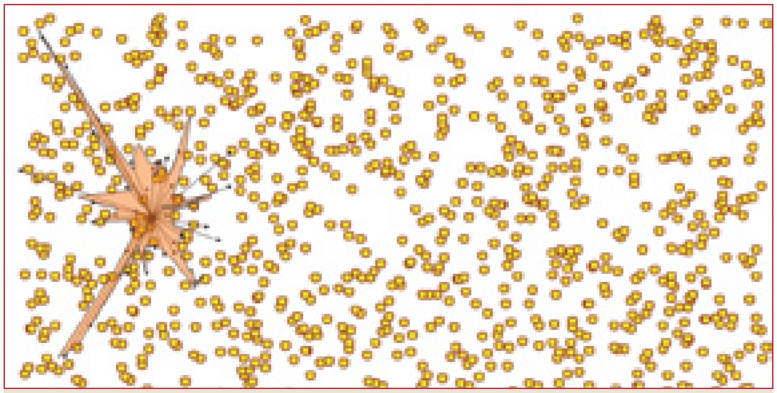


Figure 1: Limitations on line-of-sight visibility in forest areas

"The trees in a natural forest are randomly placed, as is shown in [figure 1]. The circles represent the tree trunks. Suppose a person stands somewhere in a forest, where his or her vision is limited by tree trunks. The areas that the person can see are shown by the spread of the arrows. … It can be mathematically shown that the average visible area from a point is inversely proportional to the square of the density of the trees and the square of the average radius of the trees."[8]

$$A \; \alpha \; \frac{1}{n^2 \, r^2}$$

Figure 2

This is represented by the equation shown in figure 2,

where A = the area in meters,
n = the number of trees per 1 m^2 area, and
r = the average width of the tree trunks in meters.

The optimal size of a group operating in a combat situation in a forest is determined according to the area of visibility, which in turn is determined by the density of the forest.

Thus, on average, only a limited area—which is determined by the density of the forest at any point—can be visible from the viewer's vantage point. Therefore, when a government security party or a guerrilla squad moves in a forest, its capacity to see and detect its enemy is optimal only when all members, except the leader, are spread on the outer limit of the visible area at that point of the forest. On the one hand, if they are spread beyond that limit, the leader of the group will not be able to see all the members of the team, and some of the members will not be able to see the leader. On the other hand, if team members are not spread out to the optimal limit, their combined capacity to see and act will not be at its fullest. Thus, the optimal size of a group operating in a combat situation in a forest is determined according to the area of visibility, which in turn is determined by the density of the forest.[9]

Similarly, it can be shown that the larger the group that is in hiding, the greater its chance of detection by the enemy. Maoists seem to know this intuitively, because most of the Maoist squads are typically small in number, particularly in the areas where they expect intrusion by government forces.

Isolated Population

One major difference between the demography of developed countries and that of less developed former colonies is the fact that about 80 percent of a developed country's population on average lives in urban areas, whereas in less developed former colonies such as India, less than 30 percent of the people live in urban areas.[10] Another difference that often escapes notice is the fact that many less developed former colonies have isolated populations who live in remote, inaccessible areas, and remain essentially disconnected from the mainstream sociopolitical and economic systems of the country in which they are citizens. Developed countries rarely have such isolated populations, and their remote and inaccessible areas are mostly devoid of people (Russian Siberia being one notable exception). The guerrilla's dependence on the local population was emphasized by Mao, who likened the local people to water and guerrillas to fish.[11] If an insurgent organization is to survive and grow, it must have "inputs of recruits, information, shelter and food—almost always obtained from the internal environment [the local population]."[12] So, although a revolutionary needs remote forests and inaccessible areas in which to hide, he also needs some people nearby for his survival and growth. While remote and inaccessible areas are available in developed countries, their lack of population makes such places unsuitable for proto-insurgent organizations to survive and grow. This combination of isolated population and inaccessibility is only available in the less developed former colonies. This is borne out by the fact that out of the 25 insurgencies since 1945 in which the government lost to the insurgents, 19 belonged to those countries whose urbanization was less than 40 percent.[13]

The guerrilla's dependence on the local population was emphasized by Mao, who likened the local people to water and guerrillas to fish.

Of the 25 insurgencies since 1945 in which the government lost to the insurgents, 19 belonged to those countries whose urbanization was less than 40 percent.

Administratively and Politically Bald Areas

It also is often evident that the presence of government progressively lessens as one goes from urban to rural settings, or from densely populated to less populated areas. The strength of the central government's presence in an area is the aggregate of the presence of its agencies in that place. Each agency's presence in an area in turn is a function of population density and the functional necessity of that agency to be in that area. Departments like health services, police, education, and others whose functional necessity relates directly to the needs of local citizens have little or no presence in areas where the population density approaches zero. Many less developed former colonies have isolated populations who live in small hamlets scattered over a large area. In such areas, most of the citizen-centric state agencies are virtually absent. For the same reason, representatives of the state's political parties and of the media and civil society visit these areas only rarely, if at all.

For the insurgents, these politically and administratively bald areas, devoid of any threat or competition from the civil administration and political parties, are the most suitable locations in which to weather their vulnerable initial years.

The Growth of the Maoist Insurgency and Its Terrain

Most of what has previously been discussed applies to an insurgency in its proto stage. As an insurgency grows, it typically tries to expand into areas beyond the initial sanctuary, where the terrain often is quite different. However, the Indian Maoists' areas of operation today still resemble those of their proto stage 35 years ago. The following analysis of their activities in Andhra Pradesh from 1978 until now shows why the Maoists have remained restricted to the deep forests.

The Andhra Experience

In their bid to enforce Maoist hegemony in the contested areas, it is apparent from the data that the insurgents have killed a greater number of civilians than they have security personnel.

As described earlier, the Maoist insurgency in any given Indian state can be treated as an independent theater of armed conflict for the purpose of our analysis. Maoist groups are able to start, escalate, and de-escalate conflict, or even change strategy in their theater, independent of what is happening in other places. They also are able to use one region as a sanctuary while waging guerrilla war in a neighboring theater, and bring to bear the experience they have gained to operate more effectively wherever they find themselves. This section analyzes the Maoists' activities in Andhra Pradesh from 1978 to 2012 and the possible lessons they learned and subsequently utilized in other states. Figure 3 illustrates the levels of violence committed by the Maoists from 1978 to 2012 in Andhra Pradesh, as measured by casualties among security forces and civilians. In their bid to enforce Maoist hegemony in the contested areas, it is apparent from the data that the insurgents have killed a greater number of civilians than they have security personnel.

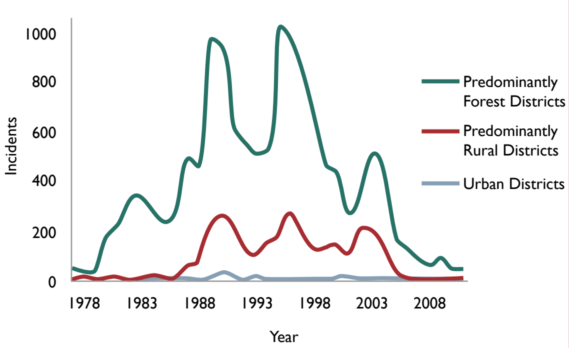


Figure 3: Violence by Maoists in Andhra Pradesh

As figure 3 shows, the proto-insurgency that started in Andhra in 1978 as the People's War Group (PWG) had evolved into a formidable insurgent organization by 1997. The Maoists consistently expanded in size and influence through phases of aggression and retrenchment. Figures 4 and 5 offer a closer look at the period by breaking it into phases between peak years.

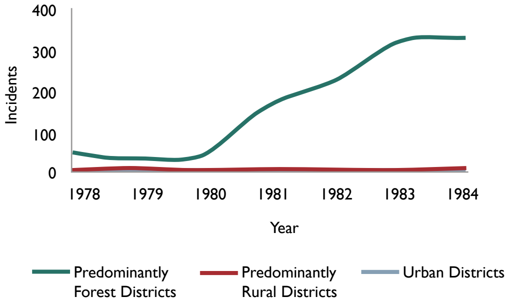


Figure 4: Violence by Maoists in Andhra Pradesh 1978–1984

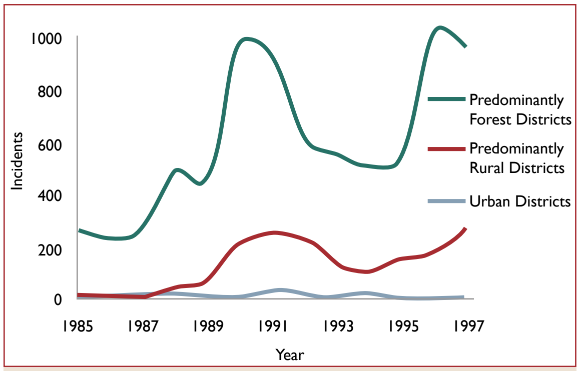


Figure 5: Violence by Maoists in Andhra Pradesh 1985–1997

The Maoists expanded their activities primarily within the forested areas till 1985 (see figures 3 and 4), largely avoiding any public outcry or the attention of the state. They even managed to pass themselves off as friendly neighbors in the remote forested regions, in spite of their violence. In 1982, one top political leader of Andhra Pradesh, N. T. Rama Rao, called the Maoists "patriotic brothers."[14]

As figure 5 shows, the Maoists started rapidly expanding their activities into rural populated areas after 1985. Rao, who had become chief minister of Andhra Pradesh by then, changed his opinion about the Maoists and banned their organization in 1987. He also created a special operations group within the Andhra Pradesh state police called the Greyhounds. This determination to create the Greyhounds and strengthen the police is cited as a reason for the Maoists' murder of Daggubati Chenchuramaiah, the father of one of Rao's sons-in-law, on 6 April 1989.[15] Many of the sustained security operations that more or less flushed the Maoists out of Andhra Pradesh in later years are credited to the Greyhounds. This is not to underestimate the state's concentrated efforts to boost development in the vulnerable areas, but such actions could be undertaken only after the Maoists lost their influence in an area, because the insurgents strongly opposed most of the government's development activities such as building roads and spreading access to education.[16] The steady retreat of the Maoists, first back to the forests and later out of Andhra Pradesh, is shown in figure 6. It is interesting to note that although the Maoists were flushed out of the rural areas by 2007, they are still holding on to the forests, though with less use of violence.

Although the Maoists were flushed out of the rural areas by 2007, they are still holding on to the forests.

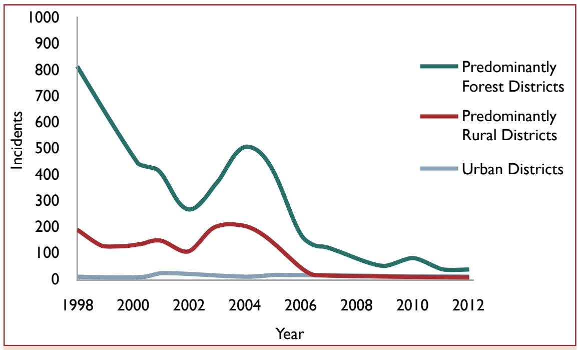


Figure 6: Violence by Maoists in Andhra Pradesh 1998–2012

Lessons Learned by the Maoists from Andhra Pradesh

It seems that the Maoists learned many lessons from their loss in Andhra Pradesh, and accordingly made course corrections. The first lesson apparently is that they must avoid both overestimating the state's weakness and prematurely expanding their operations to rural and urban areas. As political scholar Colin Gray points out, the insurgent wisely uses time as an asset against the state. However, if "[an insurgent] force enjoys military success, its leaders are always vulnerable to the temptation to … seek to accelerate the pace of history by going directly for political gold by means of a swift military victory. As often as not, such hubris brings them close to military and political nemesis."[17] A profile of Maoist violence from 1985 to 1995 illustrates this error of hubris. Since being hounded out of settled rural areas by the police in Andhra Pradesh, the insurgents have been very cautious about expanding again into such areas. The Maoists have generally minimized their activities outside the forests except for some rural areas of Bihar state, where they continue to take advantage of extreme social inequality to win local support.[18] In two experimental expansions, Maoists managed to move into settled areas close to the forest in Narayanpatna in the state of Odisha and Lalgarh in the state of West Bengal. The experiments ultimately failed because the states were able to stamp them out.

The insurgent wisely uses time as an asset against the state.

This does not mean the Maoists have not expanded their areas of operation and influence. Long before their loss in Andhra, the PWG had spread into the border areas of Odisha, Chhattisgarh (then a part of Madhya Pradesh), Madhya Pradesh, and Maharashtra, which have forested regions contiguous with the North Telangana forests on the northern side of Andhra Pradesh. The Maoists maintained a less violent mode in these areas and used the areas as sanctuaries. This relatively low profile, coupled with the remote, inaccessible nature of those areas, allowed the government to ignore the insurgents in that region for some time.[19] By 2000, however, as the insurgents' need to expand their operations again became imperative, the Andhra Pradesh police gained the upper hand and started flushing the Maoists out, even from their hideouts in the North Telangana forests.

The economics of expansion into resource-rich areas, however, was positive for the insurgents compared to lying low and defending their bases in Andhra Pradesh, particularly in view of the differences in preparedness and political will between the various state governments at that time. As the Maoists lost their bases in Andhra Pradesh, they gradually made the Bijapur and Dantewada districts in Chhattisgarh their main center of operations, while keeping southern Odisha (particularly Malkangiri) as their main hideaway.[20] Meanwhile, two Maoist groups, PWG in the south and the Maoist Communist Centre of India in the north, merged in 2004 to form the Communist Party of India (Maoist). Though the Maoists have escalated their violence and extortion activities outside Andhra, they have generally done so within the forested regions and desisted from expanding into open rural areas.

Because states face considerable difficulty and cost trying to collect intelligence in these remote, isolated pockets, they tend to avoid doing it.

Intelligence

In open rural areas, the insurgents tend to lose many of the advantages they have in the forests, some of which have already been discussed. Other advantages may be less apparent. For example, because states face considerable difficulty and cost trying to collect intelligence in these remote, isolated pockets of population, they tend to avoid doing it.[21]

This difficulty can be explained from the practitioner's point of view. An intelligence agency's capacity to collect information from an area can be seen as a product of five factors: (1) the visibility of the target, (2) the relative presence of intelligence operatives in the area, (3) the ratio of possible observers to population in the area, (4) the observers' professional and technical capacity to gather useful intelligence, and (5) the availability of communication channels for the observer to relay collected intelligence. The general lack of roads, communication, infrastructure, and facilities in India's hinterlands makes it difficult for the government to motivate its employees to go to those places or stay there long enough to develop the kinds of relationships with the locals that will yield useful intelligence.

The first factor depends largely on the insurgents themselves. They can decide deliberately to minimize their activities to avoid attention. They may use camouflage and concealment techniques to avoid detection. While the Maoists' armed squads normally wear uniforms and openly carry arms, whenever they find it necessary, they will forego the arms and uniforms and merge with the local population in crowded venues such as weekly markets. As mentioned earlier, the bigger a group moving in a forest is, the greater is its chance of detection by its enemy. Maoist squads typically are small in size, particularly in the areas where they expect intrusion by government forces. Except while directly interacting with the villagers, the squads do their best to avoid detection.

Whenever they find it necessary, the Maoists will forego arms and uniforms and merge with the local population in crowded venues.

Regarding the second factor, until insurgents move in and become active, the state government's intelligence agencies normally will not have much presence in these isolated areas, which otherwise are of little interest to them. Moreover, once they are established, insurgents will use intimidation to push out whatever little non-military presence the government has in those areas.

The third factor, regarding the ratio of possible observers to the local population, is affected by the fact that these areas have very small numbers of people who are dotted in countless hamlets over huge territories. It is possible to roam around in such areas for days together without being spotted by anyone. The capacity of the observer to observe, which is the fourth factor for intelligence work, again is restricted by the density of the forest, as illustrated in figure 1. This limitation applies to technical gadgets as well. All devices that work in a horizontal direction and depend on line of sight, such as remote cameras, night-vision devices, radar, and the like, suffer the same handicap. Other technical devices such as satellites and unmanned aerial vehicles (UAVs) that use vertical line of sight have their own limitations in heavily forested areas.[22] The canopy of the trees in tropical forests such as those of eastern India makes it difficult to observe patterns from above. These difficulties are compounded by the fact that the Maoists seem to be aware of such surveillance from above and accordingly adopt camouflage and concealment techniques.

What is more, regarding the fifth and final factor, the general lack of infrastructure and communication channels in these remote Maoist-affected areas means that even if an observer sees something, it is very difficult and time-consuming to pass the information on to an intelligence agency. By the time the intelligence reaches the agency, too often it has become stale and useless for undertaking any operation. Maoists are aware of this factor and deliberately destroy roads and ban the use of mobile phones in their operational areas.[23] They may even kill people they find using mobile phones, on the suspicion that they are police informers.[24] According to one source, "In the past four years, more than 200 mobile towers have been blown up in the nine States by Maoists alleging security forces were being informed about their movements and locations with mobile phones."[25]

Use of Technology

One more advantage that the Maoists enjoy in the forests but lose in open rural areas also relates to technology. The state's ability to acquire technology and its reliance on technological capabilities is enormous compared to that of the Maoists, who have neither the money nor the infrastructure to incorporate advanced technologies into their operations. Not being able to use mobile phones, surveillance devices, UAVs, and the like in the Maoists' operational areas, therefore, is much more of a disadvantage for the state than it is for the Maoists. The difficulties with visibility and line of sight in a dense forest apply equally to the use of long-range artillery. Because the land where the Maoists operate is often also very hilly, armored vehicles, tanks, and heavy machine guns can become more liabilities than assets.

Not being able to use mobile phones and the like in the Maoists' operational areas is much more of a disadvantage for the state than it is for the Maoists.

By the same token, because UAV surveillance over tropical forests is unreliable, the use of aircraft for transporting troops and for aerial attacks can be highly dangerous. Security forces may not be aware of the presence of insurgents in an area, and may come under fire as they fly too close or try to land.[26] Further complicating matters, the Maoist problem is one of domestic security for India, in which its own citizens—the insurgents—hide among other citizens. The target population is scattered throughout the forests, making aerial and other area-based attrition approaches counterproductive. Without highly accurate targeting information from intelligence and surveillance, the collateral damage from aerial attacks is unacceptable—a problem made even worse, of course, in more populated localities. In a liberal democracy such as India, the public outcry against any loss of innocent lives from aerial attacks by the state can become deafening, which is a risk that a democratic government cannot afford. In fact, insurgents frequently seek to goad the state into indulging in such overreactions precisely to undermine state legitimacy in the eyes of the population.[27] As North Vietnamese General Vo Nguyen Giap famously commented, the Vietnam War "was fought on many fronts … [but] the most important one was American public opinion."[28] In the same vein, while discussing U.S. involvement in irregular warfare in particular but with regard to any liberal democracy fighting an insurgency, Colin Gray observed that such a war "will not be won or lost in the local barrios and swamps, but in America's sitting rooms."[29]

Insurgents frequently seek to goad the state into indulging in overreactions precisely to undermine state legitimacy in the eyes of the population.

It is easy to imagine that access to the internet is a far cry in a place where the use of mobile phones is rare. As would be expected, the level and use of computer technology decreases as one moves away from the urban areas of India into more remote areas. Furthermore, those remote areas already dominated by Maoist violence have the lowest level of access to technology, because the Maoists actively oppose the use and spread of information technology in their areas of influence. It is their "above-ground" supporters and sympathizers who use the internet and social media to influence civil society and reach the sitting rooms of urban populations.[30] It is almost impossible, however, to reach the underground Maoist operatives through these above-ground supporters. The insurgents use only a series of trusted couriers for the exchange of letters and money or other communications. In the absence of sophisticated communications technologies, the technique of "big data mining" of social media is not available to intelligence services for counterinsurgency planning.[31] Similarly, when insurgents use couriers and hard cash, hunting through financial transactions may not yield any useful results for the state security services.

Maoist supporters and sympathizers use the internet and social media to influence civil society and reach the sitting rooms of urban populations.

The Maoist leadership's attitude toward information technology is reminiscent of that of Osama bin Laden, whose avoidance of the internet, telephones, and mobile phones helped him to escape detection for a decade despite the enormous level of effort that was undertaken to find him.[32] One wonders about the probability of bin Laden being detected if he had been willing to live in more humble dwellings without modern comforts, and had sanctuaries in the dense tropical forests of a Third World country.

Conclusion

However much the state may wish to use remote, technology-based solutions to fight insurgency, such means may be largely irrelevant or even counterproductive as long as the insurgents stay in the safety of the inaccessible forested areas of a Third World country. If insurgents opt for security over the efficiency of using communications technology, the state needs to look for solutions that are not dependent on exploiting technology.

Because the state and its security organizations are heavily dependent on the internet for their everyday activities, however, they are potentially vulnerable to the exploitation of big data analytics by a technologically competent insurgent. Just as in the business world, where "such information can provide competitive advantages over rival organizations," these opponents will have an asymmetric advantage over the state in this regard.[33]

On a positive note for the state, if officials adopt a strategy of strengthening the vulnerable areas adjacent to those occupied by insurgents through infrastructure development and access to technology, the state can use the same logic to deny an insurgency the ability to further expand. It may look expensive for less developed former colonies to make these structural investments, but a cost-benefit analysis needs to be carried out to determine the future cost of fighting insurgents over a larger area. During a recent field study, I found that the use of mobile phones spread rapidly into remote regions adjacent to Maoist-controlled areas once the construction of new roads improved accessibility. Better roads and communications will make it difficult for the Maoists to expand into those areas, since they will no longer find the security of isolation there. ❖

Better roads and communications will make it difficult for the Maoists to expand into remote areas, since they will no longer find the security of isolation there.

ABOUT THE AUTHOR

D. M. "John" Mitra is a joint director of the National Crime Records Bureau, New Delhi, India.

NOTES

[1] For more information on the Maoist insurgency in India, see Srinivas Ganapathiraju, "Maoist Insurgency in India: Emerging Vulnerabilities," *CTX* 3, no. 2 (May 2013): 75–79.

[2] From the website of the Ministry of Home Affairs, Union Government of India, see the section titled "Background": http://www.mha.nic.in/naxal_new

[3] U.S. Government, *Guide to the Analysis of Insurgency 2012* (Washington, D.C.: U.S. Government, 2012), 1: http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/COIN/Doctrine/Guide%20to%20the%20Analysis%20of%20Counterinsurgency.pdf

[4] Ibid., 2.

[5] Daniel Byman, *Understanding Proto-Insurgencies*, occasional paper (Santa Monica, Calif.: RAND Corporation, 2007), 5: http://www.rand.org/pubs/occasional_papers/OP178.html . According to Byman, the proto-insurgency "is a small, violent group that seeks to gain the size necessary to more effectively achieve its goals and use tools such as political mobilization and guerrilla warfare as well as terrorism" (Ibid.).

[6] The term *Naxalite* comes from an early Communist-led uprising in the 1950s that originated in the West Bengali village of Naxalbari. Naxalites were the forerunners of the present-day Maoists.

[7] Ernesto "Che" Guevara, *Guerrilla Warfare* (Thousand Oaks, Calif.: BN Publishing, 2012), chap. 1, sec. 2: http://chehasta.narod.ru/guerillaeng.htm#2

[8] Durga Madhab Mitra, *Understanding Indian Insurgencies: Implications for Counterinsurgency Operations in the Third World* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2007), 63: http://www.strategicstudiesinstitute.army.mil/pdffiles/pub751.pdf

[9] Mitra, *Understanding Indian Insurgencies*, 64.

[10] Population Reference Bureau, *2012 World Population Data Sheet* (Washington, D.C.: Population Reference Bureau), 11–13: http://www.prb.org/pdf12/2012-population-data-sheet_eng.pdf

[11] Mao Tse-Tung [Mao Zedong], *On Guerrilla Warfare*, trans. Samuel B. Griffith (Thousand Oaks, Calif.: BN Publishing, 2007), 93.

[12] Nathan Leites and Charles Wolf, Jr., *Rebellion and Authority: An Analytic Essay on Insurgent Conflicts* (Chicago: Markham Publishing Company, 1970), 32–33.

[13] David C. Gompert and John Gordon, *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency* (Santa Monica, Calif.: RAND Corporation, 2008), 381: http://www.rand.org/pubs/monographs/MG595z2

[14] Saji Cherian, "The States of Denial," *OutlookIndia.com*, 23 August 2005: http://www.outlookindia.com/article.aspx?228369

[15] Chenchuramaiah (also rendered Chenchu Ramaiah) had been accused by the People's War Group of conspiring to attack Dalits in the Andhra village of Karamchedu in 1985. See "SC Convicts 31 in Karamchedu Dalit Massacre," *Times of India*, 20 December 2008: http://articles.timesofindia.indiatimes.com/2008-12-20/hyderabad/27889860_1_upper-caste-dalits-life-imprisonment

[16] Satyanarayan Pattnaik, "Maoist Fear Blocks Koraput Projects," *Times of India*, 25 March 2011: http://articles.timesofindia.indiatimes.com/2011-03-25/bhubaneswar/29188122_1_villagers-acres-of-non-tribal-land-narayanpatna ; "Maoists Cause Mayhem in Malkangiri," *Hindu*, 24 February 2009: http://www.hinduonnet.com/thehindu/thscrip/print.pl?file=2009022451810300.htm&date=2009/02/24/&prd=th&; B Sridhar, "Security Issue Continues to Haunt Contractors after Chawka Incident," *Times of India*, 4 April 2011: http://articles.timesofindia.indiatimes.com/2011-04-04/ranchi/29379710_1_development-projects-contractors-security-issue

[17] Colin S. Gray, "Irregular Warfare: One Nature, Many Characters," *Strategic Studies Quarterly* (Winter 2007): 45: http://www.au.af.mil/au/ssq/2007/Winter/gray.pdf

[18] Mitra, *Understanding Indian Insurgencies*, 84.

[19] Durga Madhab Mitra, *The Genesis and Spread of Maoist Violence and the State's Handling of It* (New Delhi: Bureau of Police Research and Development, 2011), 97.

[20] Venkitesh Ramakrishnan, "Naxal Terror," *Frontline* 24, no. 18 (8–21 September 2007): http://www.frontline.in/static/html/fl2418/stories/20070921500400400.htm

[21] Leites and Wolf, *Rebellion and Authority*, 31–32.

[22] Yatish Yadav, "Heron Drone Proves a Dud in Tracking Maoists in Chattisgarh," *India Today*, 3 January 2012: http://indiatoday.intoday.in/story/heron-uav-fails-to-track-maoists-in-chattisgarh/1/166919.html

[23] "Maoists Cause Mayhem"; Sridhar, "Security Issue Continues to Haunt."

[24] "Maoists Murder Youth in Koraput District," *Hindu*, 4 May 2012.

[25] Mukesh Ranjan, "State's Naxal-Hit Zones to Get 987 Mobile Towers," *Pioneer*, 6 March 2013.

[26] Yadav, "Heron Drone Proves a Dud."

[27] Leites and Wolf, *Rebellion and Authority*, 112.

[28] Howard Langer, *The Vietnam War: An Encyclopedia of Quotations* (Westport, Conn.: Greenwood Press, 2005), 318.

[29] Gray, "Irregular Warfare," 45.

[30] In one such case, a party Central Committee Resolution of 11 June 2013 was circulated on the internet, which among other things warned of a possible aerial attack on Maoist positions by security forces. For an example of communist propaganda on the internet, see Ian Paxson, "PSL on Nepal: A Heroic Struggle for Socialism," *Kasama Project*, 19 November 2013: http://kasamaproject.org/projects/revolution-in-south-asia

[31] Big data mining is an analytic process designed to gather and analyze large amounts of data from communications technologies and social media in search of consistent patterns and/or systematic relationships between variables, and then to validate the findings by applying the detected patterns to new subsets of data. For more information, see "Data Mining," StatSoft, n.d.: http://www.statsoft.com/textbook/data-mining-techniques/#mining . Also see James Igoe Walsh, "Big Data, Insider Threats, and International Intelligence Sharing," in this issue of *CTX*.

[32] "Osama bin Laden Killed: Phonecall by Courier Led US to Their Target," *Telegraph*, 3 May 2011: http://www.telegraph.co.uk/news/worldnews/asia/pakistan/8489078/Osama-bin-Laden-killed-phonecall-by-courier-led-US-to-their-target.html

[33] For an explanation, see "Big Data Applications: Real-world Strategies for Managing Big Data," *Business Analytics*, 10 January 2012. See the *Search Data Management* website: http://searchdatamanagement.techtarget.com/essentialguide/Big-data-applications-Real-world-strategies-for-managing-big-data

Big Data, Insider Threats, and International Intelligence Sharing

Dr. James Igoe Walsh, University of North Carolina at Charlotte

How does the "big data" revolution affect intelligence sharing between countries? The sharing of intelligence derived from big data—such as intercepting text and voice communications carried over the internet—could improve intelligence about threats such as transnational terrorist groups by providing intelligence agencies with a much larger pool of data and new software tools that permit faster and more focused analysis. This is why intelligence agencies in the United States and many other countries have moved aggressively over the last decade to develop the capacity to collect and mine online data.

Intelligence agencies now collect and store electronically enormous amounts of information that they want to keep secret; however, the very ease of storing and sharing this collected data also makes the data vulnerable to foreign states, hackers, and others that want access to it without authorization. Some of these are "outsider threats," such as the intelligence agency of a foreign state, and can be thwarted with varying degrees of success by denying access to an intelligence agency's network. Here I focus instead on "insider threats," by which I mean individuals who have legitimate access to some secret intelligence and exploit their position to share the information with outsiders.

Big data magnifies the threats that such insiders pose, because they may be able to access a great deal of sensitive data and reveal it at a low cost to foreign states, criminal or violent organizations, journalists, or human rights groups. Concerns about such insider threats could reduce the willingness of states to share intelligence with each other, thereby reducing the international community's ability to collectively define and respond to security problems.

Big data magnifies the threats that such insiders pose, because they may be able to access a great deal of sensitive data and reveal it at a low cost.

I suggest a number of ways that states may decide to address this sort of problem. These solutions include

- sharing only with the most trustworthy partners,
- establishing hierarchical relations among the intelligence agencies of different countries so that one can closely monitor the other,
- greater transparency and oversight of the use of big data by intelligence agencies, and
- foreswearing at least some international intelligence sharing.

Each of these solutions has strengths and weaknesses, and it is likely that we will see a mix of these strategies implemented by different groups of countries. One counterintuitive implication of this discussion is that increased transparency about the process of data collection and analysis is valuable not only because it is consistent with democratic norms, but also because it actually reduces the problem of insider threats and makes promises by one country to share intelligence with another more credible and effective.

Big Data and Intelligence Sharing

Much lower storage and retrieval costs make it much easier to both collect and analyze electronic data, as well as to share the data and analysis widely within and across organizations.

Shared intelligence goes beyond the exchange of factual information and includes, in many cases, the sharing of analytical products. Sharing allows countries to spread the costs of intelligence acquisition and analysis across all of the participants, and, as is the case with most exchanges, the benefits from sharing increase when participating states specialize. Thus, sharing should lead to the production of both more and higher-quality intelligence.

Before going into how big data alters these calculations, it is important to understand what *big data* means in the context of this discussion. I suggest that big data is composed of three technological trends. These trends are well-known and have implications well beyond the issue of intelligence sharing, so I will mention them only briefly here. The first is the ability to collect and store large amounts of electronic communications. Intelligence agencies have been collecting such information for some time, but today the scale is much larger, since individuals rely on electronic forms of communication far more heavily than in the past. A second trend is the ability to analyze this data more effectively and quickly than before, using software tools such as search algorithms, network analysis, geographic information system tools, and other approaches. Thus, while the scale of data collection has grown enormously, the tools for analyzing data have also improved, making it somewhat easier to solve the "needle in a haystack" problem. Third, much lower storage and retrieval costs make it much easier to both collect and analyze electronic data, as well as to share the data and analysis widely within and across organizations.

Once a critical mass of states develops the capacity to use such technologies and protocols for sharing intelligence, participation should become increasingly valuable.

Big data may create powerful incentives for states to share intelligence more frequently and intensively. There are three reasons for this, as well. The first is that information technology substantially reduces the marginal cost of sharing intelligence. Sharing intelligence in an electronic format at scale requires large investments in information technologies such as storage space and protocols for remote access to data. Once these investments are made and the technologies and practices are in place, it is very inexpensive from a technical standpoint for one country to share an additional piece of information with another. In principle, any intelligence in an electronic format could be shared with any user almost instantaneously at a very low cost. Second, the creation of such sharing technologies could have powerful network effects. Once a critical mass of states develops the capacity to use such technologies and protocols for sharing intelligence, participation should become increasingly valuable as more countries are able to share intelligence with each other. Related to this, the information technology infrastructure required for sharing on a massive scale is expensive and complicated to develop and maintain. It requires investments in hardware, communications equipment, and skilled operators who can design and manage the entire system. The fixed cost is likely higher for intelligence agencies than for comparable activities in the private sector, because the collection and analysis ambitions of intelligence agencies are much higher, and also because intelligence agencies have concerns about information security that might lead them to prefer trusted suppliers inside and outside the government over the ones with the cheapest rates. Some states may lack the financial and technical means to create and maintain such systems. This gives them stronger incentives to collaborate more closely with other states, since collaboration spreads some of the costs across the budgets of multiple countries.

It is important to recognize that participants in intelligence-sharing arrangements differ in their ability to provide useful intelligence to each other. The United States is clearly the dominant actor in all of the sharing networks in which it participates. It spends far more on intelligence than any other state, has global collection and analysis needs, and was the first to develop or implement on a large scale many of the big data applications for intelligence. This dominant position has two implications for intelligence sharing. First, the network effect is really a U.S. network effect. Other states have a great deal to gain from sharing intelligence with the United States, while the marginal benefit to the United States of sharing with any particular state is likely to be much lower. Second, the United States is better positioned to "go it alone" in intelligence sharing. It may be able to collect a considerable amount of electronic intelligence without the cooperation of other states, relying on its own satellites, sensors, and other means of data collection. In some ways, the United States accrues fewer of the benefits that arise from specialization in intelligence collection and analysis. This means that Washington is well-positioned to exert the greatest influence over the content and interpretation of intelligence-sharing agreements, and that big data may increase the dominance of the United States over its partners and permit it greater leeway to operate without their active support. Big data, then, produces somewhat mixed incentives for the United States to share intelligence. On the one hand, big data allows the United States to distribute the costs of collection and analysis over more partners, and to gather and analyze more data shared by these partners. On the other hand, U.S. dominance of many of the technologies that are applied to intelligence sharing may reduce its need to rely on partners for critical intelligence. How the United States is likely to respond to these incentives, I suggest in the following sections, depends on its ability to effectively manage and oversee its partners' information security practices.

Big data may increase the dominance of the United States over its partners and permit it greater leeway to operate without their active support.

Big Data and Insider Threats

Given the benefits, why might two states not share intelligence with each other? Why would they forgo the potential benefits of sharing? Theories of international cooperation identify an important barrier to sharing in situations where mutual benefit is possible: the enforcement problem, which is very relevant for the issue of insider threats.[1] The enforcement problem arises when a country reneges on or "defects" from a commitment to share intelligence. Defection may be either deliberate or involuntary, in the sense that lower-level state officials defect without their leadership's approval. A sender of intelligence can defect by altering intelligence's content, withholding it altogether, or exaggerating the accuracy of its sources. Senders that defect deliberately manipulate shared intelligence with the intent of influencing the recipient's subsequent actions. Alternatively, individuals within a sending state might be operating under the commands of another power or group that controls the intelligence that these individuals then pass to partner states. Corruption or other administrative weaknesses might limit the state's ability to effectively collect intelligence in the first place. Sending states also might not share fully or honestly if some of their personnel who control the relevant intelligence disagree, on political or policy grounds, with the decision to share it. A recipient of intelligence might defect by forwarding shared intelligence to a third country if it concludes that its interests are served by passing along intelligence, even if this might conflict with the interests of the sender. A recipient also might inadvertently forward shared intelligence to third parties,

Senders that defect deliberately manipulate shared intelligence with the intent of influencing the recipient's subsequent actions.

such as hostile states or the media. Individuals who have access to the shared intelligence may be agents of a third state or other outside group and may violate their government's policy by sharing intelligence with their controllers.

The most valuable sharing partners have much useful intelligence, but they also can do the most damage when they defect from promises to share.

The costs of defection can be large for both senders and recipients, which is one reason why the enforcement problem looms particularly large when states consider sharing intelligence. Recipients may be deceived into providing benefits to senders that provide them with low-quality intelligence. More important, though, are the potential indirect costs of cooperating with a sender that defects. A recipient may base important foreign policy decisions involving the use of force on flawed or misleading intelligence shared by other states. Costs for the sending states can be substantial as well, including sharing secrets or sources and methods with third parties. These costs increase when the participating states have developed specialized and complementary intelligence efforts: specialization increases the costs of defection. The most valuable sharing partners have much useful intelligence, but they also can do the most damage when they defect from promises to share. Defection can remove access to the partner's specialized assets and seriously weaken the recipient's ability to gather useful intelligence on a target.

Intelligence almost always includes an analytical element, which may be more easily manipulated by a state than the raw information on which it is based.

Another reason why the enforcement problem is a powerful barrier to intelligence sharing is because it is difficult to determine whether a partner has reneged, for at least two reasons. First, intelligence almost always includes an analytical element, which may be more easily manipulated by a state than the raw information on which it is based. Second, and perhaps more important, intelligence by definition includes secret information, although most intelligence producers use open sources of information as well as secret or clandestinely obtained information. States and their intelligence communities go to great lengths to secure secret intelligence and to prevent their targets from discovering their sources and methods of intelligence collection and analysis. For this reason, intelligence agencies are reluctant to share all of the intelligence they control, even within their own governments. This concern for security makes it very difficult for one state to determine whether another has defected on a promise to share intelligence. Keeping details of intelligence collection and analysis secret is, on the one hand, recognized as a legitimate security practice, but on the other, it makes it easier for a sending state to alter or fabricate the information it passes to others. The barriers to sharing raised by security requirements also pose difficulties for the sending states. Sending states may want to ensure that recipients do not pass the shared intelligence along to enemies, either deliberately or inadvertently, but at the same time, the recipients do not want to divulge their security arrangements, to prevent others from illicitly gaining access to the intelligence they possess.

Big data can magnify these costs and risks of intelligence sharing, especially those associated with inadvertent defection by insiders in other states. The big data revolution makes it less costly and difficult to share large amounts of intelligence with a greater number of states. States participating in such arrangements, in turn, will need more technical and analytical personnel to process this information and develop it into analytical products for the consumers in their country. This means that there are more "insiders" in the recipient countries who could potentially share this intelligence with third parties. It also means that there is a potentially much larger trove of intelligence for insiders to steal. The fact that the intelligence is in an electronic format rather than on paper makes it much easier to convey to third parties. Furthermore, the highly-skilled technical personnel whom states need to manage their larger and more complex information-sharing infrastructures are in high demand in other sectors of the economy, and governments may lack the salaries to compete effectively to hire the most desirable candidates. This may be a particular difficulty for intelligence agencies, which place a high priority on monitoring the backgrounds and work practices of their employees to minimize insider threats, because information technology experts have a reputation for valuing their autonomy both in and outside of the workplace. Intelligence employees' need for access to a wide range of internal systems and processes in order to do their jobs means that traditional security practices such as compartmentalization and "need to know" may hinder their performance. This requirement gives them potential access to large volumes of intelligence information, as well as the skills to cover their tracks should they choose to copy and share such intelligence with a third party.

Information technology experts have a reputation for valuing their autonomy both in and outside of the workplace.

Possible Solutions to the Insider Threat Problem

If enforcement problems make sharing intelligence difficult, how can these barriers be overcome? This section looks at four possible solutions: selecting trustworthy partners, establishing hierarchical relations between states that share intelligence, increasing transparency and oversight of the use of big data for intelligence purposes, and scaling back and limiting intelligence sharing.

Trust

A straightforward solution to the problems created by big data and insider threats is to select intelligence-sharing partners that are trustworthy. In this context, trust is an expectation on the part of one state that another state will not defect from promises to share intelligence in a secure manner. Trust emerges most robustly when parties do not fear that their partner's interests diverge from their own.[2] Divergent interests may give the sender an incentive to deliberately communicate incorrect intelligence, in an effort to convince the recipient to act in a way that is most favorable to the sender. On the other side, a receiving state might pass along shared intelligence to third parties without the sender's knowledge or permission. From this perspective, states should focus on selecting their partners carefully, only sharing intelligence with those that have common interests and a history of living up to their promises.[3]

Divergent interests may give the sender an incentive to deliberately communicate incorrect intelligence.

Furthermore, there is much evidence that mutual trust facilitates the reliable exchange of information. In the area of intelligence sharing, many of the states with which the United States shares intelligence most intensively—Canada, the United Kingdom and other states in Western Europe, Japan, and South Korea—are long-standing allies with successful histories of cooperation on intelligence sharing and a range of other issues. Big data may erode the utility of such generalized trust, however. The fact that so much more intelligence could be shared today than in the past, and that more personnel may have access to it, increases the risks from insider threats within the intelligence agencies of partner countries. Breaches of security by even one individual could do substantial damage to foreign partners. For example, Edward Snowden's revelations about the collection of cell phone and e-mail communications data by the National Security Agency exposed a remarkably wide range of

Big data might make reliance on past trustworthiness a riskier strategy than it previously has been.

information, and Bradley Manning's alleged leaking of hundreds of thousands of internal documents to WikiLeaks provided quite detailed information about a huge range of topics. Big data, then, might make reliance on past trustworthiness, as a way to screen desirable from undesirable intelligence-sharing partners, a riskier strategy than it previously has been.

Hierarchy

Selecting only partners that are trustworthy has another cost: it can exclude partners that may have particularly valuable intelligence. In practice, it appears that states not infrequently share intelligence with partners they consider less than completely trustworthy. The United States is one prominent example. In these circumstances, intelligence-sharing agreements between states can be constructed as a hierarchy. Hierarchy differs from anarchy, often considered the normal state of affairs in international politics, in that a subordinate state voluntarily gives up some autonomy to a dominant state. The dominant state can monitor the subordinate state for defection and punish such defection when it occurs.[4]

Hierarchy provides one possible solution to the enforcement problem by allowing the dominant state to take direct and intrusive steps to ensure that the subordinate is not defecting.

Hierarchy can help to manage the risks of defection. The dominant state in the hierarchy takes the role of making important decisions about the form of the intelligence-sharing partnership. Subordinates give some of their decision-making autonomy to the dominant state, in return for which the dominant state provides the subordinate with some combination of its own shared intelligence, diplomatic support, economic assistance, and other valuable goods and services. Hierarchy provides one possible solution to the enforcement problem by allowing the dominant state to take direct and intrusive steps to ensure that the subordinate is not defecting from its promise to securely share intelligence. In the context of big data, hierarchy would involve the setting of commonly agreed standards for preventing insider threats. It would also require the dominant state to play an active role in vetting how well the subordinate partners implement these standards. This role can be carried out in a number of ways. For example, the dominant state can assign liaisons who directly participate in, and can thus oversee, the intelligence activities of subordinate states. Such liaisons can play an important technical role in facilitating cooperation, by, for example, ensuring that each country's information technology can communicate efficiently and securely. But liaisons also serve as a useful way to check on the day-to-day internal security practices of subordinate states. The dominant state can also pay for a disproportionate share of the physical and information technology infrastructure needed to carry out large-scale data sharing, helping its partners develop more sophisticated data collection, storage, and analysis capabilities. Such cost-sharing typically comes with strings: for instance, the dominant state asserts the right to audit how funds are spent and technology is used. This gives the dominant state some direct control over the processes that are used by subordinates.

Hierarchical arrangements also create costs and risks for the participants. Most obviously, they give much greater freedom of maneuver to the dominant state than to subordinate participants. Subordinates surrender some degree of control over their internal standards for preventing insider threats, which will lead some to conclude that these sacrifices are not worth the benefit of sharing intelligence. Hierarchy works most effectively when the participating states' underlying interests are compatible enough to prevent large incentives for defection, since compatible interests allow states to use the institutions of hierarchy to bridge their differences. What do subordinates get in return? As suggested previously, the dominant state typically provides valuable goods and services to the subordinate, such as access to some of its much more extensive collection of intelligence products, technical support for developing the capacity to collect and analyze large amounts of data, and financial inducements. These, in turn, are some of the costs that the dominant state pays to entice subordinates to join it in a hierarchal relationship. A more important cost, though, is that the dominant state must reassure its subordinates that it will not defect on them. There is a risk that the dominant state might use its extraordinary position in the relationship to secretly obtain intelligence from its partner that the latter does not wish to share. The dominant state might also be subject to its own insider threats. This possibility will be of particular concern to subordinates, which often prefer that the details of their intelligence-sharing arrangements, including their subordinate status, not be revealed to outsiders. How the dominant state reassures potential subordinates that it will not defect, deliberately or inadvertently, is a key question that must be addressed if a hierarchy is to function smoothly and serve the interests of participating states.

Hierarchy works most effectively when the participating states' underlying interests are compatible enough to prevent large incentives for defection.

Transparency

Another way to address the issue of intelligence sharing is through greater public transparency, especially on the part of the dominant state, about the processes it uses to collect and share intelligence. To this point, I have assumed that all insider threats are identical. But it is likely that the motives and goals of insiders willing to reveal intelligence are at least somewhat varied. Two types of insiders dominate current discussion of the problem. The first, more traditional type are insiders who volunteer, are paid, or are coerced to provide intelligence to a foreign power or organization. The second type are insiders who are disturbed by the scope and scale of contemporary intelligence collection because, in their view, it violates privacy rights or the law. These different types are likely to behave quite differently. Those in the first group have powerful motives not to publicize their theft or unauthorized sharing of intelligence, because their illicit actions will be brought to an end and they probably will be prosecuted. But publicity is the key motive for the second type, who hope that revealing the extent of intelligence collection will spark public outrage and lead to restraints on intelligence activities. Prosecution may even be part of their publicity strategy.

These different types of insiders may be countered with distinct policies. Traditional counterintelligence practices, such as background checks, should have some chance of catching both types. Insiders of the second type, however, may also be dissuaded from releasing information by greater official transparency about how and what data is being collected, and under what circumstances this data is analyzed by intelligence agencies. Such transparency about the general processes of data collection and analysis (but not, of course, about the content of this data) may mollify insiders who want a vigorous public debate about the trade-offs between security and privacy. Subjecting such practices to some sort of systematic legislative and/or judicial oversight would also ensure that new collection techniques, which emerge frequently because of rapid changes in communication and commercial technologies, are regularly included in the oversight process.

In addition to preventing some insider threats, greater transparency could help to reinforce international hierarchies for intelligence sharing. Recall that one difficulty with hierarchical relationships is that the dominant power must figure out a way to reassure subordinates that it will not abuse its extraordinary position. Greater transparency about big data and intelligence collection and analysis within the political institutions of the United States, for example, could also provide some information to foreign partners that could, for example, monitor open hearings in Congress and the courts. Assuming that these institutions have some incentives to exercise vigorous oversight and to push the executive to detail and justify its data collection strategies, they might both reduce the danger from insider threats and also reassure intelligence allies overseas that their dependence on the United States is not being secretly exploited.[5] At the same time, transparency is not free of risk. An important dynamic is the trade-off between using intelligence for counterterrorism or other goals, and privacy rights. Greater transparency risks revealing sources and methods to opponents, which can then take active countermeasures to more effectively mask their communications and activities. Striking a balance between enough transparency to mollify the critics of intelligence agencies (and reassure foreign partners) and sufficient secrecy about the details of how intelligence is collected and analyzed is not easy.

An important dynamic is the trade-off between using intelligence for counterterrorism or other goals, and privacy rights.

Go It Alone

In some cases, technological and political developments arising from big data might render intelligence sharing less attractive compared to other options. If insider threats in partner countries are judged to be severe, an intelligence service might be better served by "going it alone" and refraining from sharing. The United States may be uniquely well-positioned to pursue this sort of approach, because it has more alternatives to foreign intelligence services as sources of intelligence in the big data domain. A large fraction of internet communications traffic transits the territory of the United States, providing the opportunity to intercept foreign communications of interest. Many of the dominant hardware, software, communications technology services, and online communications services (such as e-mail, social media, and cloud storage) are headquartered in the United States. These firms often have terms of service that give them considerable latitude to share the data and communications they facilitate, and their status as American firms gives the U.S. government legal leverage to encourage or require them to collaborate with requests for data from the intelligence community. In addition, the U.S. military and intelligence community have unparalleled technologies for collecting intelligence remotely through networks of satellites, surveillance drones, and other devices.

If insider threats in partner countries are judged to be severe, an intelligence service might be better served by "going it alone."

The key advantage of going it alone is that it makes one country less reliant on another country that may be unwilling or unable to live up to the terms of an intelligence-sharing arrangement. But even if the quantity of intelligence collected by a single state could match that gathered by a group of states sharing intelligence, the quality of the intelligence is likely to suffer. Good intelligence analysis is typically based on both a range of sources and a close knowledge of the context in which the target of analysis is embedded. Both of these elements may be lacking when intelligence collection comes to rely primarily on intercepted communications and related sources. Analysts might misjudge the behavior of targets when they have only one type of information. Targets may begin to communicate strategically, saving their most important messages for offline communications and using electronic media to communicate less important or misleading information. Human intelligence is a useful corrective for these problems, and often a foreign partner is far better positioned to collect it. Another advantage of collaboration among intelligence agencies is that it exposes the agencies to the different points of view, assumptions, and judgments made by their counterparts, pushing them to critically review how they reach their own analytical conclusions. Much of this advantage would be lost if intelligence collection and analysis came to rely more exclusively on information that could be collected only by the domestic intelligence services.

Good intelligence analysis is typically based on both a range of sources and a close knowledge of the context in which the target of analysis is embedded.

The age of the internet and global social media—big data—has come on us so suddenly that most individuals, businesses, and governments are scrambling to determine the proper boundary between the private and the public, the secret and the open. Wherever this boundary eventually falls, intelligence services will continue to share some of the information they collect. Each of the strategies discussed here has benefits and drawbacks, but some combination of them is likely to provide the best way forward for dealing with intelligence sharing in the age of big data. ❖

ABOUT THE AUTHOR

Dr. James Igoe Walsh is a professor of political science at the University of North Carolina at Charlotte.

NOTES

[1] There is a large body of literature on enforcement and defection in international politics; some of the fundamental works are James Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379–414; Robert Keohane, *After Hegemony* (Princeton, N.J.: Princeton University Press, 1984); Kenneth Oye, ed., *Cooperation under Anarchy* (Princeton, N.J.: Princeton University Press, 1984); and Arthur Stein, *Why Nations Cooperate* (Ithaca, N.Y.: Cornell University Press, 1990).

[2] For social science perspectives on trust, see James S. Coleman, *Foundations of Social Theory* (Cambridge, Mass.: The Belknap Press of Harvard University Press, 1990); Vincent Crawford and Joel Sobel, "Strategic Information Transmission," *Econometrica* 50, no. 6 (1982): 1431–51; Russell Hardin, *Trust and Trustworthiness* (New York: Russell Sage Foundation, 2002); and Carl I. Hovland, Irving L. Janis, and Harold H. Kelley, *Persuasion and Communication* (New Haven, Conn.: Yale University Press, 1953).

[3] Chris Clough, "*Quid Pro Quo:* The Challenges of International Strategic Intelligence Cooperation," *International Journal of Intelligence and Counterintelligence* 17, no. 4 (2004): 603; Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and Counterintelligence* 16, no. 4 (2003): 528; and Derek Reveron, "Old Allies, New Friends: Intelligence-sharing in the War on Terror," *Orbis* 50, no. 3 (2006): 456.

[4] James Igoe Walsh, *The International Politics of Intelligence Sharing* (New York: Columbia University Press, 2010).

[5] On transparency, oversight, and international cooperation, see Lisa Martin, *Democratic Commitments: Legislatures and International Cooperation* (Princeton, N.J.: Princeton University Press, 2000).

A Roundtable Conversation on Intelligence and Terrorism
Part Three: Sharing Intelligence in Counterterrorism

MODERATOR: I would like to suggest we not restrict our discussion to the issue of sharing intelligence between nations, but that we also consider the domestic experience represented by the participants in this meeting. In the United States, we have a lot of problems with information and intelligence sharing, both within the federal government and between the federal government and the states. I suppose I am asking whether we can learn about international sharing from considering our domestic problems. I am inclined to think that our domestic experience is relevant, that the problems that crop up among U.S. agencies, for example, are not too different from the problems that nations have with sharing intelligence.

◆ Let me explain what our experience is in Europe. We distinguish two different types of relations: bilateral or trilateral and multilateral. Normally, the operational sharing, all of which is of a sensitive technical nature, we do with a partner, or two or three partners. Multilateral sharing, of course, is used to spread a warning: to communicate the name of suspects, for example. In Europe, for 50 years now we have had a club called the Club of Berne. Members' internal security services are invited to join the Club. There are 25 members, all of which are members of the European Economic Community (EEC), plus Switzerland and Norway. Now Croatia also will be invited to join. What do we do? We have a cyphered communication system, which is very convenient, and we can extend it to other countries like the Federal Bureau of Investigation (FBI) in the United States, Australia, and Japan. It depends on the case. We exchange names of suspects, and other information. We also meet twice a year at the director level. The directors can talk quite confidentially about many things, and we also have working groups on counterespionage, on technical issues, and on terrorism. After 9/11, the antiterrorist group was changed to a bigger one called the CTG, the Counter Terrorist Group, and we now have more meetings and work more intensively. We also have tried, even before the Arab Spring, to have contact with services in North Africa. So the Berne Club is an organization that is not very well known, but which works well. It is again easier for internal security services [to share information] than for external services. The Berne Club can't exist unless smaller clubs of three or four—the British, the German, the French—meet regularly, but there is no such global organization because we think that this is a problem for the EEC. The EEC will want to develop its own international intelligence service. Members are not ready for that yet because it's a question of sovereignty.

The information given by a friendly service is the property of the friendly service that gave it.

Another thing that I wanted to raise—this is very important in matters of intelligence—is that the information given by a friendly service is the property of the friendly service that gave it. You [the recipient] do not have the right to share it. This is a principle for all the services. The advantage that all services, both intelligence and law enforcement, have is that we have special judges. We can prepare the manner in which we are going to communicate the information together with the service that gave the information to us. We must protect the source. This is very important.

● As the situation in Syria deteriorated, we established a JIC, a Joint Intelligence Center. It exists at both the domestic level and the international level. We have partners from the United Kingdom, France, Canada, and the United States. All services are represented in this center, which is a very effective center: it collects and analyzes information for all the requirements of the intelligence services that are focused on Syria.

✕ I think, from my experience, that intelligence sharing is based on two elements. First is the legal framework in which your country is operating and the framework in which the intelligence sharing partner's country operates. I will come back to that in just a minute. The second element is a very calculated decision on the risks and benefits of sharing that intelligence. In Europe, it is relatively straightforward in terms of the legal framework because we are all bound, for instance, by the European Convention on Human Rights, and we have similar jurisdictional approaches to the way in which investigations are conducted. These ultimately lead, we hope, to a successful conviction in court. That becomes much more problematic when you are dealing with other countries that are not bound by the European Convention of Human Rights; that situation has led to very different interpretations between, for instance, the UK and the U.S., on the interpretation of the Geneva Conventions. That problem relates specifically to the way in which information has been extracted from prisoners and detainees. Also, it leads to a potentially very difficult situation in which the UK might want to share some lead intelligence on a target of interest to the U.S., but there is concern about how that intelligence will be exploited, because it is very clear in the UK that we cannot conduct straightforward kill operations. The U.S. has a different position. That does cause problems for us in the UK and for some of our European partners.

> The UK might want to share some lead intelligence on a target of interest to the U.S., but there is concern about how that intelligence will be exploited.

+ You mean, in Iraq, all of those operations in which the British killed people were originally intended just to capture them?

✕ Absolutely. The purpose of those operations, the primary purpose of those operations, had to be to capture. We could not legally conduct kill-or-capture operations. It was always capture. If the individual chose not to surrender in circumstances where lethal force had to be used, that was regrettable, but then lethal force was used. That was our default setting, and of course, that does

British soldiers in Iraq

then create problems when you are dealing with your closest ally which had a different approach.

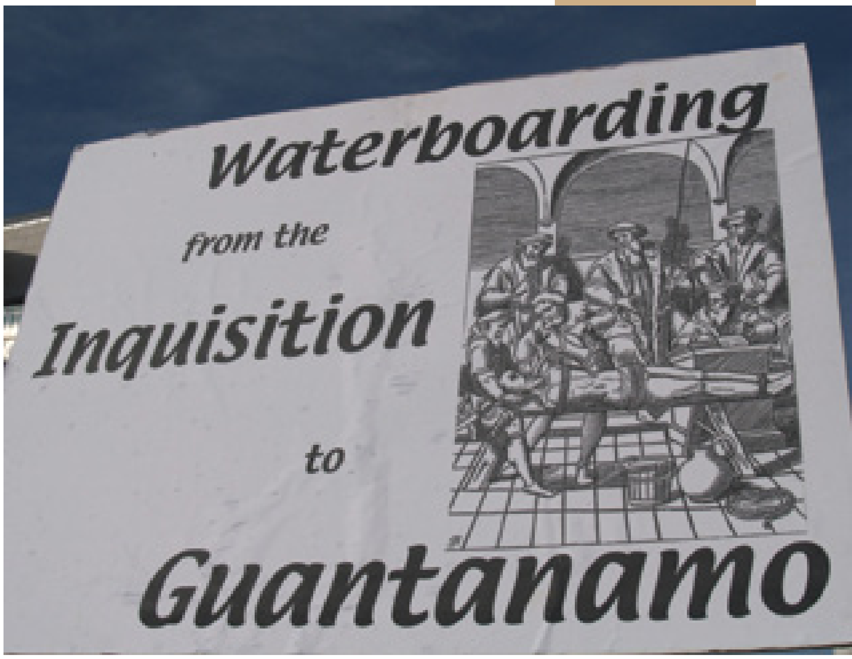
The second element [governing the sharing of information] is the risk/benefit analysis. The situation post-9/11, I think, has fundamentally changed the way in which the need to share intelligence has developed. We got to a point where the default setting was "need to share" rather than "need to know" when it came to counterterrorism. I think we need to consider counterterrorism separately, because when it comes to counterintelligence and counterespionage, I think the rules remain very different. In those cases, you take a very calculated view on the reliability of the partner service with which you potentially want to exchange information. You know, Moscow rules[1] still apply, and I suspect there are one or two other target countries [besides Russia] that conduct very successful and very aggressive penetration operations against most of our partners. Therefore you would choose very carefully what it was you want to share with those countries, for fear of that intelligence becoming compromised.

But when it comes to counterterrorism, then again the default setting has been "need to share" rather than "need to know." From my experience, that default setting has become slightly eroded. The reason it has become eroded is because of concern for what would eventually happen to that intelligence. If any of the intelligence services acquires intelligence on a target that is the subject of an investigation, then I think they will find it very difficult to keep control of that intelligence, and not be required to release that intelligence into the criminal justice system. Certainly, when I first joined the service, which is not that long ago, you were confident that when you acquired intelligence and you recorded that intelligence, you were never going to have to release that intelligence unless you chose to do so. The situation now is very different. Certainly my former colleagues who work in the counterterrorism world now work on the assumption that absolutely everything that they do, say, and record could become a matter of public record [through a trial]. That potential just makes the whole business of exchanging and managing intelligence that much more difficult, and creates concern in the minds of some of our closest allies. We have seen it with the United States, where the United States has asked for assurances that intelligence that is going to be shared with us will remain out of the criminal justice system. That is no longer, I think, a guarantee that we can give.

Colleagues in the counterterrorism world now work on the assumption that absolutely everything that they do, say, and record could become a matter of public record.

+ Not to say this is a contradiction, but it seems to me that you are arguing that, on the one hand, sharing intelligence in counterterrorism is easier because the threat is more shared, so to speak. On the other hand, it is more problematic because, from the viewpoint of the intelligence organization, it may become a [public] criminal matter.

✕ What I am saying is that the constraints and the concerns when it comes to sharing intelligence on counterterrorism are very different from the constraints and the concerns that exist from sharing intelligence on counterespionage and counterintelligence matters. I think there are several reasons why it [sharing counterterrorism intelligence] is easier. One is because in counterterrorism, there is a threat to life. Therefore, with any intelligence we receive that relates to a threat to life, we are under a duty to do something with that intelligence. Where that becomes problematic is where you think, know, or



believe that this intelligence will then be exploited in a way that is contrary to the legal framework in which you are operating. Then it becomes a question of whether you share that intelligence in a way, with caveats, so you have a reasonable degree of assurance that this intelligence will be exploited in a way that is appropriate [according to the laws you are operating under]. It works both ways, and it has become really problematic for the UK government to receive intelligence from governments where we believe that intelligence could have been extracted in a way that is unlawful [in the UK]. It has become such a problem that the Foreign Office is now investing what is, for the UK, very significant sums of money in enhancing capability and capacity in certain countries' criminal justice systems so that they can conduct operational activity and extract information and intelligence in a way that is compatible with our legal framework. We have gotten ourselves into terrible trouble in the courts through having to admit that we have intelligence that was extracted through the use of torture.

MODERATOR: Could you explain why there has been this shift that has made it more difficult to prevent the intelligence from getting into the criminal justice system? What is the origin of that change?

✕ In the UK, you absolutely have to disclose to the defense any evidence or intelligence that you have on which you have based your investigation, and which has resulted in someone being arrested and brought to trial. So we have now got vetted [security cleared] defense lawyers, and there are special procedures for managing the way that intelligence will be used in trial. But they are still jury trials and they can be held in camera[2] up to a point, but you still have to disclose to the defense, and therefore by and large to the defendant, how that intelligence has been acquired. It is a real problem in terms of compromising our own tactics, techniques, and procedures, and then there is a real problem in compromising intelligence that has been acquired from a foreign country.

◆ It is interesting to hear how that is done on the other side of the channel, because [in France] until now we could tell the court, "This is our investigation, we have nothing to add." We didn't give our sources when we presented the case. Now we do because there are special judges, special courts. But sometimes, of course, the lawyers for the defense will say, "Maybe this information you have was obtained under torture." When we receive information, we don't specify whether it is from abroad or from a [domestic] source. Also, can you imagine asking a friendly service if they have obtained the information under torture? No, you receive the information and you check the information. That's all.

Can you imagine asking a friendly service if they have obtained the information under torture?

✕ But the French judicial system is very different. We [in the UK] have an adversarial system where the prosecution has to prove someone's guilt. You know the defendant will have a good idea of how the case is being developed against him or her. If the defendant suspects that some of the intelligence could have come from a friendly country in another part of the world where there is less—there is a different respect for human rights and where they are not bound by the European Convention on Human Rights, then the defense lawyer is under a duty to find the best possible defense. The lawyer can then go on a fishing expedition, and will ask, "Where does this information come from, how was it acquired, was it acquired lawfully, is it admissible?" because of course, the first thing the defense lawyer is going to try to achieve in court is to get the most damaging evidence removed as inadmissible.

● The same is true in the United States. It is called "defense by CIA." The defense asks for all these intelligence documents to prepare the client's defense and the government has to give up the prosecution because it can't turn all of that information over.

✕ We [in France] have another problem that now preoccupies us. The court, the judges—most of them—more and more often ask that we declassify our documentation. Of course, we can't accept this, because we have to protect our sources and protect the information coming from abroad. An independent commission examines the documents, and they say we can declassify this or that. Until now, the independent commission always protected sources, but there is a lot of pressure now. Courts and judges are more and more aggressive, so of course we are concerned about this for the future.

The defense asks for all these intelligence documents and the government has to give up the prosecution because it can't turn all of that information over.

A last point. In terms of my professional experience of managing liaison relationships, there have been instances where it has been easier to share intelligence with certain organizations within the U.S. system than with others, where it had been made very clear that we shouldn't be sharing certain intelligence [given to us by one U.S. organization] with other U.S. government organizations. This is less common in France, but it has happened in France as well, but maybe that was the bad old days.

● I think that the counterterrorist threat and the whole world of counterterrorism has changed intelligence in every way; in particular, it has changed intelligence sharing. It used to be that you could give a colleague from another country or another service a piece of paper and say, "This is the number, say, of SX-20 missiles that we believe the Soviet Union possesses. This is the result of our analytical product." They would either agree or disagree, and you might have some minor technical differences and so on, and then you passed documents back and forth. There was no particular legal action expected on either party at the end of that. The counterterrorist threat, however, always contains the expectation that this is a matter that could go to court. So right from the beginning, every partner has to assume that the other partner has specific responsibilities and restrictions and limitations on what can happen to data and how data can be transmitted.

Our colleague and I shared some experiences trying to work with the incredibly difficult German legal system, where, when we gave them a piece of information, it was almost guaranteed that it was going to get into the court system. We have the same problem in the United States when information is given to us. If it looks like it is prosecutable or could result in an investigation, we don't want to receive it. Give it to the Bureau [FBI] because it is going to become a legal matter. It is eventually going to have to go through some kind of a legal system. So while we may want it as intelligence, we don't want to be the action agency for it. We want the Bureau to obtain it on their own so that they have a clear chain of evidence from the origin of the information right to the moment where they take it in trial, so that they can do their job. The other thing about intelligence sharing that I think is important to understand, at least from the point of view of the problem that the Americans have, is we don't go to you anymore, to anybody, with a piece of paper. We say, "Open your pipeline." Many countries don't have a pipeline.

When you are dealing with counterterrorism, people don't want analytical conclusions. They want raw data.

+ When you say pipeline, what are you… ?

● When you are dealing with counterterrorism in particular, people don't want analytical conclusions. They want raw data. We—the Americans, British, French, and others—set up a program in Europe a few years ago that eventually involved six nations and 12 intelligence services in an operational mode. Simply to get the information to those partners that needed it to do the operational part required us, the United States, to construct an entire transmission system from NSA [National Security Agency] headquarters all the way through several modes, nodes, and everything else, into a certain office in Paris where that information could be received. Now, we are talking about huge data pipelines that nobody in Europe had. It would not have done us any good at all to try to set up that program without providing the partners with the intelligence—not the analytical product, but the raw, continuing data stream. That required several countries to make agreements between [their own] external and internal services on data sharing, which had never existed before. They didn't share that data with one another [in the past]. They had to share the data with one another now because that was the only way that we, through our system, could get the data to them and move the data around in an efficient manner. The public has no idea of how much data is flowing around. Or maybe I shouldn't call it data. But I have read all the academic theories and papers and everything else about how this should be done, and they have no idea what the daily stream looks like. It looks like what you see in that movie, *The Matrix*—falling dots and ones and zeros and everything else—that is the world you are entering into. Out of all of that crap, there might be one iota of importance. But those machines need to be talking to one another to get that one iota of difference. It is beyond human capability.

They have no idea what the daily stream looks like. It looks like what you see in that movie, *The Matrix*—falling dots and ones and zeros and everything else.

+ Was there any filtering done?

● No, not really. You can't filter it. That is the problem. You cannot filter it.

+ Okay, but when this data is transmitted, that data alone won't reveal …

You can't filter the data. That is the problem. You cannot filter it.

● It is not a product that any human being has intervened with and said, "Oh, this is Mr. So-and-So, and he is talking to Mr. Jones." First of all, you should not be sharing intelligence broadly with anybody. You should be sharing intelligence on subjects of mutual concern. I don't care whether it is internal or external. I do not believe in "need to share." I don't really believe Bradley Manning[3] needed to be reading diplomatic cables between different posts that had nothing to do with his job. But we set up a system where he had it.

Anyway, the problem of the huge data sets—I shouldn't use that term *data sets* because they are not data sets. It is just raw garbage traffic, SIGINT [signals intelligence], HUMINT [human intelligence], everything. You have got to have an agreement among the partners, whether it is one, three, or 90, that this is the kind of data that they want to have. That is sometimes difficult to achieve. You can continue to share pieces of paper on other matters. You don't set up one system to preclude another one. But when you are talking about the counterterrorism world, because it [the information] could result in arrests, trials, and convictions, you have got to offer all of those partners—everybody has got to be sharing the same original data. Believe me, that is hard to do. I examined something once where we were looking at passing some simple stuff by classified fax system to a partner or to a major ally. We realized that the nature of the software itself militated against simply sending faxes back and forth, because the other data that was in the original document before it got redacted for whatever purposes internally remained inherently in the document according to the way Microsoft structured the software. So we actually had to go to Microsoft and make a change in the software so that we could securely pass data that we meant to pass, without creating the kind of case that our colleague described, in which somebody would innocently get a Microsoft document, but then the trial lawyer knew the Microsoft system well enough to figure out how to look at all of the earlier versions so he could see what people had redacted, changed, and everything else. This is not what you want to wind up with in court. So you don't want to be passing that to an ally. You want to make sure what you are passing to an ally is your best estimate or the reality, and that it is in a form that the ally can use.

+ But that is separate from that raw data flow you were talking about.

You're going to pass intelligence to partners whom you may not want to deal with. That's simply the way it is.

● That is separate from it, but it is just an example of the kind of real problem that you run into that people don't expect or understand. But let's go back to the big data pipe. The other problem that you are inevitably going to have is that somebody is going to come along and say, "You are sharing stuff with another intelligence service that you are not sharing with us." And we say, "Well, you have no need for it." But they don't like that.

The other thing is that in the world of counterterrorism, you are going to deal with intelligence matters, and you're going to pass intelligence to partners whom you may not want to deal with. That's simply the way it is. What you do in that case is you have to make sure that what you are sharing is very clearly delineated and defined, and that the sharing is restricted to that. We then get back to the problem of the big pipeline. How the hell do you restrict that pipeline? It is not an easy process. It can be done, it is done on a daily basis, and occasionally there are mistakes, and occasionally traffic gets into that pipeline that is supposed to be restricted—that shouldn't get into it. Then you have hell to pay. But you know, these are the realities that you are dealing with every day.

The last thing I will say about [intelligence sharing] is that everybody wants to come to Washington. People are thinking, "Let's move our liaison operations to Washington because then we get closer to headquarters." That is the worst place to be. The people who are furthest removed from any idea of what is going on on the ground, anywhere in the world, are in Washington, D.C. They think they are the greatest experts, but what you have always got to remember, when you're dealing with the people in any national capital, is that you are dealing with political appointees. You're no longer dealing with professionals. The decisions are being made by political appointees, and I have seen over and over and over again a very good intelligence relationship ruined because somebody says, "Wow. Let's get around the local representative and let's move everything to Washington where we have direct access." The next thing you know, you've got someone from a foreign intelligence service with his briefcase going all over Washington, asking, "Will you give me this?" "No, I won't give you this for the following reasons." He'll go to another agency: "Will you give me this?" "Did the other guy say he won't give it to you?" "Yes." "Oh, I'll give it to you then because I want to establish a relationship." That is what winds up happening to you. People start bartering, and it becomes a nightmare.

The people who are furthest removed from any idea of what is going on the ground, anywhere in the world, are in Washington, D.C.

◓ A fundamental reality that I think is important to bear in mind in all of this—and the various folks here have touched on it already—is that in the counterterrorism world, speed is probably more important than in almost any other aspect of intelligence work, and I think it complicates information sharing. You see this as soon as you go to work in the CT area. It is not just that days matter, but hours matter and sometimes minutes matter. Not in every case, certainly, but in some cases. You know, these days the person who learns that some suspect character is taking flight lessons—but is not interested in learning how to land the plane, only in how to maintain it in flight—and doesn't pass that information up the chain rather quickly and make sure it ultimately gets shared around, is in very, very serious trouble. So I think that's an underlying reality that complicates this whole question as well, because you have to make these decisions as to what gets shared very, very quickly. In some cases, anyway.

◆ Maybe we should think of it as a balance. The American partner brought huge amounts of material, but we sometimes had the possibility to verify something through our own sources, human sources, and everybody realized that it was an advantage to share very concretely.

MODERATOR: So in other words, there will inevitably be specialization. Some information that is passed to another country can only be made effective because of particular local knowledge or access to people. The FBI is the agency that is going to talk to people in the United States, not the French Service, and vice versa. Without even planning it, there is a kind of specialization that is implied.

There will inevitably be specialization. Some information that is passed to another country can only be made effective because of particular local knowledge or access.

◆ Yes, you share because your partner can do something that you cannot, or can do it better.

MODERATOR: I wanted to ask our colleague: When you are talking about the JIC concerning Syria, is its work intended to be operational or more analytical? Is it to understand what is happening in Syria, or to deal with the consequences of what is going on in Syria?

● Yes, it is analytical, but it can be used operationally. This center is just for the armed forces. It is concerned about the terrorists or the fringe groups that are active in Syria.

MODERATOR: So for example, it watches the movement of people into Syria to join in the fighting? And possibly is stopping them from moving there?

● Yes. Collecting information from all the refugees and all the people who are coming to Jordan as visitors, actually. It is concerned about all of these people [coming from Syria].

MODERATOR: When that JIC was set up, was what would be shared clearly established?

● It is a common interest, actually. For all partners in the JIC, it is a common interest. The United States is interested in Syria. France the same, the UK the same, Jordan the same. So I think in this matter, there is no sensitive information about these things. The members have a common interest in these things. In my opinion, regarding the Syria situation, the terrorists who move there or the fringe groups, there is no sensitive information at all.

■ That is a very important point. When you start dealing with counterterrorist information, classification doesn't really matter any longer.

✕ I disagree.

■ Wait a minute. Let me finish. Classification doesn't matter in the sense that you need to move on the data, on the information. So yes, you are going to respect your classification guidelines and everything else, but what does matter is the methods that you have used to gather that data. They may need to be protected. But the data itself you can move. That is what I meant.

✕ The way that counterterrorism needs to be approached has required a change in the way that the military and law enforcement community operates. The United States may always have been much more sophisticated than the UK in this, but when we first started conducting kinetic operations against high-value targets in Iraq, it took a long time to explain to the military that there was enormous value to be had in collecting pocket litter. It took a while to get some of our specialist units to understand that the body at the end of the operation wasn't necessarily the most important thing, but the mobile phone, the computer, all the rubbish that was in the flat or the building in which the target was found—all of that stuff potentially was gold dust. That concept in itself has required the military to change and adapt the doctrine by which they operate, and it has also required a huge infrastructure

It took a long time to explain to the military that there was enormous value to be had in collecting pocket litter.

behind it to enable what is called the personnel and material exploitation phase of an operation.

When it comes to the law enforcement community, the other aspect is that the sheer volume of information that needs to be moved and needs to be shared, certainly in the UK's experience, has meant that agencies that were traditionally UK-focused, and UK-focused alone, now operate in the international arena. It started off with the [British internal] security service having a liaison officer in Paris, which was in itself a big deal for SIS [Security Intelligence Service, the British external service], because up until that point, SIS wanted to protect the liaison relationship, wanted to be the "front of house" for the whole of the UK's intelligence and law enforcement community. Just the sheer volume and scale of the exchange that was required brought the recognition that it would make sense to have a security service officer present in Paris who was liaising directly on issues that were of specific interest to the security service. We now have got to the point where we have any number of UK police counterterrorism liaison officers posted around the world to liaise with local police and to facilitate the ongoing investigations that are taking place. I believe there is a UK CT liaison officer in Jordan, for instance.

When it comes to the law enforcement community, the other aspect is the sheer volume of information that needs to be moved and needs to be shared.

● Yes, that's true.

✕ Until recently, that role was the sole preserve of SIS. We wouldn't have allowed anyone else to come anywhere near our liaison relationships. They were ours, we protected them, and we guarded them very jealously. In the real world, you can't do that anymore. So that has required the Metropolitan Police, and others—we now have immigration officers overseas, and so on—culturally to change the way they operate, and it has also brought them into this really difficult world of information sharing: what are the legal constraints, what are the operational considerations that need to be thought through, and so forth? My understanding is that the same thing has happened in the United States. There has been a similar encroachment, as it were, by NYPD [New York Police Department] and potentially others, into areas that have traditionally been the preserve of the CIA.

★ But I think counterterrorism is not a competition between countries or between services or between agencies.

✕ I agree; it shouldn't be. But the reality is different.

★ If you hide something from other agencies or from other services, this may be the most important information those other agencies need to complete the whole picture about the situation or about somebody. When you hide this information, maybe it will allow this person or this organization to [carry out an attack] someplace: maybe in your country, maybe in my country, or in other countries. If you share the information, just a small piece of information, because of other information that the other service has, then maybe it will bring the end of this terrorist attack or terrorist organization. So, in my opinion, sharing information is very important for everybody.

Information may appear in the newspaper because the police agency has a close personal relationship with the reporters.

■ You are exactly correct, but respect for the sources and methods used to obtain that information is extremely important. For example, if Jordan has a singular source within a group who is providing information about a potential attack in the United States, and you pass that information to a local police representative as opposed to the CIA or the FBI representative in Amman, that information may appear in the newspaper because the police agency has a close personal relationship with the reporters, and then your singular source is in danger.

+ That happens? [Laughter]

■ I know, it's a mystery to me, too. [Laughter] So it is very important that the agencies involved in the collection of intelligence [overseas] understand that those of us who are involved at the U.S. federal level have certain rules and regulations that we follow in regard to intelligence collection, whether counterespionage, counterintelligence, or counterterrorism, in respecting your sources of information, the CIA's sources of information. It is extremely important, and I can guarantee that American domestic law enforcement for the most part does not understand that.

⬮ American law enforcement culturally uses what they call CIs, confidential informants. Snitches. It is one criminal ratting out another criminal. There is no real respect for that person as a source. They don't protect them. I am not talking about the federal level, the FBI level. I am talking about police at the local level.

▲ First of all, U.S. law enforcement is very fragmented, decentralized, and you're dealing with different agencies and different people who don't have that experience of dealing with classified information. Also, they don't all get along, especially not the federal agencies and the state and local agencies, so the only way that [sharing information] is going to work in that case is if people get to know each other and they come to trust each other.

MODERATOR: But it seems to me that, as our colleague was saying before about Europe, one of the ways intelligence sharing can work is when there is a set of procedures that all involved agree to follow. In that case, there is no question that the personal relationship alone is what makes information sharing possible. Also, in the case of the JIC focus on Syria, our colleague didn't say, "Well, it's just because these guys got to know one another." Common interests were important to encourage sharing in that case, but procedures—not just personal relationships—seem to make sharing possible.

Procedures—not just personal relationships—seem to make sharing possible.

◗ But you have to be careful about whether the information might end up in court, because then you can't protect sources and methods.

⬮ Yes, exactly. There is an assumption that everything is going to end up in court, and therefore you don't want to risk the exposure of sources and methods.

MODERATOR: But in the case of the Syria JIC, for example, the information is not criminal, so that should not affect the exchange of information.

◆ But when you stop someone who has tried to go to Syria, he can end up in court in the future. You don't know that, but it could be happen.

✕ I am fairly confident when I say that the security classification on a piece of information makes no difference as to whether it will be disclosed in court or not. So you can put the lowest or the highest security classification on information, and if the court wants to see it, the court will see it. Also, it is very difficult to disassociate the security classification that you give a piece of intelligence from the sourcing. I am not quite sure that point has been accepted by everyone here, but if you have a very sensitive source, then you are probably going to classify whatever information you get from that very sensitive source with a very high classification.

The security classification on a piece of information makes no difference as to whether it will be disclosed in court or not.

There is also—let's be frank—a game that is played when exchanging intelligence with liaisons, with partners: your default setting is to ensure that this information that you are sharing is going to be protected in an appropriate way. Therefore, the likelihood is that you are going to put a high level of classification on it rather than a very low level of classification, even if that information actually doesn't really warrant a high level of classification. You do this also because you want to give the impression that you're giving something that is valuable rather than something they probably could have gotten themselves just from doing a bit of open source research.

● You mentioned procedures, so let me give you some ground rules for successful intelligence sharing based on my experience. First, you have to have a "round table." No one is at the head of the table. Everyone is equal. Second, every participant has to be prepared to share all the information. You can't have someone say, "I can't take that or share that." Third, any participant can opt out of an operation, depending on their rules or their abilities. You just have to acknowledge that that is going to happen. But I want to stress that you have to have a round table. You cannot have a hierarchy at that level if you want effective sharing.

You want to give the impression that you're giving something that is valuable rather than something they probably could have gotten from open source research.

◆ Another important thing is to remember that there is over-sharing. If you share everything that comes in, then you are sharing items that aren't good, and then other people won't take your information seriously. So you have to decide what is worth sharing.

✕ But if there is a threat to life, then you have to share. You can caveat it, you can say that you don't think it is credible or that you aren't sure, but you have to share it.

MODERATOR: If the procedures are important, then it's important to know whether they are being followed. How do you do that?

If the procedures are important, then it's important to know whether they are being followed. How do you do that?

✕ Trust but verify. [Laughter]

MODERATOR: Okay, but what does that mean? How do you verify?

✕ You find out from a bad experience. When a third party provides you with information that you gave someone else, for example, then you know [that the people you gave it to violated the procedures]. You also need to pay attention to how your partners are behaving. Are they professional?

◆ Yes, the reputation of a service matters. Also, countries will want to follow the procedures because if they don't, they risk losing access to information.

⛊ Countries also give aid, and in other ways try to build a relationship. Or you give training and so forth, so that gives you some leverage, and it helps reinforce the procedures, makes them common knowledge.

☂ Police forces also sometimes have officers from other departments who work with them, are integrated with them, but that is more difficult for intelligence services to do. That is anathema for an intelligence service.

⋈ It seems to me that we have been talking about two very different models that both seem to work. The first is informal, just between two countries or organizations, with few procedures or rules, where personal relationships are very important. The other is formal. A good example of this is the Joint Terrorism Task Force in the United States, usually run by the FBI, where there are more procedures and rules, and personal relationships are not as important; the sharing occurs because of the way the task force is set up.

If we are talking about sharing between countries, culture and language are important, not just procedures.

◆ In Europe, the more formal model is Interpol. The Club of Berne is less formal, maybe.

★ But if we are talking about sharing between countries, culture and language are important, not just procedures. For personal relationships, culture and language are important. ❖

NOTES

[1] Moscow rules were the unwritten rules of spycraft impressed on U.S. operatives who worked in Moscow during the Cold War. For more, see the International Spy Museum website: http://www.spymuseum.org/exhibition-experiences/argo-uncovered/moscow-rules/

[2] A Latin legal term meaning a discussion or procedure done in private.

[3] U.S. Army private Bradley Manning (aka Chelsea Elizabeth Manning) was convicted in 2013 of leaking large numbers of classified documents to the website WikiLeaks.

Preventing a Day of Terror: Lessons Learned from an Unsuccessful Terrorist Attack

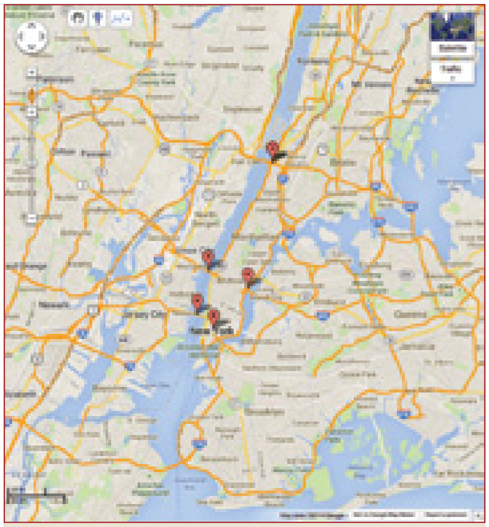
Dr. Erik J. Dahl, U.S. Naval Postgraduate School

One of the first and most successful cases of terrorism prevention in American history is also one of the least known.[1] The case involved what the U.S. government later called a conspiracy "to levy a war of urban terrorism against the United States."[2] A group of men plotted to bomb a number of targets in the New York City area, including the federal building at 26 Federal Plaza in Manhattan, which housed the New York headquarters of the Federal Bureau of Investigation (FBI); the United Nations (UN) Headquarters building; the Lincoln Tunnel and Holland Tunnel; the George Washington Bridge; and several military installations.[3] The case, known as the Day of Terror plot, ended in 1995, when 10 defendants were convicted following a nine-month trial that remains the longest and most complex international terrorism trial in American history. Federal Judge Michael B. Mukasey said the planned attacks would have caused destruction on a scale "not seen since the Civil War," and would have made the 1993 World Trade Center bombing "seem insignificant."[4]

Ten defendants were convicted following a nine-month trial that remains the longest and most complex international terrorism trial in American history.

The fundamental reason that security officials were successful in foiling the plot is clear: the FBI had an informant, Emad Salem, among the plotters. But how did this informant happen to be there? If Salem's presence had been simply good luck, then the Day of Terror plot might offer few lessons for future counterterrorism efforts. But government officials maintained that the success of the case was due to more than just luck or coincidence, but rather was the result of a long-term project to cultivate contacts among the Muslim community. "There was some damn good police work involved," said one FBI agent.[5]

The FBI was able to gather information about the Day of Terror plot from several confidential informants, but the key source of intelligence was Salem, a former Egyptian military officer who immigrated to the United States in 1987. He was a burly, bearded, enigmatic figure who worked as a private investigator, and also supported himself as a jewelry designer. During the trial in 1995, the *New York Times* described him as "a commanding presence. His bald pate is tanned and his rim of neatly trimmed black hair slicked back. He tends toward expensive suits, especially double-breasted models that cover an expanding bulk."[6] Another account described him as "handsome, muscular, meticulously well groomed, and quite the charming actor."[7] He appears to have been something of a chameleon, at times dressing in Islamic robes, at other times in jeans and T-shirts; to some he appeared to be a religious man, while to others he came across as being not religious at all.[8]


Planned bombing sites

According to press accounts, Egyptian officials said Salem had entered the Egyptian army as a private and was "pensioned out" as an officer 18 years later, although he maintained a relationship with Egyptian military intelligence. He arrived in New York City from Cairo on 25 September 1987, leaving behind a wife and two children in Egypt. According to press accounts citing U.S. government sources, he had agreed to report to the

Egyptian authorities on any contacts with Egyptian military personnel who failed to return home after receiving training in America.[9]

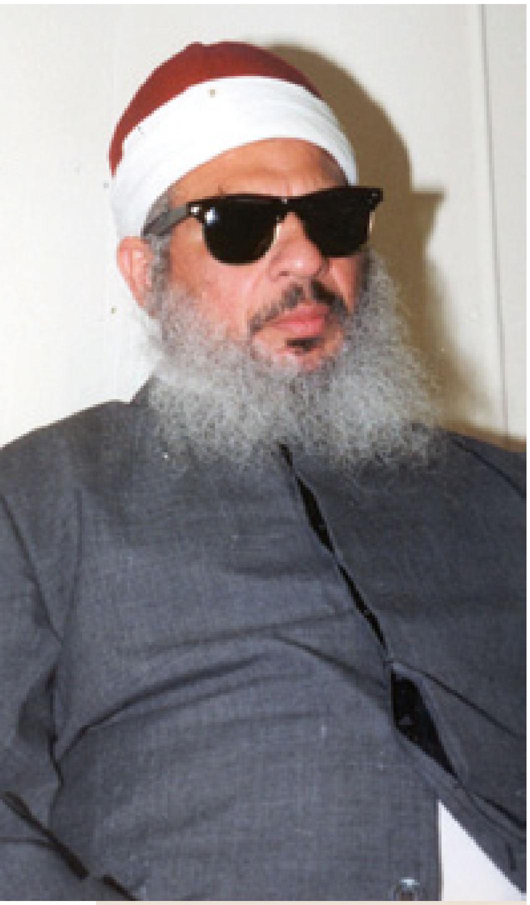
Salem told his wife he had been an intelligence officer in the Egyptian Army, and that he had been in charge of security for the president of Egypt—stories he eventually admitted were lies.

Within a week after his arrival in the United States, Salem met a woman named Barbara Rogers, a secretary at Mount Sinai Medical Center. They were married only six weeks later on 8 November 1987, in a Muslim ceremony. Salem told Rogers he had been an intelligence officer in the Egyptian Army, and that he had been in charge of security for the president of Egypt—stories he later would repeat to his FBI handlers, but which he eventually admitted were lies. In his trial testimony in 1995, he said he had actually been a radar officer in Egypt.[10]

During Salem's first several years in the United States, he worked as a security guard at several different stores in New York City, including Bergdorf Goodman and Henri Bendel. He drove a cab briefly but quit when an angry customer threw a two-cent tip in his face. His wife explained to a newspaper reporter that such an insult was difficult for a proud man to take. "You have to understand," she said. "This man had his own driver in Egypt."[11] From 1991 to early 1993, he made several trips to Egypt, including at least once with Rogers. He and Rogers separated in 1990, and he later moved into the apartment of a jewelry designer, Karen Ohltersdorf. He became an American citizen in August 1991, and soon afterward he and Rogers began divorce proceedings. In late 1991, he married Ohltersdorf, although he was still married to Rogers; he and Rogers were eventually divorced in 1993.[12]

Salem Becomes an Informant

Salem first came to the attention of the FBI in August 1991, when he was in charge of security for the Best Western Woodward hotel in Manhattan. FBI agent Nancy Floyd visited the Woodward as part of a program in which she went to second-rate hotels, hoping to find misbehaving Russian diplomats who might be willing to share secrets. Salem proved able to provide leads on just the sort of people the FBI was looking for, and Floyd later used him to gain information on Russians suspected of gun-smuggling and selling counterfeit green cards.[13]



The "Blind Sheikh," Omar Abdel Rahman

Salem indicated to Floyd that he could provide information about the "Blind Sheikh," Omar Abdel Rahman, so Floyd introduced him to John Anticev and Louie Napoli of the New York City Joint Terrorism Task Force (JTTF).[14] The New York JTTF, the first to be established in the nation, had been formed in 1980 in response to incidents of domestic terrorism. Anticev and Napoli attempted to recruit Salem to be an undercover informant, offering to match his hotel salary of $500 a week, but Salem hesitated at first, telling them he already had a full-time job.

In October 1991, Salem was injured at work when he fell off a stepladder and hit his head while trying to adjust a boiler. The manager of the hotel later said Salem's behavior changed after the accident: he began shirking work, and other employees started complaining about him. He apparently was let go from the hotel job.[15] As Salem told the story later during the trial, he found himself out of work for a while because of his injuries, and when the FBI agents came back in November to renew their offer, he decided to take them up on it.[16]

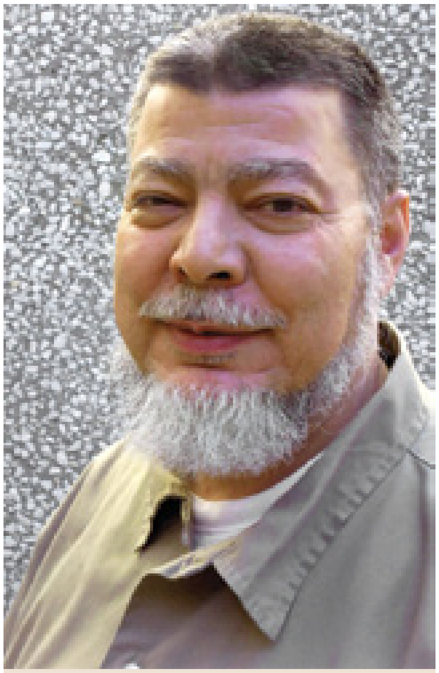
Salem insisted on one condition, however: that his identity would never be disclosed. The FBI agents told him that if he wore a wire (a hidden recording device), he might have to testify sometime down the line, so Salem refused to wear one. The agents therefore agreed to his condition, telling him they would use him purely as an intelligence asset. If surveillance was necessary to develop trial-worthy evidence, other agents would move in to conduct it.[17] This condition would later play a critical role in Salem's being terminated as an informant in 1992.

The Nosair Trial

Soon after they brought him onto the government payroll, Salem's FBI handlers approached him with a request. The trial of El Sayyid Nosair, suspected in the murder of Rabbi Meir Kahane, was beginning in New York, and Nosair had developed quite a large circle of admirers and supporters among radical Islamists and others. Would Salem be able to infiltrate the group of followers around Nosair, and help the FBI keep tabs on what they were up to? Salem agreed, and he quickly turned out to be very good at undercover work. A source told journalist Peter Lance, "We had given him six weeks to get under [infiltrate the group]. He did it in two days."[18]

"We had given him six weeks to get under [infiltrate the group]. He did it in two days."

Salem began to attend the trial and visit mosques, and he befriended Nosair's cousin, Ibrahim El-Gabrowny. El-Gabrowny, a vocal supporter of Nosair, headed a fundraising committee and called for support for Nosair from mosques and Muslim associations. At one point during the trial, El-Gabrowny introduced Salem to Nosair, describing Salem as "a new member in the family."[19] Soon El-Gabrowny told Salem that he and some friends were assembling materials for a bomb. He was vague about what their target might be, but Salem thought he sounded serious, and when El-Gabrowny asked him to join the group, he accepted.[20]



El Sayyid Nosair

Before the Nosair trial ended, Salem was invited for dinner at El-Gabrowny's house. During dinner, El-Gabrowny indicated that he was concerned about being bugged by the FBI, so he turned up the television and then began to discuss the building of high-powered explosives. El-Gabrowny asked Salem if he knew how to make bombs, and Salem said that he did, because of his army experience in Egypt.[21] By early 1992, Sheikh Abdel Rahman, the spiritual leader of the group planning to carry out the attacks, had also welcomed Salem into the group, and Salem even traveled to Detroit with Abdel Rahman and others to attend a conference on the Islamic economy.[22]

"Don't Call Me When the Bombs Go Off"

By June 1992, Salem still had not learned what the group was planning to do, but he had been told that the operation would involve 12 bombs and that guns would be needed in case the participants encountered police.[23] In early July 1992, however, a dispute developed between Salem and the FBI that would result in Salem being released as an undercover informant.

Salem still had not learned what the group was planning to do, but he had been told that the operation would involve 12 bombs.

The problem arose when Agents Napoli and Anticev, who were in charge of the Salem operation, gave their superiors a briefing on the progress they had made, and were told it was now time to build a case that could be taken to court. In order to do that, Salem would have to wear a wire, which he had previously said he would never do. At about the same time, another problem arose for Salem: the FBI asked him to take a polygraph examination, apparently because they were suspicious he might be working for Egyptian intelligence. He was given three tests during the spring and summer of 1992, and although the agent who administered the tests believed he had passed, when experts in Washington reviewed the results, they determined he had lied on at least one of the tests.[24] In June or July 1992, Salem went to the FBI's New York City headquarters to meet with senior FBI officials Carson Dunbar and John Crouthamel. They told Salem he would have to wear a wire and be prepared to testify in court about the plot that was developing, but he continued to refuse.[25]

In July 1992, Salem was dismissed as an informant, but he continued to get his weekly salary of $500 to tide him over until he found another job. To explain his disappearance to the conspirators, Salem told El-Gabrowny he needed to go to Spain to take care of a problem in his jewelry business.[26] Nancy Floyd continued to meet with him at a Subway sandwich shop near the FBI New York office to give him the cash. Salem warned her that something was going on with Sheikh Abdel Rahman's cell, and told her the FBI should be keeping track of the cell members.[27]

As Salem left the Subway shop, he turned toward Floyd and said, "Don't call me when the bombs go off."

Floyd had her last meeting with Salem in early October 1992, and again he warned her that the FBI should be worried about what was going on. She told him she had been transferred to another area, and was no longer involved in the case. As he left the Subway shop, he turned toward her and said, "Don't call me when the bombs go off."[28]

After the World Trade Center Bombing, Back on the Payroll

On the afternoon of the day the World Trade Center was bombed, 26 February 1993, Salem called Floyd in a panic from a room at St. Clare's Hospital in Manhattan, where he had been admitted for an inner-ear infection. He told her he was worried that no one had listened to him, and that they might now think he had been involved. Floyd told Salem the FBI had accomplished all it could with the information he had given them, but she would talk to her supervisor to see what could be done for him. She called her boss in the National Security Division (now called the Counterintelligence Division), who said that it would be up to the Terrorism section to handle Salem if they wanted to. So Floyd called Napoli and told him that Salem wanted to talk.[29]

World Trade Center bombing aftermath

At 1:00 a.m. that same night, Napoli and Anticev were in a meeting in the office of the FBI's assistant director in charge of the New York field office. Running the meeting was Mary Jo White, who had recently been appointed U.S. attorney

for Manhattan. Napoli mentioned that they had an asset "that was very close to these people," and told White about Salem. White said she wanted to meet him, but Napoli answered, "Well, we were paying him like five hundred a week. This time, you know, considering what's happened, he's probably gonna want—a million dollars." To which White answered, "I don't give a damn *what* he wants. If he can deliver, give it to him."[30]

After weeks of negotiation between Salem and lawyers and agents representing the FBI, it was agreed that the government would pay Salem over one million dollars to once again become an undercover source and serve as a witness at any future trial. They also guaranteed that he would be put into the witness protection program afterwards. It didn't take long for the decision to rehire Salem to pay off. In April 1993, Salem told Detective Louie Napoli that he had been approached by Abdel Rahman's interpreter, Siddig Ibrahim Siddig Ali, who told Salem that he was planning a series of simultaneous bombings against four major New York City landmarks: the Lincoln and Holland tunnels, the UN, and 26 Federal Plaza, where the New York offices of the FBI were located.[31]

The government would pay Salem over one million dollars to once again become an undercover source and serve as a witness at any future trial.

Although the FBI was already involved in the massive investigation—codenamed TRADEBOM—into the World Trade Center attack, an investigation was now begun into the new plot, dubbed TERRSTOP. The FBI's Special Operations Group outfitted Salem with an array of listening devices, including two recorders in the trunk of his car and a specially designed pair of pants with an electronic chip in them that recorded voices. Salem got back in touch with Siddig Ali and began providing supplies to the conspirators, including a video camera for surveillance and a van that the FBI had wired for sound.[32]

The investigation was almost exposed in May, when Siddig Ali confided to Salem that there were additional plans to assassinate several political figures sympathetic to Israel, including U.S. Senator Alfonse D'Amato of New York and Brooklyn Assemblyman Dov Hikind. Authorities informed the officials about the threats against them but stressed how sensitive the information was: because only a few of the conspirators knew about these plans, it was felt that Salem might be exposed as the source if the information on the threats became public.

Despite the FBI's efforts, however, the threat to Hikind leaked to the press, and on 25 May, the *New York Post* ran headlines announcing this new, second terrorist plot. Salem believed his cover had been blown. He later told his ex-wife, Barbara Rogers, that when Siddig Ali heard the news, he lined up Salem and several others who knew about the plot against Hikind and put a revolver to each man's head. "Allah is going to tell us who the traitor is," Siddig Ali said.[33] But luckily for Salem and the FBI, when no one confessed, Siddig Ali concluded it might have been a coincidence, or that the FBI could have gotten its information through some sort of surveillance of the group.[34]

Siddig Ali put a revolver to each man's head and said, "Allah is going to tell us who the traitor is."

The FBI and the JTTF continued monitoring the plot until the group had begun to actually mix the explosives that would go into their bombs, on the night of 23–24 June 1993. It was then that the safe house was raided and the Day of Terror plot was foiled.

At some points, FBI officials appeared to encourage Salem to risk pushing the cell's members to make incriminating statements and possibly entrap themselves.

For Salem, the stress involved in living a double life as a terrorist conspirator and government informant brought on an asthma attack, and after the FBI raided the bomb factory, he ended up in the emergency room of Mount Sinai Hospital, seeking treatment under a false name.[35] But he recovered, and prospered from his role in the case. At the 1995 trial, it was revealed that the government had agreed to pay Salem a total of $1,056,200 for his work as an informer, and until he received that payment, he was given $7,000 a month. Before that, his payment as a government informant had been $500 a week, plus expenses. The federal witness protection program, which reportedly moved him 14 times from the time he entered it in June 1993 until the trial, also paid him $2,600 per month for living expenses.[36]

The Case Goes to Trial

Soon after the 24 June arrests, it was discovered that the terrorist conspirators were not the only ones whom Salem, the informant, had been secretly spying on and tape recording. He had also been making secret recordings of his conversations with government agents, going back at least to the Nosair trial. He apparently wanted the tapes as an insurance policy in case the government backed away from its promises of money and protection. The "bootleg" tapes came to light when Salem hurriedly left his West Side Manhattan apartment after the Day of Terror plot was broken up, leaving behind cassettes of the secret recordings. Judge Michael Mukasey allowed the transcripts of the hundreds of hours of tape to be given to the defense lawyers, but ordered that they be kept secret. The *New York Times* obtained a copy of the transcripts nevertheless, and their existence became public. Eventually the transcripts of the tapes were introduced into evidence during the trial.[37]

The tapes revealed some new details about the terrorist plot. Salem could be heard saying that the conspirators also discussed bombing Grand Central Terminal, the Empire State Building, and Times Square.[38] But more significantly, they showed how sensitive and troubled the relationship was between Salem and his FBI handlers. At some points, FBI officials appeared to encourage Salem to risk pushing the cell's members to make incriminating statements and possibly entrap themselves.

The trial opened in New York federal court in January 1995, and ended nine months later, after the jury had heard testimony from more than 200 witnesses and listened to more than 100 hours of the tape recordings that Salem had secretly made. The jury deliberated for seven days before pronouncing all 10 defendants guilty of attempting to carry out a campaign of terrorism.

Conclusion

Terrorism was seen as a primarily international problem, backed by hostile states such as Libya.

What might have been America's most devastating terrorist attack prior to 9/11 was foiled because an FBI informant provided authorities with precise, tactical-level intelligence on the plot as it was developing. But the history of this case demonstrates the obstacles that law enforcement agencies face in obtaining and using this type of human intelligence.

The FBI and the New York JTTF had originally recruited Emad Salem as a confidential informant in the fall of 1991, but senior officials in the FBI and the JTTF were not receptive to the information he was providing. This was in part because they did not trust Salem's motives. In addition, they were reflecting the conventional assessment of the terrorist threat in the United States at that time. Terrorism was seen as a primarily international problem, backed by hostile states such as Libya; although officials recognized a limited domestic threat from disgruntled or deranged individuals, they saw domestic terrorism as much less threatening.

This case also demonstrated several techniques that have been shown to be critical today in the fight against terrorism. One technique is the use of a joint terrorism task force, linking the FBI, local law enforcement, and other government agencies together in a cooperative effort.[39] A second technique is electronic surveillance: much of the evidence introduced in the case came from secret wiretaps, some of which were authorized by the Foreign Intelligence Surveillance Court.[40]

The Day of Terror plot demonstrated the utility of taking a slow, careful approach to terrorism investigations.

In addition, the Day of Terror plot demonstrated the utility of taking a slow, careful approach to terrorism investigations: letting plots go forward long enough so that the full scope of the conspiracy can be determined and as many of the plotters can be caught as possible. "We had to let the information develop," said a former FBI assistant director who had been involved in the case. "Taking them off the street at an early stage of the investigation, I don't believe would have afforded us the opportunity to discover and resolve the intent to blow up the tunnels."[41]

This case raised a number of issues that continue to be debated today concerning the prosecution of terrorist suspects, such as how to balance the need for security and civil liberties in terrorist investigations, and how to balance the need for physical security during the trial with the right of the accused to an open and public trial.[42] The case also was an early example of how terrorists and their supporters make use of modern information technology: throughout the trial, supporters of Abdel Rahman and the other defendants used the internet to solicit funds for their defense.[43]

The Day of Terror plot provided an early model for how a group of loosely affiliated extremists can come together, train, plan, and very nearly carry out a terrorist attack.

Finally, the Day of Terror plot remains useful for study today because it provided an early model for how a group of loosely affiliated extremists can come together, train, plan, and very nearly carry out a terrorist attack intended to inflict wide-scale death and destruction. The conspiracy proceeded through a number of distinct stages, including member recruitment, group paramilitary training, target selection, and weapons acquisition. Similar patterns can be seen in a number of terrorist plots that have been foiled since then, suggesting that such a template may prove useful in analyzing and preventing complex terrorist plots in the future. ❖

ABOUT THE AUTHOR

Dr. Erik J. Dahl is an assistant professor of National Security Affairs at the U.S. Naval Postgraduate School.

NOTES

[1] This article draws upon my book, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, D.C.: Georgetown University Press, 2013), and a paper presented at the International Studies Association annual conference in Montreal, Canada, in March 2011. The views presented here are those of the author and do not represent the official position of the U.S. Naval Postgraduate School, the U.S. Department of the Navy, or the U.S. government.

[2] Mary B.W. Tabor, "Specter of Terror: U.S. Indicts Egyptian Cleric as Head of Group Plotting 'War of Urban Terrorism,'" *New York Times*, 26 August 1993.

[3] United States v. Rahman (Indictment), S5 93 Cr. 181 (MBM) (S.D.N.Y. 1994), 6. The case is sometimes referred to as the "landmarks" or the "monuments" plot. The primary sources of information for this article are the records and transcripts resulting from the initial trial of the plotters, *United States v. Rahman,* U.S. District Court, Southern District of New York, held in 1995; and the appeal made by the defendants to the 2nd U.S. Circuit Court of Appeals, with a decision handed down in August 1999, 189 F.3d 88.

[4] Joseph P. Fried, "Sheik Sentenced to Life in Prison in Bombing Plot," *New York Times*, 18 January 1996.

[5] George J. Church, "The Terror Within," *Time,* 5 July 1993.

[6] Neil MacFarquhar, "In Bombing Trial, a Deluge of Details," *New York Times*, 19 March 1995.

[7] Jim Dwyer, *Two Seconds under the World: Terror Comes to America: The Conspiracy behind the World Trade Center Bombing* (New York: Crown Publishers, 1994), 183.

[8] Alison Mitchell, "Official Recalls Delay in Using Informer," *New York Times*, 16 July 1993; Ralph Blumenthal, "Tapes in Bombing Plot Show Informer and F.B.I. at Odds," *New York Times*, 27 October 1993. Some accounts say Salem first arrived in the United States in 1988, but most accounts agree it was 1987.

[9] Ralph Blumenthal, "The Informer: Tangled Ties and Tales of F.B.I. Messenger," *New York Times*, 9 January 1994; Blumenthal, "Tapes in Bombing Plot."

[10] United States v. Rahman, trial testimony, 7 March 1995: 4584–85; Blumenthal, "The Informer"; Mitchell, "Official Recalls Delay." On Salem's admission to lying about his background, see *Rahman*, trial testimony, 7 March 1995: 4575; and James C. McKinley Jr., "Key Witness in Bomb-Plot Trial Admits Lying about His Exploits," *New York Times*, 8 March 1995.

[11] Dahl, *Intelligence and Surprise Attack*, 120.

[12] Blumenthal, "The Informer."

[13] Peter Lance, *1000 Years for Revenge: International Terrorism and the FBI—The Untold Story* (New York: Regan Books, 2003), 53. Salem testified at the trial that Floyd first came to the hotel in the spring of 1991 (not August), but he also said he was not very good at remembering dates; *Rahman*, trial testimony, 7 March 1995: 4588–609.

[14] On the New York Joint Terrorism Task Force, see National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: Norton, 2004), 81–82; Mary Jo White, "Prosecuting Terrorism in New York," *Middle East Quarterly* 8, no. 2 (Spring 2001): http://www.meforum.org/25/prosecuting-terrorism-in-new-york

[15] Blumenthal, "The Informer."

[16] *Rahman*, trial testimony, 7 March 1995: 4609; McKinley, "Key Witness in Bomb-Plot Trial."

[17] Lance, *1000 Years for Revenge*, 58–59.

[18] Ibid., 60. See also *Rahman*, trial testimony, 7 March 1995: 4609–11.

[19] United States v. Rahman, 189 F.3d 88 (S.D.N.Y. 1999); *Rahman*, trial testimony, 7 March 1995: 4713–15.

[20] This period is discussed in *Rahman*, trial testimony, 7 March 1995: 4611–22, 4874–85, 6094–95. See also John Miller, Michael Stone, and Chris Mitchell, *The Cell: Inside the 9/11 Plot, and Why the FBI and CIA Failed to Stop It* (New York: Hyperion, 2002), 70; United States v. Rahman (Indictment), S5 93 Cr. 181 (MBM) (S.D.N.Y. 1994), 9.

[21] *Rahman*, trial testimony, 7 March 1995: 4710–13.

[22] *Rahman*, 189 F.3d 88; Lance, *1000 Years for Revenge*, 66–67.

[23] *Rahman*, 189 F.3d 88; Miller, Stone, and Mitchell, *The Cell*, 73.

[24] James C. McKinley Jr., "Witness in Bombing Plot Once Failed Lie-Detector Tests," *New York Times*, 3 March 1995.

[25] United States v. Rahman, trial testimony, 13 March 1995: 4939–44; Miller, Stone, and Mitchell, *The Cell*, 74–75, 85–93.

[26] *Rahman*, 189 F.3d 88.

[27] Lance, *1000 Years for Revenge*, 102–3.

[28] Ibid., 104.

[29] *Rahman*, trial testimony, 13 March 1995: 4998–5004; Lance, *1000 Years for Revenge*, 134–36.

[30] Lance, *1000 Years for Revenge*, 136. This episode is also described in a 9/11 Commission *Memorandum for the Record* of its staff interview with NYPD Detective Louis Napoli, 4 September 2003: http://media.nara.gov/9-11/MFR/t-0148-911MFR-00390.pdf

[31] Lance, *1000 Years for Revenge*, 151–52; Miller, Stone, and Mitchell, *The Cell*, 113.

[32] Lance, *1000 Years for Revenge*, 152; Miller, Stone, and Mitchell, *The Cell*, 114.

[33] Dahl, *Intelligence and Surprise Attack*, 123.

[34] Miller, Stone, and Mitchell, *The Cell*, 115–16; Dwyer, *Two Seconds*, 217–18.

[35] Blumenthal, "The Informer."

[36] United States v. Rahman, trial testimony, 7 March 1995: 4579–80; MacFarquhar, "In Bombing Trial."

[37] Blumenthal, "Tapes in Bombing Plot." Salem discussed his decision to make tape recordings in his testimony on 13 March 1995.

[38] Blumenthal, "Tapes in Bombing Plot"; Blumenthal, "The Informer."

[39] *Foreign Terrorists in America: Five Years after the World Trade Center: Hearing Before the Subcommittee on Technology, Terrorism, and Government Information, of the Committee on the Judiciary*, 105th Cong. 41 (1998) (testimony of Dale Watson).

[40] The U.S. Foreign Intelligence Surveillance Court, also called the FISA Court after the Foreign Intelligence Surveillance Act that created it, is a special court of 11 (originally seven) appointed judges who review applications for warrants from law enforcement agencies that relate to national security investigations.

[41] Jim McGee, "Ex-FBI Officials Criticize Tactics on Terrorism," *Washington Post*, 28 November 2001.

[42] Judge Mukasey received death threats as a result of the case, and U.S. marshals were posted outside his chambers and at his New York apartment. He was transported in an armored limousine with a chase car. Susan Schmidt and Dafna Linzer, "Attorney General Nominee Made His Name with Terror Cases," *Washington Post,* 11 October 2007.

[43] On the use of the internet, see *Foreign Terrorists in America* (1998).

Annotated Bibliography

All of the articles in the bibliography are available either on the Web or through the Dudley Knox Library at the U.S. Naval Postgraduate School. In some cases, we have provided URLs.

Andradé, Dale. *Ashes to Ashes: The Phoenix Program and the Vietnam War.* Lexington, Mass.: D. C. Heath, 1990.

Perhaps the best account of the program that targeted the Vietcong, Andradé's book describes the importance of intelligence in the targeting, as well as various problems in the program. Pages 188–91 of the book describe an operation quite similar to those developed to target al Qaeda in Iraq.

Berdal, Mats. "The 'New Wars' Thesis Revisited." In *The Changing Character of War,* edited by Hew Strachan and Sibylle Scheipers, 109–33. New York: Oxford University Press, 2011.

A critical review of the idea that recent civil wars and ethnic conflict are a new kind of war, Berdal's article describes various ways in which non-state actors are taking advantage of globalization to carry on their activities. His account suggests an array of intelligence requirements.

Betz, David J., and Tim Stevens. *Cyberspace and the State.* New York: Routledge, 2011.

A brief review of the effect of the information revolution on state power, and thus an analysis of how that revolution is changing the competition between states and non-state actors.

Collins, Liam. "The Abbottabad Documents: Bin Ladin's Security Measures." *CTC Sentinel* 5, no. 5 (May 2012): 1–4: http://www.ctc.usma.edu/wp-content/uploads/2012/05/CTCSentinel-Vol5Iss51.pdf

In this article, Collins explains how Osama bin Laden managed for 10 years to frustrate those trying to find him.

Crenshaw, Martha. "'Old' vs. 'New' Terrorism." In *Explaining Terrorism: Causes, Processes, and Consequences,* 51–66. New York: Routledge, 2011.

Reviewing the claims and evidence offered by those who believe that terrorism has changed, Crenshaw concludes that "a close look at the objectives, methods, and organizational structures of what is said to be 'new' and what is said to be 'old' terrorism reveals numerous similarities rather than firm differences. It cannot really be said that there are two fundamental types of terrorism."

Defense Science Board. *Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations.* Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2011: http://www.acq.osd.mil/dsb/reports/ADA543575.pdf

This report by the Defense Science Board is a comprehensive effort to determine "appropriate intelligence capabilities to assess insurgencies, understand a population in their environment, and support COIN operations."

Felix, Christopher [James McCargar]. *A Short Course in the Secret War.* 4th ed. New York: Madison Books, 2001.

Originally published in 1963 and now a bit dated, Felix's account of espionage is still probably the best available. Part 1, chapters 2 and 3 are particularly good accounts of the character of espionage and the heart of the business, the relationship between the intelligence officer and the agent. Felix was involved in covert political action in Eastern Europe after World War II.

Flynn, Michael T., Matt Pottinger, and Paul D. Batchelor. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.* Washington, D.C.: Center for a New American Security, 2010: http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf

Major General Flynn (USA), Captain Pottinger (USMC), and Batchelor describe the problems with military intelligence in Afghanistan and suggest some ways to fix them there and in similar future conflicts. One unresolved issue is whether the structures of military intelligence, even with the modifications recommended by Flynn and his colleagues, will suffice to give commanders on one-year tours the situational awareness they need.

International Institute for Strategic Studies. *Strategic Survey 2012: The Annual Review of World Affairs.* London: International Institute for Strategic Studies, 2012.

The first section of chapter 2 of the survey, "Intelligence Agencies and the Cyber World," analyzes how the information revolution affects intelligence organizations and activities. In keeping with the purpose of the survey, the section focuses on strategic implications.

Kitson, Frank. "Insurgency Part 1: Tactics, The Handling of Information." In *Low Intensity Operations: Subversion, Insurgency, Peace-keeping.* Harrisburg, Pa.: Stackpole Books, 1971.

Kitson's account in this chapter from his book is the *locus classicus* for the claim that irregular warfare is a game of hiders and finders. Kitson also shows the importance of deductive methods in identifying terrorists, in both rural and urban settings. Key to this process is understanding "patterns of life," a term Kitson uses, and developing contact information from those patterns. Written before the development of modern information technology, Kitson's approach is low-tech. He emphasizes the importance of the operational commander's dual role as the chief intelligence officer. This is a point missing in Flynn's understanding of the role of intelligence.

Mobley, Blake W. *Terrorism and Counterintelligence: How Terrorist Groups Elude Detection.* New York: Columbia University Press, 2012.

A comprehensive review of how terrorist organizations try to protect themselves. Examining the Provisional Irish Republican Army, Black September, al Qaeda, and Egyptian Islamic Jihad, Mobley argues that a centralized ("hierarchical") organizational structure, popular support, and a safe haven are most important for the security of terrorist organizations. He describes various ways that intelligence services have exploited the inevitable vulnerabilities of their terrorist opponents.

Schiattareggia, M. H. [pseud.]. "Counterintelligence in Counterguerrilla Operations." *Studies in Intelligence* 57, no. 2 (June 2013): 39–63: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-57-no-2/pdfs/Archive-CIandCOIN-1962.pdf

Written by a CIA operations officer and originally published in 1962, this article remains a useful discussion of various aspects of intelligence operations in irregular warfare. The author includes an appendix on guerrilla intelligence activities based on the writings of Mao, Che Guevara, and captured documents.

THE CTAP INTERVIEW

Peter Berg, Director of *Lone Survivor*

Interviewed by Rebecca Lorentz and Elizabeth Skinner, U.S. Naval Postgraduate School

This interview is taken from the collection of the Combating Terrorism Archive Project (CTAP).[1] On 12 December 2013, writer and director Peter Berg came to Monterey, California, for a special pre-release screening of his new film, *Lone Survivor*. Based on the book of the same title by Marcus Luttrell, the film depicts Operation Red Wings (June 2005), in which Luttrell and three other members of SEAL Team Ten were dropped into the mountains near a village on the Afghanistan-Pakistan border.[2] Their mission was to capture or kill a Taliban leader who was responsible for the deaths of a number of Marines. Shortly after they landed, the team was discovered by three goatherds: an older man and two boys. The SEALs' decision about what to do with these villagers and the aftermath of that decision are at the heart of Luttrell's book and Berg's film. After the screening, Mr. Berg sat down for an interview with Rebecca Lorentz of CTAP and Elizabeth Skinner of *CTX*.[3]

Spoiler alert: This discussion covers many of *Lone Survivor*'s major plot points, so if you intend to see the film, you might want to save this article to read afterward.

REBECCA LORENTZ: Thank you, Mr. Berg, for agreeing to do an interview with us. We just finished watching a screening of *Lone Survivor*. Can you explain what you were most nervous about when you got ready to screen the movie for the public?

We were very conscious that we had a very opinionated and involved audience that was going to see this film.

PETER BERG: I think I was probably most nervous about the fact that we had a unique audience. We knew that part of our audience base for *Lone Survivor* would be the families, moms, and dads of the 19 soldiers who were killed: the men's children, their brothers and sisters, their widows. I knew they were going to see the film, and I wanted to make sure that they felt we had paid our respects, that we had done our work, that we had honored their sons. The other challenge was with the Special Operations community as a whole. I knew that Navy SEALs and Green Berets and PJs [pararescue jumpers] from the Air Force, Force Recon from the Marines, Delta, SEAL Team Six—we knew that these guys were all going to see the film, and they were going to have very strong opinions. If we were not accurate, if we hadn't done our work in advance and made a real effort to understand how that SEAL community operates, we would be ripped apart by that part of the audience. So we were very

conscious that we had a very opinionated and involved audience that was going to see this film.

LORENTZ: When you began to make the film, what surprised you the most about delving into the military operations?

They didn't always get along; but when it came time to work, the level of professionalism and commitment and self-reliance was kind of mind-blowing to me.

BERG: That is a good question. Everything was new to me as I started to research the SEAL community. I spent a month in Iraq, and I was able to embed in the Foxtrot Platoon in SEAL Team Five and see the closeness of the men, the brotherhood, the bond between men of different shapes and sizes and races and religion. The unity among men and the singular focus they have, the willingness to protect each other and the love they have for each other was something that I had never seen before. You know, these are guys who have problems with each other, they would argue. They didn't always get along; but when it came time to work, the level of professionalism and commitment and self-reliance was kind of mind-blowing to me.

LORENTZ: I have got to say, we just watched about a two-hour film, and it was really intense. My heart is still beating. How have you recovered from doing that film over four years, from that intensity?

The decision that Mike Murphy made to let those goatherds go and spare their lives—that was the core of why I wanted to do this film.

BERG: It has been a really unique, special experience for all of us involved in the film. Again, these are 19 men who died, and we have come to know their families, we have come to know their friends, we have come to know their coworkers within the SEALs. It has been very emotional for all of us, and movies like this don't come along that often. I can tell you I am very emotionally connected to this film, very close to Marcus Luttrell and also the SEAL community in general. It is going to take some time to let this go, I mean, for me to find another project that will mean as much to me as this one has.

LORENTZ: Yes. There is the moment in the film when the SEALs have the goatherds, and they have to make a decision about what to do. How heavy do you feel that moment weighs with regard to ethical decision making?

BERG: The decision that Mike Murphy made to let those goatherds go and spare their lives—that was the core of why I wanted to do this film. I think it shines a very bright light on what we are asking our Special Operations soldiers to do today, and how outside of the box their thinking needs to be, how situationally aware they need to be, how prepared for the unimaginable they need to be. That captures so much about the story. Special Ops personnel are trained to do almost anything. Everything that happens to them in the field is new. It is not in books, and there is no manual. I could certainly form an argument as to why they probably should have killed those goatherds, and if I did, I would now have 19 Special Operations soldiers still alive. Trying to imagine what Mike Murphy was thinking, and what was going through his mind with zero information—that's out of my pay grade.

For a month, I sat with Luttrell and ran through that gunfight beat by beat. Those cliff jumps, tree by tree. Those injuries, bullet by bullet.

ELIZABETH SKINNER: Did the actors react emotionally, and how did you work with them to get them into that intensity?

BERG: We had Marcus Luttrell come to the set about a month before shooting. He came with eight Navy SEALs—four current and four who were retired—and we set up a training facility in Albuquerque, New Mexico. For a month, the actors lived with Marcus and eight SEALs, all of whom knew the guys who were killed. That was a very formative experience for those actors. Prior to that, they had met the families of the SEALs they were playing—so Taylor Kitsch spent time with the Murphys, and so forth. I tried to immerse the actors into the families as much as I could and then into the SEAL teams as much as I could. They got it. It is impossible to read Marcus's book, spend time with the SEAL families, and spend time with the SEALs, and not get very emotionally connected. So those actors were very, very invested in what they were doing.

SKINNER: You were creating the illusion of extreme violence and this combat experience that none of you who were involved in the filmmaking had actually experienced. You were involved with the SEALs to get a sense of how that

felt, but as a director, you tried to create a reality and present it to people who have been through it. How did you gain that perspective on how that violence should look?

BERG: Good question. In the book, Marcus described that gunfight in vivid and graphic detail. It was a five-hour gunfight in reality, and the first thing I did was really analyze what Marcus had written. I invited him to my house, and for a month, I sat with Luttrell and ran through that gunfight beat by beat. Those cliff jumps, tree by tree. Those injuries, bullet by bullet. I sat with one of the men's fathers, and he read me the autopsy report of every injury: every bone, ankle, knee, thigh, groin, stomach, throat. I was trying to educate myself and get as complete a knowledge as I could. I tried to be as comprehensive and understanding as I could have been about the reality of that gunfight.

I was certainly aware that these types of screenings would occur, and it probably made me work a little harder to at least be able to justify my choices.

We tried to be very specific about every gunshot—where someone was getting hurt. Every hit, every injury. The makeup guys were very specific about what these injuries would look like, the sound guys about what they would sound like. We tried to go into the detail of that violence and not just throw it at the audience.

LORENTZ: Is it difficult to direct a movie that has such a varied audience? You know that the Special Forces will see it, but you know American citizens will see it who have nothing to do with the war.

BERG: Directing any movie is difficult. It is always tricky to figure out who is going to like it and who is not going to like it. You know, generally, I am willing to kind of take the Serenity Prayer and say there is only so much I can control.[4] But in making *Lone Survivor*, knowing I was going to have to see each mother again when this film was over, knowing that I was going to have to see Marcus Luttrell again when this film was over. . . . Knowing that I am going to come to places like this [Monterey]—this is a very unique audience. To have elite members of Special Operations Forces from all around the world, warriors and families of warriors and academic soldiers—people who are going to look at this with a very unique and critical eye—it didn't make it harder to make the movie, but I was certainly aware that these types of screenings would occur, and it probably made me work a little harder to at least be able to justify my choices. It made me want to do things like go to Iraq for a month and live with the SEAL platoon, so that at the end of the day, if a Navy SEAL comes up to me—which has happened many times—and says, "Why did you make this choice?" I can have an answer.

SKINNER: Do you consider this an anti-war movie?

I think we as citizens have to look at the reality of what it means to send soldiers to war.

BERG: People have asked me if I am pro-war or anti-war. I am anti-war. I mean, who in their right mind would be pro-war? I have had friends who have died. I have been to many military funerals. I have enough respect and appreciation for what we ask these men and women to do.

These men will fight, and these men will die very, very painful and bloody and gruesome deaths. I think it is important for any citizen—everybody should understand what the costs are. If we are at war where people are dying, we need to have an opinion, whatever that opinion is. If you are supporting it and believe the cause is right, you then support it and make sure that our soldiers come back home, and support them. If you don't support it and you think it is wrong, then do something about that, too. For me, it is not pro-war or anti-war. I think we as citizens have to look at the reality of what it means to send soldiers to war. ❖

ABOUT THE INTERVIEWEE

Peter Berg is an actor, writer, and director who has been working in Hollywood for more than 20 years. He wrote and directed the feature film *Friday Night Lights* (2004) and the award-winning TV series of the same title.

Rebecca Lorentz is the manager of CTAP.
Elizabeth Skinner is the managing editor of *CTX*.

NOTES

1 The Combating Terrorism Archive Project aims to collect and archive knowledge on strategy, operations, and tactics used by military and other security personnel from around the world in the twenty-first-century fight against global terrorism. Collectively, the individual interviews that CTAP conducts will create an oral history archive of knowledge and experience in counterterrorism for the benefit of the CT community now and in the future.

2 The other members were team leader Mike Murphy, communications officer Danny Dietz, and navigation specialist Matt Axelson. Luttrell was the team's medic.

3 This interview was edited for length and clarity. Every effort was made to ensure that the meaning and intention of the participants were not altered in any way. The ideas and opinions of all participants are theirs alone and do not represent the official positions of the U.S. Naval Postgraduate School, the U.S. Department of Defense, the U.S. government, or any other official entity.

4 A common variant of the Serenity Prayer by Reinhold Niebuhr begins, "God grant me the serenity to accept the things I cannot change,/ courage to change the things I can,/ and wisdom to know the difference."

Navy SEALs operating in Afghanistan in support of Operation Enduring Freedom. (L-R) Sonar Technician (Surface) 2nd Class Matthew G. Axelson, of Cupertino, California; Senior Chief Information Systems Technician Daniel R. Healy, of Exeter, New Hampshire; Quartermaster 2nd Class James Suh, of Deerfield Beach, Florida; Hospital Corpsman 2nd Class Marcus Luttrell; Machinist's Mate 2nd Class Eric S. Patton, of Boulder City, Nevada; and Lt. Michael P. Murphy, of Patchogue, New York pose in Afghanistan. With the exception of Luttrell, all were killed June 28, 2005, by enemy forces while supporting Operation Red Wings.

THE CTAP INTERVIEW

Part Two: A Roundtable Discussion of *Lone Survivor*

This interview is taken from the collection of the Combating Terrorism Archive Project (CTAP).[1] On 12 December 2013, writer and director Peter Berg came to Monterey, California, for a special pre-release screening of his new film, *Lone Survivor*.[2] A few days after the screening, MAJ Patrick Collins, U.S. Army Special Forces; LTC Gabor Santa, Hungarian Army Special Forces; and CDR Brian O'Lavin, U.S. Navy SEALs, met to discuss the film with Rebecca Lorentz of CTAP and Elizabeth Skinner of *CTX*.[3]

Spoiler alert: This discussion covers most of *Lone Survivor*'s major plot points, so if you intend to see the film, you might want to save this article to read afterward.

BRIAN O'LAVIN: Last week we watched a private screening of the movie *Lone Survivor*, so we've gotten together now to discuss some finer points of the movie. First off, going around the room, what are your initial thoughts about the movie: did you like it, did you not like it? Were there aspects that you thought were well done and aspects you thought maybe could have been improved on, or any kind of general comments?

PATRICK COLLINS: I thought it was a good movie. It was definitely very action-packed and entertaining. It doesn't follow the book exactly, but it definitely is very close. I know during the gunfight scene, the writers had a lot of advice from Marcus Luttrell [the author of the book *Lone Survivor*, from which the *Lone Survivor* film is adapted], so I am just going to assume that was all pretty accurate.

My military occupation specialty was long-range reconnaissance, and we always had this concern: what if we met a little kid while on an operation?

GABOR SANTA: Well, first, I liked the movie very much, even though I haven't read the book yet. I am pretty sure I will take time to read the book after seeing this movie. In military college, my military occupation specialty was long-range reconnaissance, and we always had this concern: what if we met a little kid while on an operation? In long-range reconnaissance, we do special recon all the time, like these guys in the movie. You know, it is a never-ending discussion about what would be the best option to choose. In my personal opinion, which is not an official Hungarian position, and with all due respect for the movie makers—they did a great job—and with all my respect for the soldiers in the field: I am not quite sure that those men really made this decision to let the goatherds go, the one they made in the scene. Just thinking militarily, this was probably the worst choice they could make: leaving those guys free, immediately, with no physical restriction like tying their hands or just delaying them a little bit from going back to the village. As far as I saw, those SEALs were much smarter than that. I can understand that from the director's perspective, he had to do something that would be more effective for the civilian population, because this movie was made for civilians, not for the small military community. If you know whether they made that decision, then okay, I'm not sure we should talk about a better solution here.

But that was my impression: that the movie cannot show 100 percent what really happens in the field. But it still was a good movie.

O'LAVIN: I looked at the book before coming here, and it seems like those men put themselves in a kind of rapid-decision-making mode. At least Luttrell's account was that way: "Hey, we need to make a decision—is it X or Y?" In the book, as soon as the goatherds ran off, everyone on the team was asking, "Gosh, couldn't we have done something else?" But yes, I thought the movie was good. I think it was a fitting memorial for those three guys who died. It seemed in his *60 Minutes* interview that Marcus was still going through a lot of post-traumatic stress and survivor's guilt. And obviously the families of the soldiers and sailors who went down during the attempted rescue are still coping with their losses. From that perspective, I thought it was really well done. I also thought the sounds from the gunfight scene were well done: the snaps of the bullets and the different sounds that all the guns made were pretty accurate. Patrick, have you gone through the book at all?

I think the movie was a fitting memorial for those three guys who died.

COLLINS: Yes, I read the book a while ago.

O'LAVIN: How well do you think the movie stuck with some of the key points in the book?

COLLINS: The director also talked about that decision being one of his main focuses—that dilemma of "Hey, do we let them go, or do we kill them, or how do we do this now that we are compromised?" I think that decision actually took a lot longer than what was reflected in the movie. In the movie, it was only over a span of about five minutes. They were saying rapidly, "Hey, what do we do? What do we do? Okay, let's just do this." Then that was it. In actuality, it took a lot longer, and they did make a very strong effort to get comms [communications] during that time, to seek guidance. But unfortunately, they would have had to move from where they were, and I think they were afraid of moving along that ridgeline during the middle of the day because they would have been more visible to the [Taliban] fighters. So it really was a "damned if you do, damned if you don't" type of dilemma. But I thought that was something in the movie I would like to have seen a bit better explained—why they came to that decision during that time.

It really was a "damned if you do, damned if you don't" type of dilemma.

If I remember right, in the book, the men went over that: "If we keep them here until dark, some of their family members might come looking for them. We don't know when they are expecting them back. If we leave the goats and we just take the guys up to go and try to get better comms, somebody is going to see the goats running around and somebody is going to come up. If we kill them, they might hear the gunshots, they may come up if we …" I mean, it just goes on and on and on. It was just a horrible dilemma, and I don't know if we can say whether they made the right decision or not.

SANTA: No, you can't. No one can say that. You have to make a decision alone, and no one has the right to blame you if you do something wrong, because you're alone. And those men were alone.

What actually surprised me a little bit is that they had so many comms problems and they had no contact with the higher [command]. We have multiple choices of how to make contact with highers, and all of them failed? I am not saying that someone made mistakes before the operation, but that is surprising from a military perspective. From the movie's perspective, it was actually a good thing because the audience gets more excited, but from our perspective, it is kind of hard to believe that none of their comms worked.

O'LAVIN: And that is the risk you run, obviously. You have four guys going somewhere as a small unit, and they can carry only so much stuff. So perhaps they took a risk on backup comms. In the movie, the comms in that area just weren't very good for whatever sort of meteorological or terrain reasons. That's what I took away.

ELIZABETH SKINNER: I have a question concerning the communications at headquarters. How realistic was the scene where Commander Kristensen has gotten the satellite call in Bagram, and he tries to get the general's attention, but he seems to be told off? I was wondering if you had a reaction to that scene or anything to say about it.

You have to make a decision alone, and no one has the right to blame you if you do something wrong, because you're alone.

O'LAVIN: The general was saying, "Hey, how come I'm just hearing about this now, when you should have been telling me about this two hours ago at least, that you had a small, isolated force that hadn't made communications with you for a while?"

In most cases, if something like that happened, you would start requesting that assets be pushed over the last position you knew they were in, and that is why you call higher. You would say, "I haven't heard from my team, and I want some dedicated ISR [intelligence, surveillance, reconnaissance] platforms pushed over the site so we can try to figure out what is going on and why they haven't made comms." But if you know that folks are going into an area with bad communications, that should start making you a little bit concerned about the size of the element you are sending, if it is especially small and you know that they are going to have comms problems. That should lead you to think, "Maybe we need to rethink the size of the force we are sending, or the force structure itself. What is the mission risk that I am willing to accept compared with what I'll gain from this operation?"

SKINNER: It surprised me, as you were saying, how surprised they were by the fact that they didn't have communications.

O'LAVIN: Comms never work. That is, you test every one of your radios before you leave, and then 50 meters outside the front gate, you can't talk to other vehicles. You wonder what sort of voodoo magic is going on in those things, only 100 meters away from where you tested them!

"What is the mission risk that I am willing to accept compared with what I'll gain from this operation?"

COLLINS: It's like Murphy's Law: whatever communication can go wrong will go wrong. As you wrote in your message inviting us here, we can probably come up with some lessons learned concerning the two communication windows that they missed.

SANTA: One of the lessons is that you really have to have contingency plans for missing communication windows, especially for the recon element. You don't want them to be compromised, so you give them really wide communication windows. I am guessing that the windows for that team were at least four hours between, or even more, so they wouldn't have to go to the hilltop every 30 minutes to set up the radio, the communications set, and take the risk of being compromised. Then, if you miss two or three of those wide-spaced windows, you assume something really happened. So what I missed was the contingency plan. When Commander Kristensen was reporting to his highers that they had missed three communication windows, if I were the higher commander, I would probably ask what went wrong. Missing two or three communication windows means something happened, so I have to react. I should have a contingency plan, like, "Okay, now I need to rescue them, because either they got compromised or something happened to trigger the mission abort criteria, or something else happened."

If you miss two or three of those wide-spaced windows, you assume something really happened. So what I missed was the contingency plan.

That higher commander could have been acting like he did because there was no additional action report. Which goes to the same point I made earlier, that the decision they had to make as a recon element was very basic. They should have had contingency plans for a case such as meeting the goatherds. It seems fairly obvious near a village in Afghanistan that you will find goats and sheep walking around. They should have had a contingency plan: "We got compromised. Let's do plan C. Okay, we go to this point and get extracted, or just kill the target and get extracted," or something. These are the two main points I really missed from the action. They might have had some plan, but just didn't want to put it into the movie.

COLLINS: I think it just wasn't well portrayed in the movie. They were found, and it was a risk that they probably looked at: "Is it better for us to move during the day and get as far away as possible or to hide out?" It's another one of those dilemmas where you're damned if you do and damned if you don't. So I think all of those contingencies were in place, but maybe the movie didn't portray them well enough.

As for the higher's action, I think Commander Kristensen wanted to start spinning assets [sending rescue helicopters] right away after the first two missed comm windows. The problem was that the Apache escorts weren't available. There was another TIC [troops in contact] going on, and the Apaches were handling that issue, so Kristensen had to wait. By the time he finally decided to take off, he just said, "Hey, we are not going to wait any longer. Let's just go!" That's when the Chinook got shot down. So the assets, in theory, were in place, but they just weren't available for that QRF [quick reaction force]. You need those escorts, especially if it is an air infiltration, and those Apaches should have been dedicated versus just waiting there to be used for anything.

REBECCA LORENTZ: As operators, when you are watching a depiction of an actual military operation, is it difficult to separate watching this as entertainment, or do you pay attention to the TTPs [tactics, techniques, and procedures] throughout?

Is it difficult to separate watching this as entertainment, or do you pay attention to the TTPs [tactics, techniques, and procedures] throughout?

COLLINS: I think whenever I watch a film like that, I look more at the TTPs. At the same time, it is entertaining, but I admit I do look at the TTPs quite a bit.

O'LAVIN: I think any professional is paying attention. Obviously, the better the manipulation of the weapons and all of those details, the better you are able to say, "Yes, they have some good folks helping with the tactical/technical aspects of the movie."

COLLINS: Whenever I watch a movie that is about something I'm familiar with, I watch it with critiques ready. In the first second after *Lone Survivor* started, I was thinking, "Okay, what would I do if I were there? Would I do the same, or am I going to do something else? How could it be wrong or worse or better?" When I realized that something went wrong, it couldn't really entertain me anymore because the same could happen to me. In the field, you don't have time to be as smart as when you're sitting comfortably, watching a movie with popcorn and a Coke in your hands. I don't know how the temperature was in those mountains, but in a really rough environment like that, you can't make the perfect decision. Making the decision in the field is really, really hard. At least for me, watching these guys make a decision that cost their lives—that wasn't really entertaining at all. None of the scenes. From a certain perspective, yes, it was entertaining—nice TTPs, actions—but I wasn't happy at the end.

Watching these guys make a decision that cost their lives—that wasn't really entertaining at all.

O'LAVIN: You know how the movie is going to end. It's a downer as soon as things start going bad.

SANTA: Yes, and for the whole time I was thinking, "Okay, if they didn't take that step, or didn't turn right but went left, hopefully they could survive." This is all I had in my mind while watching the movie: what they should do differently to survive. For me, it is not an entertaining movie. It is more like you want to do something for them. You know it is too late, but you really want to do something even if it is only a movie. At least I wanted to do something. I don't know how you guys felt about that.

COLLINS: I think you're right. I think at the end of it, everybody was ready to grab their kit and go to Afghanistan.

O'LAVIN: Well, nobody wanted to ask Peter Berg a question, either. The mood in the theater was identifiably morose.

COLLINS: Yes, even having read the book, I was sitting there watching and hoping that something would change.

LORENTZ: How do you think the general public will view this movie? How do you think it will be received?

O'LAVIN: It's one of the questions I have. I think one of Peter Berg's goals was to try to show the general public the sacrifice and the realism of the battles that some of these units are having to fight somewhat frequently. So I think this movie will bring the realism home, and maybe some folks will say, "Hey, what exactly are we still doing in some of these places years and years later? What objectives are we really trying to accomplish—or do we really think we can accomplish—in some of these places? Is it worth the sacrifice of these folks to do that?"

I think this movie will bring the realism home, and maybe some folks will say, "Hey, what exactly are we still doing in some of these places?"

LORENTZ: Did any of you have your spouse there? I ask because in the [U.S. Naval Postgraduate School Defense Analysis] department, we have this question. The movie was very, very difficult to watch as a civilian, as a layperson. We wondered what spouse would watch this and be able to sleep again.

O'LAVIN: I came home and told my wife, "If we go, you'll probably need two boxes of tissues," because it is pretty hard to watch these guys basically dying over a 30-minute period. You know everything that is going to happen, and then, obviously, there's the memorial scene at the end for all of the folks who were killed, with the pictures of families and the men when they were alive.

I came home and told my wife, "If we go, you'll probably need two boxes of tissues."

SANTA: Wives always ask, "What are you guys doing out there? What is that noise I hear behind you on the phone?" "Well, that is the generator. Don't worry." So they know all of this stuff, but they just don't really know how tough it is. We don't talk very often about how tough the life is. I guess they deserve to know what we are doing, but at least personally, I don't want to have my wife in a situation where, whenever we are out [on deployment], she thinks, "Okay, my husband might be rolling down a hill hitting his head like 100 times on rocks." You don't want your wife to have to think about this. But they are human beings, and they are our life partners. They actually should know, but it is just not comfortable for me to talk about this. But I guess it's okay for them to watch these movies.

COLLINS: Yes, my wife didn't go, and I think it is for the same reasons these guys talked about. She just—doesn't want to see it.

SKINNER: In previous interviews and in the interview he did with us, Berg talked in a very compassionate way about these men and their families, and what he went through to try and bring this movie to life. The actors actually went and met the families and got to know them. I'm curious: was his compassion for those men apparent to you, or did the movie feel at all exploitative of these deaths?

COLLINS: I don't think it seemed exploitive. I guess anybody can say that this guy is making a multimillion-dollar movie about this story. It is obviously tragic, but I don't think it was exploitive at all. I think the memorial scene at the end was very good, and from the way he talked about it in the theater, I think he took the families' feelings into consideration a great deal before he put together the movie. That was good.

LORENTZ: One of the questions we asked Berg was "What surprised you most about your experience of embedding with the team?" and he answered that it was the camaraderie between the men that surprised him, how tight they were. Was that what you would think he would say?

COLLINS: Yes, I think so.

LORENTZ: Were you surprised to hear that?

O'LAVIN: I don't think so. I think the film reflected that—the brotherhood. That was my experience, and I think that is why most guys hang around, if they enjoy the folks that they work with. You sign up for the challenge—to be one of the cool guys. But then, what keeps you in is that you like all of the guys that you work with. They are a lot like you, and you can hang out with them on the weekends or at night or whatever. So that doesn't surprise me at all.

COLLINS: I agree. I have yet to meet a team that isn't tight like that. Even if they all hate each other, they all love each other, too. It is like a brotherhood.

I have yet to meet a team that isn't tight like that. Even if they all hate each other, they all love each other, too. It is like a brotherhood.

SANTA: It actually surprised me that he was surprised to see that this brotherhood is so tight within a team. I don't see why it is so surprising for a civilian.

O'LAVIN: Maybe "surprising" was just the word he used to mean what stood out the most about his experience.

LORENTZ: I agree, that is probably what stood out the most. But I do think that on the civilian side of things, there are not many other places where you see that.

SKINNER: If, God forbid, any of you should die in some situation like this, would this movie feel like a fitting memorial to you? Would you want to be portrayed in something like this?

O'LAVIN: I don't think it dishonored anyone, or the memory of the folks who were portrayed in the movie. I think that was a good thing. They could have made it a documentary of mistakes folks made, and then it wouldn't have been as fitting a memorial. Personally, I don't know if I would want a film made about me, just from the perspective of reliving the loss. They talked to the families beforehand and everything, but for family members or children to have to relive this event, I don't know if that is necessarily something that I would want. But it would be up to my family, because I wouldn't be there anymore.

COLLINS: Yes, I agree. I think one of the reasons this story was made into a movie—similar to *Black Hawk Down* or some of the other great military movies that were made—was because it was an extraordinary kind of situation. We have people who are fighting and dying over there, doing heroic acts all of the time, but what separates this one story is that it shows really extraordinary circumstances: a lot of things going wrong on our part and a lot of things going right on the enemy's part, which isn't always the case. So yes, I agree with Brian.

I don't know how the real action was on the ground, but even if this movie changed things a little bit to make these guys more heroic, they definitely deserve it.

SANTA: I am not sure I can answer this question. If I were in an operation, I wouldn't really be thinking, "Is there a director who is going to make a movie about this?" and then control my actions so that it will be a good movie. [laughter] From a military perspective, I don't really see any point to answering this question. But for a civilian population, you definitely need these types of movies. I don't know how the real action was on the ground, but even if this movie changed things a little bit to make these guys more heroic, they definitely deserve it because they started the operation, they fought through until they died. They tried to save each other, they tried to accomplish their mission, and they fought for their country, for their mission, and for that other country. So they definitely deserve to be seen as heroes by 350 million people, plus the rest of the world and me. That is good stuff.

LORENTZ: Do you have a favorite part of the movie, either for good or for bad reasons?

SANTA: Well, there are a couple of scenes. One is when the little Afghan kid at the end hugged Luttrell, and Luttrell hugged him back—that was really touching. And this *pashtunwali* [Pashtun code of honor], when Afghan villagers take care of the foreigner or someone who comes to their house—well, we learned about this tradition, but I didn't really understand it, that this is what it really means. You give your whole heart to the one who comes to your house, and that scene made me understand that. Even that little kid understood that *pashtunwali* required him to watch over this guy [Luttrell]. So that scene was probably my favorite.

COLLINS: I liked the early portion of the movie leading up to the operation. I thought all of that was pretty accurate, everything from the two guys competing against each other in the run to hazing the new guy, and all the planning stuff. I thought all of that really portrayed what team life is like in the different war zones, at least from my experience.

O'LAVIN: Yes, everything that showed the brotherhood-in-arms and the caring for each other. It isn't one specific scene, but everything in the movie that emphasized that aspect stood out for me, was reinforcing why I've stayed in the service. The only other question I really have—and we may have answered this—is, How do you think films like this influence the public? Is it positive? Is it negative? Are we over-glamorizing war with these types of movies? This question isn't necessarily limited to just this movie. But this one is much harder to watch, if you will, than films like *No Easy Day* or *Act of Valor*—or other more fictionalized movies. Net positive? Net neutral?

COLLINS: I think in some ways, it does glamorize war and it serves as a recruitment tool, especially for young men who are thinking about joining the Army or the Navy. But I think everybody wants to be in a firefight until they are in one, and then, as you know, things change. So I don't know. I think if I had seen this movie before I joined the Army, it would just have made me want to join even more, so I guess it does glamorize the fighting a little bit. But overall, I think it definitely does show the sacrifices and the things that a lot of our soldiers and SEALs are doing over there.

I think if I had seen this movie before I joined the Army, it would just have made me want to join even more.

SANTA: Well, I think that it can have a positive effect on young teenagers who were thinking about joining the Army or the Special Forces—especially those kids who like Xbox and PlayStation 4. It's funny, but I have personal experience with my son, who is a teenager. The military is not his life, but he knows much more about Black Hawks than I do. For these kids, it's really exciting to think, "Wow, that happens in real life as well!" So they are probably really happy to see these movies. But human beings don't really like sacrificing their partner or another human being for a country's cause. For those people, I think the movies have a kind of negative effect. When you read in a newspaper that 3,000 are dead, you don't really take seriously that those are human beings. But when you actually can see it, that has more of an effect on you than a number in a newspaper. I think most of the population who watch this movie will have a negative reaction, instead of thinking, "That is a great movie, and I want to watch it three times more."

O'LAVIN: It's impossible to generalize, but what do people in your country [Hungary] think of movies like *Lone Survivor* and *Black Hawk Down*? Is it similar to how they are received here [in the United States]?

> The current Hungarian generation doesn't really know what war means. For them, these types of movies are only entertainment, nothing else.

SANTA: No, definitely not. My country hasn't been in a war for some 60 years, and in our defense strategy, we don't really expect any war within the next 50 years. So we are in the middle of peacetime. Since 1956, we haven't really heard any gunshots except for crime. So the current Hungarian generation doesn't really know what war means. For them, these types of movies are only entertainment, nothing else. Even if they know that this movie is based on a true story, for them it is just an Xbox game or a PlayStation game. They will come out of the movie thinking, "Okay, it was good. What's next?" I would guess that applies to all of those countries that are not involved in any war as deeply as you are.

LORENTZ: Very interesting. That was a great discussion. Thank you all very much for talking with us. ❖

ABOUT THE INTERVIEWEES

CDR Brian O'Lavin, U.S. Navy, is working toward his PhD in security studies at the U.S. Naval Postgraduate School (NPS).

LTC Gabor Santa, a member of the 34th Special Forces Battalion, Hungarian Army, is studying at NPS.

MAJ Patrick Collins, U.S. Army Special Forces, is working toward his master's degree in Defense Analysis at NPS.

ABOUT THE INTERVIEWERS

Rebecca Lorentz is the manager of CTAP.
Elizabeth Skinner is the managing editor of *CTX*.

NOTES

[1] The Combating Terrorism Archive Project aims to collect and archive knowledge on strategy, operations, and tactics used by military and other security personnel from around the world in the twenty-first-century fight against global terrorism. Collectively, the individual interviews that CTAP conducts will create an oral history archive of knowledge and experience in counterterrorism for the benefit of the CT community now and in the future.

[2] Based on the book of the same title by Marcus Luttrell, the film depicts Operation Red Wings (June 2005), in which Luttrell and three other members of SEAL Team Ten were dropped into the mountains near a village on the Afghanistan-Pakistan border. Their mission was to capture or kill a Taliban leader who was responsible for the deaths of a number of Marines. Shortly after they landed, the team was discovered by three goatherds: an older man and two boys. The SEALs' decision about what to do with these villagers and the aftermath of that decision are at the heart of Luttrell's book and Berg's film.

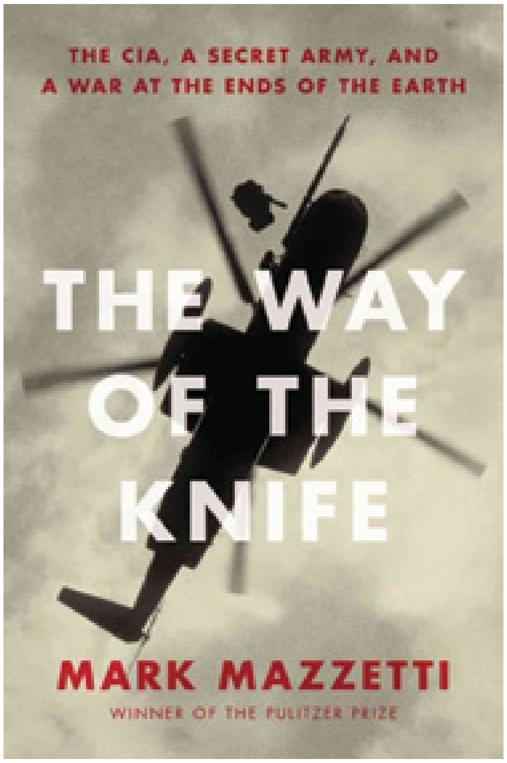
[3] This interview was edited for length and clarity. Every effort was made to ensure that the meaning and intention of the participants were not altered in any way. The ideas and opinions of all participants are theirs alone and do not represent the official positions of the U.S. Naval Postgraduate School, the U.S. Department of Defense, the U.S. government, or any other official entity.

THE WRITTEN WORD

The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth

MAJ Anthony A. Keller, U.S. Army

Mark Mazzetti
New York: Penguin Press, 2013
ISBN-10: 1594204802
ISBN-13: 978-1594204807
Hardcover: US $29.95
400 pages


THE CIA, A SECRET ARMY, AND
A WAR AT THE ENDS OF THE EARTH
THE WAY OF THE KNIFE
MARK MAZZETTI
WINNER OF THE PULITZER PRIZE

Mark Mazzetti's nonfiction thriller *The Way of the Knife* captures the essence of the relationship between the U.S. Central Intelligence Agency (CIA) and U.S. Joint Special Operations Command (JSOC), while engaging the reader in a contemporary and easily comprehensible read. Although cooperation between the CIA and JSOC developed long before 9/11, Mazzetti decodes the complexities and global reach of U.S. counterterrorism engagements and effectively demonstrates how the CIA transcended the "cloak-and-dagger" operations of the Cold War to forge a more dynamic relationship with JSOC. As a result, the two services have brought the full range of espionage, drone technology, and small wars to bear in support of U.S. national interests. Precision drone strikes and the use of small military elements from the Pentagon and the CIA's clandestine forces have made for a deadly combination in the fight against terrorism since 9/11.

Mazzetti describes how, in the first days after the 9/11 terrorist attacks, members of the CIA and officials of the George W. Bush administration[1] formulated a plan to begin the hunt for al Qaeda in eastern Afghanistan and the Federally Administered Tribal Areas of Pakistan. The CIA and the Pakistani Inter-Services Intelligence (ISI) conducted joint operations beginning shortly after 9/11, based on intelligence acquired through the ISI's complex spy networks of tribal warlords and the use of U.S. surveillance drones. This was the beginning of CIA and JSOC operations to capture or kill Taliban leaders and al Qaeda operatives. Mazzetti illuminates not only the turbulent relationship between the CIA and the ISI but also the deeper and longer standing relationship that the Taliban maintained with the ISI. The loyalty of the ISI, he makes clear, will always lie with Pakistan and its national security; for its members, every other concern is secondary to that.

Mazzetti also examines how the CIA has evolved as an offensive organization, from the spy agency's infancy as the Office of Strategic Services during World War II to the modern CIA. He uses several case studies from the last 50 years, documenting covert operations from Latin America to Central Europe, to illustrate the Agency's gradual modernization. Mazzetti tells us that in November 1984, President Ronald Reagan signed a secret document that allowed the CIA and JSOC to train Lebanese hit men in retaliation for the bombings against the Marine barracks in Beirut that killed 241 Marines (p. 51). While the author fails to clarify when exactly the rift between the CIA and the Pentagon began, he does point out that the more recent problems were not at the tactical level but primarily at the national policy level, between Secretary of Defense Donald Rumsfeld and the CIA leadership. "The confusion in Afghanistan [during the initial invasion] was partly the result of normal battlefield turmoil, but it had its origins in the jockeying between the Pentagon and the CIA for supremacy in the new American conflict. Secretary of Defense Donald Rumsfeld felt stung that CIA paramilitary teams had been the first into Afghanistan" (p. 18).

To make the spy game more complicated post-9/11, it now had a new player, JSOC, which reported directly to the Pentagon's Special Operations Command, but, more important, to Secretary Rumsfeld as well. By 2004, elements of JSOC had operatives around the globe, from South America, Africa, and Asia to the Middle East. The use of drone strikes along with small operational units of the CIA and JSOC became the modern-day cloak-and-dagger method used to hunt and exterminate al Qaeda operatives. Mazzetti notes, "In 2004, Rumsfeld issued a secret directive—known internally at the Pentagon as the 'Al Qaeda Network Executive Order'—that expanded the powers of special operations troops to kill, capture, and spy in more than a dozen countries" (p. 128). The order gave JSOC broad authority to conduct operations on a global scale.

"Secretary of Defense Donald Rumsfeld felt stung that CIA paramilitary teams had been the first into Afghanistan."

In the subsequent chapters regarding Pakistan, readers learn that Pakistan's game plan for supporting the Afghan insurgency was written in 1989, 12 years before the 9/11 attacks, in the library of the U.S. Command and General Staff College at Fort Leavenworth, Kansas. While a student at the college, General Ashfaq Kayani of the Pakistani Army wrote his thesis on the topic of Pakistani support for the Afghan resistance movement and the use of a proxy militia to fight against the Soviet occupation and the then-Communist Afghan government. This same game plan would be covertly implemented again by the ISI after 2001, but against U.S. and allied forces in Afghanistan and the new elected Afghan government, instead of the USSR and its puppet regime. It took three years after 9/11 for anyone in the United States to realize that the current head of the ISI, that same General Kayani, had been the author of the thesis.

Pakistan's game plan for supporting the Afghan insurgency was written in 1989, 12 years before the 9/11 attacks.

As bureaucratic infighting continued in Washington, one gleam of hope for the future of counterterrorism was the fusion between the CIA and JSOC. Their cooperation proved successful in the capture and killing of high-level operatives from al Qaeda and other terrorist groups in Pakistan and other regions of the globe. Mazzetti describes this relationship in terms of a masterpiece painting: it was perfect for what the White House wanted, which was a machine to capture or kill terrorists. The ability to share intelligence and resources allowed the CIA and JSOC to analyze critical intelligence in a timely manner and execute successful high-risk raids. War by proxy under covert U.S. guidance also became a template used by the Bush administration for operations in multiple regions of the globe. In Africa, for example, the use of Ethiopian troops in Somalia against al-Shabaab was critical to the Bush team's counterterrorism strategy.

The increasing use of drones by both the CIA and JSOC during counterterrorist operations has proved to be a less than perfect solution, not infrequently because of flawed intelligence. To illustrate this point, Mazzetti describes one particular operation in Yemen against al Qaeda in the Arabian Peninsula (AQAP). A joint CIA-JSOC operation mistakenly killed the deputy governor of Ma'rib province, Jaber al-Shabwani, with a drone strike while he was meeting with AQAP operatives to discuss a truce. U.S. officials had been told—inaccurately—by their Yemeni counterparts that no one within the Yemeni government had a relationship with or was in negotiations with AQAP, and believed that the meeting was among high-level AQAP leaders only. Many of the successes of the CIA will never be known, but its failures are always publicly placed upon the Agency's shoulders.

Readers of this book should find themselves grateful for the role the CIA and JSOC play in support of U.S. national security policy. Mark Mazzetti captivates the reader by offering a historical perspective on the transformation of the CIA and the agency's powerful partnership with JSOC. I highly recommend *The Way of the Knife* for anyone, particularly any member of the Department of Defense, who doubts the resolve of the United States to combat international terrorism. ❖

ABOUT THE REVIEWER

MAJ Anthony A. Keller, U.S. Army, is currently a student in the Department of Defense Analysis at the U.S. Naval Postgraduate School.

NOTES

[1] Vice President Dick Cheney, legal advisor David Addington, and chief of staff Lewis "Scooter" Libby.

Clockwise from top left: Donald Rumsfeld; Scooter Libby; Dick Cheney; George W. Bush; George Tenet.

THE MOVING IMAGE

The Wire
HBO Serial Television Drama, Created by David Simon

MAJ Matthew P. Upperman, U.S. Army

> "The game is rigged, but you cannot lose if you do not play."
> —Marla Daniels—a character in *The Wire* (season 1, episode 2)

It's all about "the game."[1] In HBO's *The Wire*, a crime drama series that aired from 2002 through 2008, the game is centered on the drug trade in present-day Baltimore and on the players' attempts to win—whether as a drug dealer controlling a corner or a police officer trying to make a difference.[2] Despite the show's focus on domestic police work, it is full of excellent parallels and lessons that can easily be applied to the special operations and intelligence communities, or any organization that is involved in irregular warfare (IW) or unconventional warfare (UW). Instructors at several universities, including Harvard and Duke, have used *The Wire* as the basis for courses covering studies in sociology and social anthropology. Warfighters and policymakers alike should not overlook the value of this show. The writers impart no "silver bullet" solutions for the problems of inner-city Baltimore, but *The Wire* does offer mental and emotional exercise for viewers, especially when it is watched through the lens of operational and intelligence planning in IW/UW.

The series centers on the development and operations of a major crimes unit within the Baltimore Police Department as it grapples with the illegal drug trade that plagues the city (and all of the social baggage that goes along with drug crimes). All five seasons are woven together and include the points of view and struggles of a complicated web of players. These include drug dealers, citizens, police, city hall employees and city prosecutors, newsmen, school staff, policymakers, longshoremen, and the transnational components of the illicit narcotics trade, among many others. Every season presents a new angle to the city's problems, and viewers are presented with dramatic twists in which the creative grassroots efforts of community organizers and local police are derailed, political jockeying and policy objectives address symptoms but fail to tackle core issues, struggles to control territory and information occur within and between government organizations—the list goes on. Although the series portrays the drug trade in inner-city America and one city's efforts to tackle it, *The Wire*'s story lines will be familiar to military and interagency operators overseas.

The first major takeaway message that this show has to offer is the need for a holistic view of the operating environment and any external strains that can or do affect the system. In *The Wire*, success too often hangs on the wrong metrics or faulty data; bureaucratic infighting results in missed opportunities; and competing priorities, political agendas, and misguided police work all contribute to the city government's failures to solve the problem. Nevertheless, opportunities for small successes develop out of creative ideas from members of the major crimes units, attention to good policing (including developing an intimate understanding of the players and environment), and the help of allies in City Hall and the city prosecutor's office who have a deep understanding of the problem and a wide view for implementing solutions. In addition, sound intelligence operations, from collection to analysis, help in formulating comprehensive strategies. As the show demonstrates, however, the successful efforts of a few can be undermined by both the mistakes of others and endemic strains within the bureaucratic system. The show thus conveys familiar emotions, such as the frustration implied in the question, "Are we really making any difference?" In episode 10 from season 5, for example, Baltimore Police Colonel Cedric Daniels rants about how the mayor has not carried out promised systemic changes to the police department:

Opportunities for small successes develop out of creative ideas from members of the major crimes units.

> I'll swallow a lie when I have to; I've swallowed a few big ones lately. But the stat game? That lie? It's what ruined this department. Shining up s*** and calling it gold so majors become colonels and mayors become governors. Pretending to do police work while one generation f****** trains the next how not to do the job. And then I looked Carcetti [the mayor] in the eye, I shook his hand, I asked him if he was for real. Well, this is the lie I can't live with.

A second important takeaway involves slotting the right individuals into the right jobs. Successes—in the inner city and on the battlefield—often spring from leaders who have the courage to go against the grain in order to alter the status quo; provide a relatable vision for others to follow; and empower, mentor, and enable subordinates to come up with creative solutions. This truth is illuminated in *The Wire* by stories of a "good" beat cop or having the right mayor in city hall. There are also plenty of examples of "what wrong looks like." *The Wire* does an excellent job of illustrating how the wrong policies and the mistakes people make affect efforts all the way down the chain. The following quote comes from *The Wire*'s Major Howard "Bunny" Colvin, who is venting his frustration with poor police work and leadership in the police department:

> This drug thing, this ain't police work. No, it ain't. I mean, I can send any fool with a badge and a gun up on them corners and jack a crew and grab vials [of drugs]. But policing? I mean, you call something a war, and pretty soon everybody gonna be running around acting like warriors. They gonna be running around on a damn crusade, storming corners, slapping on cuffs, racking up body counts. And when you at war, you need a f****** enemy. And pretty soon, damn near everybody on every corner is your f****** enemy. And soon the neighborhood that you're supposed to be policing, that's just occupied territory.[3]

"You call something a war, and pretty soon everybody gonna be running around acting like warriors."

A third takeaway for those involved in IW/UW is the importance of a deep understanding of the players in the operating environment and building relationships with the right individuals, whether it be cultivating a snitch with access and placement, knowing all of the "corner boys" (low-level drug dealers), working with influential citizens, or learning whom to leverage at city hall to get support. For members of the Baltimore Police Department, building relationships helps them break down bureaucratic stovepipes and create cooperative approaches, including properly applying social outreach and using locals to help solve local problems.

Military practitioners will be surprised by how many of *The Wire*'s themes will resonate with their deployment experiences.

The Wire's relevance to the special operations community lies in operating in complex environments; understanding and navigating core issues in the face of ambiguous opposition (enemy and social forces alike); and understanding the disconnect that often exists between policymakers, bureaucrats, and the several echelons of community leaders and police (read: the warfighters). Apart from *The Wire*'s entertainment value, military practitioners will be surprised by how many of the show's themes resonate with their deployment experiences; they may even find themselves contemplating how they could have approached situations differently had they seen the show earlier. ❖

ABOUT THE REVIEWER

MAJ Matthew Upperman is a U.S. Army military intelligence officer who is currently assigned to the 7th Special Forces Group (Airborne).

NOTES

[1] Editor's note from Anna Simons: Credit is due to LTC Sam Curtis, an early fan of *The Wire*, who insisted that everyone deploying to Iraq or Afghanistan needed to watch it. Like Matt Upperman, Sam considered everything—from the challenges the police face in Baltimore to the tradecraft they develop over the course of the series—to be relevant to his work overseas. I watched the series on Sam's recommendation and came away with this: We Americans haven't been able to "fix" Baltimore, and yet we expect to go halfway around the world and "fix" Iraq and Afghanistan?!

[2] *The Wire* is no longer being broadcast, but it remains widely available on DVD or through online streaming services.

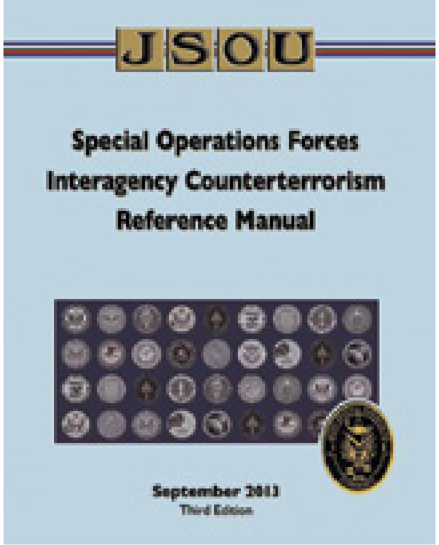
[3] Season 3, episode 10.

PUBLICATION ANNOUNCEMENTS

The newest research published by JSOU Press!

These four new JSOU Press publications are now available electronically from the JSOU public website, https://jsou.socom.mil, in the Publications section under 2013. They are also available in the JSOU Library Management System: https://elibrary6.eosintl.com/U60005/OPAC/Index.aspx

Special Operations Forces Interagency Counterterrorism Reference Manual, Third Edition
edited by Chuck Ricks
Issue Date: September 2013



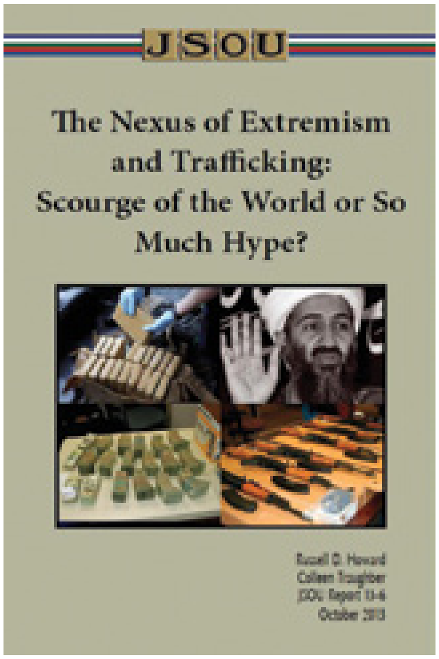
JSOU

Special Operations Forces
Interagency Counterterrorism
Reference Manual

September 2013
Third Edition

This third edition builds on the success of the manual's earlier versions and continues to incorporate the evolving policy guidance and strategic vision that guide ongoing interagency counterterrorism efforts. It provides an outline of the organizations, missions, programs, and relationships that comprise the interagency process. This manual provides insight and information regarding various counterterrorism organizations in the U.S. government's national security apparatus. It also includes an explanation of the expanded concepts of civilian power and their implications for diplomacy and development that emerged from the publication of the *First Quadrennial Diplomacy and Development Review* in 2010. Expanded sections on countering terrorist finance operations, interagency responses to cyber threats, and strategic communication reflect a general acknowledgement of the importance of these capabilities. As before, this new edition includes updated collections of definitions, organizations, programs, and acronyms to provide the special operations warrior with an improved, practical, quick-reference guide to the interagency community.

The Nexus of Extremism and Trafficking: Scourge of the World or So Much Hype?
by Russell D. Howard and Colleen Traughber
Issue Date: October 2013

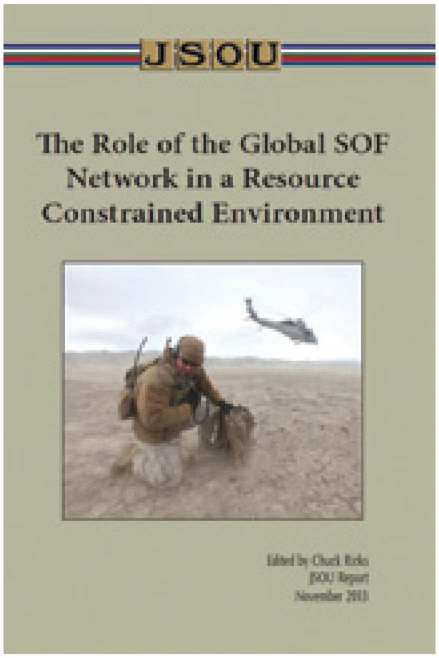


JSOU

The Nexus of Extremism
and Trafficking:
Scourge of the World or So
Much Hype?

Russell D. Howard
Colleen Traughber
JSOU Report 13-6
October 2013

In this monograph, retired Brigadier General Russ Howard and Ms. Colleen Traughber delve into the nexus between violent extremist elements and transnational criminal elements by first clarifying whether a real problem exists and, if so, identifying the appropriate role for Special Operations Forces in confronting it. The authors bring rigor to the subject matter by dissecting the issues of intention and opportunities for criminal organizations and violent extremists. The authors note that these motivations and opportunities can vary widely among the different organizations. They further make clear that the trafficking of humans, weapons, drugs, and contraband (HWDC) is a natural way for the criminals and extremists to cooperate. To bring the issue into focus, the authors systematically examine case studies dealing with the nexus between specific organizations and HWDC trafficking opportunities. The authors then explore how this nexus will affect SOF and interagency partners, including issues for SOF such as the traditional delineation between law enforcement activities and military activities.



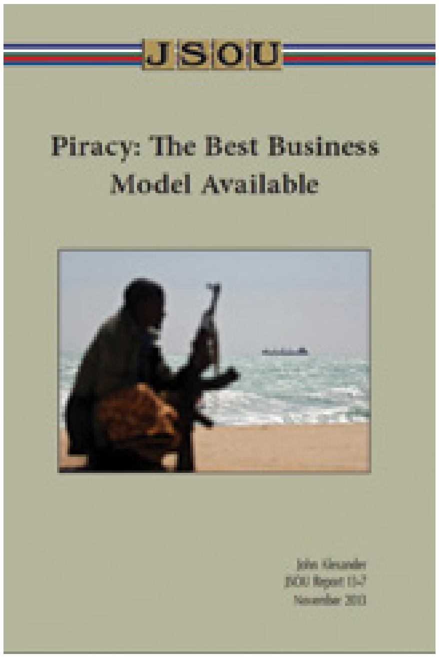
JSOU

The Role of the Global SOF Network in a Resource Constrained Environment

Edited by Chuck Ricks
JSOU Report
November 2013

The Role of the Global SOF Network in a Resource Constrained Environment
edited by Chuck Ricks
Issue Date: November 2013

In February 2013, more than 125 SOF personnel from Canada, the United States, and eight other countries gathered at MacDill Air Force Base in Tampa, Florida, for a two-day symposium on "The Role of the Global SOF Network in a Resource Constrained Environment." This was the third symposium in a series held by the Joint Special Operations University and the Canadian Special Operations Forces Command Professional Development Centre. The event featured a mix of individual presentations, panel discussions, and social interaction to introduce issues, engage in productive discussions, and strengthen SOF network relationships. The subject matter ranged from the tactical *(The Acid Test of Reality-Experiences of the Operators)* to the strategic, with senior civilian and military leadership from both Canada and the United States assuming active, contributing roles. This report offers insights and suggestions on how to deliver operational success while accommodating both changing mission sets and resource-constrained environments.



JSOU

Piracy: The Best Business Model Available

John Alexander
JSOU Report 13-7
November 2013

Piracy: The Best Business Model Available
by John Alexander
Issue Date: November 2013

In this monograph, Dr. Alexander sets the stage with a brief historical account of how maritime piracy has evolved over the centuries to its current state: a vast enterprise whose increasing profitability has attracted a confluence of nefarious actors, including warlords and international criminal organizations. Dr. Alexander speculates on the potential for an intersection between pirates and ideological terrorist movements such as al Qaeda and associated groups. Such a future would significantly elevate the stakes in a U.S. whole-of-government counter-piracy response. What role should the U.S. military, and SOF in particular, play in addressing the global issue of maritime piracy? Dr. Alexander points out many of the thorny legal considerations that contextually color any efforts to address counter-piracy, and notes that the best solution to criminal acts occurring hundreds of miles at sea may in fact lie with efforts, including the use of SOF, to improve the security apparatus on shore.

COVER CREDITS

Top to bottom, left to right:

Boral River in village Bangladesh by Shahnoor Habib Munmun, licensed under Creative Commons 3.0 via Wikimedia Commons

Iraqi girls on a donkey cart through the streets of Abu Atham, Iraq by James (Jim) Gordon, licensed under Creative Commons 2.0 via Wikimedia Commons

Mosque, Damascus (photographer unknown), public domain via Wikimedia Commons

Jagalchi fish market in Busan, South Korea by Warszk, licensed under Creative Commons 3.0 via Wikimedia Commons

Red Balloon challenge, U.S. Government work via DARPA

The Afghan national police commander marches to greet distinguished visitors at the graduation of Afghan National Police Academy cadets by Brian Ybarbo, U.S. Government work via Wikimedia Commons

Tengeru market near Arusha, Tanzania by Fanny Schertzer, licensed under Creative Commons 2.0 via Wikimedia Commons

CPI(M) rally in Agartala, Tripura by Soman, licensed under Creative Commons 3.0 via Wikimedia Commons

Shi'a and Sunni Muslims make their way to the Imam Husayn Shrine in Karbala, Iraq, Feb. 27, 2008, during their pilgrimage in observance of the Arba'een and Ashura holiday, by U.S. Navy photo Petty Officer 1st Class Denny C. Cantrell via Wikimedia Commons

Times Square balloon from above by Anthony Quintano, licensed under Creative Commons 2.2 via Wikimedia Commons

Last day party in Latinoware 2007–Brazil by Fernando da Rosa, licensed under Creative Commons 3.0 via Wikimedia Commons

180° panoramic view over San Francisco photographed from Twin Peaks by Tuxyso, Damascus by night viewed from Mount Qasioun by Zelidar, licensed under Creative Commons 3.0 via Wikimedia Commons

Damascus by night viewed from Mount Qasioun by Zelidar, licensed under Creative Commons 3.0 via Wikimedia Commons

Takeshita dori, Tokyo, Japan by Kakidai, licensed under Creative Commons 3.0 via Wikimedia Commons

Iraqi boys giving peace sign by Christiaan Briggs, licensed under Creative Commons 3.0 via Wikimedia Commons

Looking west at Roman Catholic Church of the Capuchins on Broadway and Isham Street on a sunny midday by Jim.henderson, Public domain via Wikimedia Commons

The flea market in the Old City of Jerusalem, Israel by Ester Inbar, available from http://commons.wikimedia.org/wiki/User:ST via Wikimedia Commons

Shepherd in a village in Tamilnadu by tshrinivasan, licensed under Creative Commons 3.0 via Wikimedia Commons

Village bridge Sapa, Ta Van, Lao Chai, Vietnam by Lori_NY, licensed under Creative Commons 2.0 via Wikimedia Commons

Chechen women plead for Russian troops not to advance towards the capital Grozny, December 1994 by Mikhail Evstafiev, licensed under Creative Commons 3.0 via Wikimedia Commons

Luxor (Egypt): street scene by Marc Ryckaert (MJJR), licensed under Creative Commons 3.0 via Wikimedia Commons

March 8 rally in Dhaka, organized by Jatiyo Nari Shramik Trade Union Kendra (National Women Workers Trade Union Centre), an organization to the Bangladesh Trade Union Kendra by Soman, licensed under Creative Commons 3.0 via Wikimedia Commons

Baking bread in a traditional Iraqi way by Aziz1005, licensed under Creative Commons 3.0 via Wikimedia Commons

Kabul–An Afghan National Civil Order Police (ANCOP) honor guard stands in formation while attending an ANCOP Officer Candidates School (OCS) graduation May 6, 2010 at the Ministry of Interior by Staff Sgt. Sarah Brown, U.S. Government work via Wikimedia Commons

IMAGE CREDITS

Pages 6–7: via Wikimedia Commons, U.S. government work

Page 11: via Wikimedia Commons, licensed under Creative Commons

Page 23: CIA.gov, U.S. Government work

Page 25: via DoDImagery.mil, photo by 1LT Richard Norris

Page 28: Screen capture, *Wired*, at http://www.wired.com/vanish/2009/11/ff_vanish2/

Page 29, 30, 31, 33: via DARPA at http://archive.darpa.mil/network-challenge/Photos/Balloon21.jpg, U.S. government work

Page 30: Screen capture, Tag Challenge, at http://www.tag-challenge.com/ U.S. Government work

Pages 39, 40: Images courtesy of the author

Page 59: Left, via DoDImagery.mil, by SGT Gustavo Olgiati; right, via DoDImagery.mil, by Corporal Rob Knight, RLC

Page 61: via Wikimedia Commons, licensed under Creative Commons 3.0

Page 62: via Wikimedia Commons, licensed under Creative Commons 3.0

Page 63: via Wikimedia Commons, licensed under Creative Commons 3.0

Page 72: via Wikimedia Commons, U.S. Government work

Page 73: via *LA Times* at http://www.latimes.com/news/nation-world/nation/la-sc-dc-0515-first-terrorist-pictures-006,0,2941158.photo#axzz2r9V55OHo, U.S. Government work

Page 74: via Wikipedia at http://en.wikipedia.org/wiki/File:WTC_1993_ATF_Commons.jpg U.S. Government work

Pages 81–85: All images via IMDB.com

Page 96: Donald Rumsfeld, Dick Cheney, George W. Bush via DoDImagery; Scooter Libby and George Tenet via Wikipedia

Pages 98–100: all images via IMDB.com

CALL FOR SUBMISSIONS

The *Combating Terrorism Exchange* (*CTX*) is a quarterly peer-reviewed journal. We accept submissions of nearly any type, from anyone; however, submission does not guarantee publication. Our aim is to distribute high-quality analyses, opinions, and studies to military officers, government officials, and security and academic professionals in the counterterrorism community. We give priority to non-typical, insightful work, and to topics concerning countries with the most pressing terrorism and CT issues.

Submission Guidelines

For detailed submission guidelines go to www.GlobalECCO.org/journal/ and click on the "Submit to CTX" link.

CTX accepts the following types of submissions. Please observe the following length guidelines:

- **academic analyses** (up to 6,000 words)
- **reports or insightful stories from the field** (up to 5,000 words)
- **photographic essays**
- **video clips** with explanation or narration
- **interviews** with relevant figures (no longer than 15 minutes)
- **book reviews** (up to 2,000 words); review essays (up to 2,000 words); or lists of books of interest (which may include books in other languages)
- reports on any **special projects**

Submissions should be sent in original, workable format. (In other words, we must be able to edit your work in the format in which you send it to us: no PDFs, please.)

Submissions should be in English. Because we seek submissions from the global CT community, and especially look forward to work which will stir debate, WE WILL NOT REJECT submissions outright simply because of poorly written English. However, we may ask you to have your submission re-edited before submitting again.

Ready to Submit?

By making a submission to *CTX*, you are acknowledging that your submission adheres to all of the submission requirements listed above, and that you agree to the *CTX* Terms of Copyright, so read them carefully.

Submit to:
CTXSubmit@GlobalECCO.org

If you have questions about submissions, or anything else, contact:
CTXEditor@GlobalECCO.org

Submission Requirements

Submissions to *CTX* **must** adhere to the following:

- The work must be copyedited for basic errors *prior to* submission.
- Citations should adhere to the *Chicago Manual of Style*, available online.
- The work submitted may not be plagiarized in part or in whole.
- You must have consent from anyone whose pictures, videos, or statements you include in your work.
- You must agree to our Terms of Copyright.
- Include a byline as you would like it to appear and a short bio as you would like it to appear (we may use either, or both).
- Any kind of submission can be multimedia.

Terms of Copyright

CTX is now online at globalecco.org/journal

현대택배
한진택배
Takeshita Street
CodeColle
祝 街路灯完成！ご協力ありがとうございました。竹下通り商店会
WOLFGANG PUCK EXPRESS