



# Asian Conflicts Reports

- ◆ Japan's home-made bomb threat
- ◆ Internet radicalization ◆ Maoist violence in India
- ◆ Counter-Terrorism in the Philippines

Issue 5 | May, 2009

Council For Asian Terrorism Research

# New threats from home-made explosives in Japan

Katsuhisa Furukawa



Traditionally, Japan has enjoyed an international reputation as a safe country. However, the expansion of the internet has changed the situation significantly. Over the past few years, there have been an increasing number of incidents in which individuals attempted to cause mass casualties using homemade explosives or attempted to commit suicide or cause harm to others using hazardous chemicals.

Regarding hand-made explosives, several cases have drawn the particular attention of Japanese law enforcement authorities. In those cases, amateurs attempted to construct explosive devices using commercially available materials and instructions available on the internet.

The first example occurred in June 2007 when a Japanese man was arrested on charges of violating the Criminal Regulations to Control Explosives. According to prosecutor statements during the court trial, the 38-year old man conspired to detonate explosives on a commuter train during the morning rush hour in Tokyo. While he was not an explosives expert, this individual had managed to produce a sufficient amount of TATP, a home-made explosive, "after reading about a method for manufacturing the explosives on the Internet." He did not have stable employment and had, reportedly, come to hate those people who did. Although he was inspired by information on the internet about the July 2005 suicide terrorist attacks in London, this Japanese man had nothing to do with violent, radical religious extremism. Before reading about the London attacks and learning bomb-making on the internet, he was simply a disaffected individual who wanted to commit suicide.

Similarly, in February 2008, a former mechanic was arrested for having synthesized explosives, including TATP, RDX, and other unidentified explosive material which he manufactured by himself. According to his court testimony, the man was obsessed with the belief that the world was coming to an end, and that the devil would take over human beings' souls, making them like the girl in the Hollywood movie, *The Exorcist*, whose head could turn 360 degree. He claimed to have synthesized the explosives with the purpose of preparing for a war against those evil forces. Forensic investigators were unable to identify the specific type of explosive material he created, because it was so unstable that it might detonate at anytime. The police contained the homemade explosive in a safe container. Under controlled detonation, it was shown to have had strong destructive power. This individual had also learned how to synthesize explosives, in part by using information on the internet, supplemented by other professional books and articles that are available in the open sources. He synthesized his explosive materials in his home using commercially available materials.

In September 2008, a third man was arrested for having discharged fire-extinguishers containing black gunpowder toward the Imperial Palace. His purpose was simply to take delight in people's reaction to his crime. After his arrest, the police discovered that he had also tried to synthesize ANFO-based bombs, using a total of approximately 930 kilograms of commercially available materials that he had procured in stores. Later, authorities found out that he had conducted explosive experiments, the videotapes of which he had posted to a particular internet website on which contestants compete over the explosive power of various hand-made explosives.

In February 2009, a high-school student in Sapporo City in Hokkaido Prefecture in the northern part of Japan, was arrested for having conspired to kill his classmates with hand-made explosives that were made of organo-peroxide and black gunpowder. Reportedly, this student intended to kill approximately 30 classmates with hand-made explosives that he had learned to synthesize through the information on the internet because they had allegedly ridiculed. When he was arrested, he seemed to have just begun the initial process to synthesize the explosives, but he already possessed a sufficient amount of gunpowder and other chemical compounds, including hydrogen peroxide and sulfur, to fabricate a bomb, as well as screws and hobnails intended to enhance the bomb's kinetic killing power. All these materials were procured at drug stores and other commercial stores, at a cost of approximately 80,000 YEN (about US\$800). He came up with his plan after an acquaintance told him that such a bomb could be constructed easily. He, like the individual arrested in June 2007, also intended to imitate the bombs used in the London terrorist attacks on July 7, 2005. The police contend that the bomb, if completed, would have had sufficient power to destroy an entire house or school classroom.

1

Several individuals have tried to cause mass casualties using home-made explosives and chemicals

2

The internet and other open sources have been used to fabricate these devices

3

Counter-terrorism efforts must engage with the threat from disaffected individuals



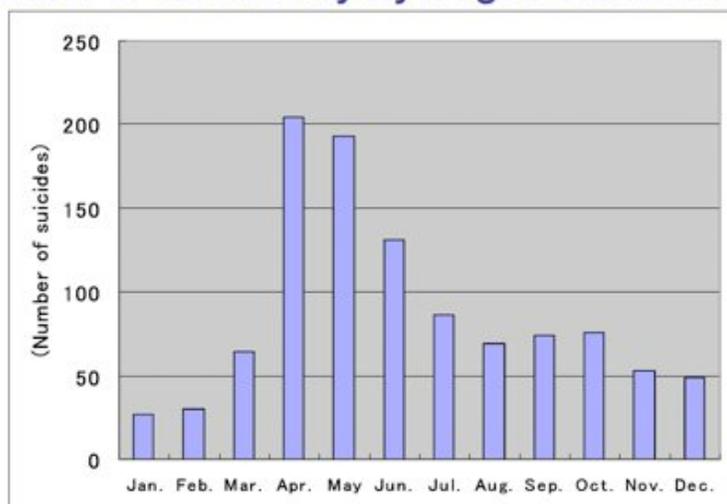
In the area of chemical incidents, the Japanese government paid particular attention to the rapid surge in the number of cases in which individuals conducted suicide attacks using homemade hydrogen sulfide that can be synthesized using toilet bowl cleaner containing hydrogen chloride and liquid bath essence or lime sulfur containing calcium polysulfide. After the information about how to synthesize hydrogen sulfide was posted on a website, sometime in December 2007 or January 2008, the number of incidents involving hydrogen sulfide surged rapidly in subsequent months. Specifically, whereas in January 2008, only 27 people committed suicide using this method, the number suddenly increased to 204 people in April of the same year. The number of individuals committing suicide using hydrogen sulfide was only 29 in 2007 but had increased rapidly, to about 1,056, in 2008 – a rate 36.4 times greater than in the previous year. The information on the internet inaccurately described this method of suicide as one that would enable individuals to commit suicide painlessly and smoothly, leaving them with restful expression on their faces after death. Sadly, many individuals believed this information.

In several cases, family members and neighbors have inadvertently also fallen victim by inhaling the toxic gas. In one incident, a 14-year-old girl, third-year student at a public junior high school, was found dead after apparently intentionally inhaling hydrogen sulfide in the bathroom of her apartment inside a municipal housing complex. Subsequently, a total of 21 nearby residents were transported to four hospitals, and 14 were hospitalized. Another 68 residents went to hospitals on their own. Due to lingering fears of hydrogen sulfide poisoning, another 75 residents of the housing complex were evacuated and spent the night at a nearby gymnasium.

In April 2008, the Japanese government classified the information about synthesizing hydrogen sulfide as “harmful information” and, with the help of internet providers, restricted general access to the information. While the number of suicide cases involving hydrogen sulfide peaked in April 2008 and subsided subsequently, they have still continued since.

These incidents bring to light important policy considerations for counter-terrorism in Japan. The tools employed by terrorists abroad are now readily available even to those individuals who have no particular ideological agenda but are disaffected or frustrated by such realities of life as unemployment or bullying. In this environment, a disturbed individual’s suicide attempt could develop into a plan for a suicide attack involving other casualties, either intentionally or accidentally. We live in a society where copy-cat ‘terrorists’ or ‘criminals’ could emerge from among disaffected individuals of all kinds. “Religious” motivation is not a prerequisite for someone planning to harm others. Historically, many of the most costly mass casualty terrorist attacks, including in Japan, were domestic, conducted by native individuals. The lesson is that Japan’s counter-terrorism effort cannot concentrate solely upon foreign terrorists or radical violent extremists with specific religious or ideological orientations. •

### Number of suicides by Hydrogen Sulfide in 2008



The National Police Agency reported, total:1,056 people (In 2007: 29 people)

Presentation material by Yumiko Kuroki, Ph.D., Kaoru Iida, and Toshiharu Yoshioka, M.D. Ph.D., Japan poison Information Center, at the Japan-US Chemical and Biological Collaboration Conference at the RISTEX, in Tokyo, Japan, February 17-19, 2009.

# Countering internet radicalization in South-East Asia

## RSIS and ASPI Joint Report \*

The internet is a powerful tool for terrorist groups to promote extremist ideology and hatred. The writings of terrorist groups are regularly posted on websites in our region. And convicted terrorists have given evidence about the influence of the internet on their recruitment and communication strategies.

Although the internet has become important tool for the dissemination of propaganda and tradecraft manuals, it is also being used as a tool to radicalize potential supporters. Throughout Southeast Asia, extremists are increasingly using web forums and chat rooms to entice and groom new recruits.

Until recently, the radicalizing influence of the internet has been rare. Very few individuals have been convinced to carry out terrorist operations simply by engaging with material online. There are complex social and psychological factors at play in the process of radicalization. The pathway between curiosity for a cause and commitment to violence has occurred mostly through direct social contact.

But this may be changing. Recent evidence shows that the internet has become more central to how individuals and groups become radicalized in support of violent action.

The internet has made it easier for individuals to search for an identity and a cause. This was the case for Abdul Basheer, a law graduate in Singapore who was arrested in 2007 for attempting to join the Taliban in Afghanistan. He had turned to the internet for answers to his questions on religion and chanced upon radical explanations that resonated with his state of mind and his personality. He believed martyrdom and the promise of paradise would bring moral redemption within his family.

In Australia, the trial of Abdul Benbrika and others on terrorism-related charges shows how the dissemination of extremist material can contribute to radicalization. The court heard that the Melbourne-based Benbrika group downloaded, collated and distributed extremist material, including videos of hostage beheadings and documents that contained recipes for the manufacture of explosives. In sentencing Benbrika to 12 years in prison, the court noted that, although the possession of such material might not be a criminal offence, it takes on a more sinister complexion when used by charismatic leaders to encourage or engage in acts of terrorism, for which such material provides extremely useful instruction.

Recent research from Ireland shows the potential radicalizing influence of Web 2.0 applications that integrate information with social networking. A study of how YouTube videos were posted and distributed online showed how an individual browsing generic websites could be drawn in to a dangerous network. In one example, a young man who identified himself as an Irish rugby fan was targeted by radical groups after he posted a comment on a martyrdom video expressing his interest and support.

Although there is a growing body of research on how terrorists use the internet in Europe and North America, less attention has been given to the role of internet in online radicalization in Southeast Asia.

In the last decade, access to the internet has increasing on average by over 300 per cent in most Southeast Asia countries. And the number of radical and extremist websites has grown from around 17 in 2000 to more than 100 today.

The material on these websites is also changing. In the past, websites tended to mimic the contents and features of their Arabic and Middle Eastern counterparts. More recently, the Southeast Asian websites have posted tradecraft materials, such as hacking and bomb-making manuals. One of the first appearances of a tradecraft manual was in August 2007 in the then new forum, *Jihad al-Firdaus*. The forum had an entire section on electronic *jihad*.

The websites in Bahasa Indonesia and Malay reflect popular internet trends. Blogging and social networking using *Friendster* and *Multiply* have caught on across the spectrum of internet users. Southeast Asia seems more open to online social networking than the Middle East. Moreover, the average age of terrorists appears to be declining, as is the age when young people are becoming radicalized. Teenagers are the greatest users of the internet and are therefore most likely to be influenced by it. They've grown up with computers and they spend much time online. The trend of increased internet usage is expected to continue over the next decade.



1 The internet is increasingly being used as a tool of radicalization in South-East Asia

2 Governments have so far done little to arrest internet radicalization

3 A range of stakeholders will have to be involved in counter-measures.



At the core of the extremist message we find calls to operate as a decentralized network and encouragement for individuals to develop technical computer skills. It's no surprise that much of the focus of terrorist recruitment activity is on university and college campuses, where access to computers and skilled operators is highest. The internet is used to reinforce religious and political messages, to increase commitment and to build online communities sharing similar perspectives. These messages can provide inspiration, ideological support, practical instructions, friends and a social support network that facilitates links with other cells. A growing number of young people are turning to the internet for guidance in all aspects of their lives.

Of course, we shouldn't neglect offline networks. As Marc Sageman notes, most terrorist networks consist of a mixture of online and offline elements. Their respective in-person and online discussions are mutually reinforcing.

Most countries in the region, including Australia, now face the problem of home-grown radicalization. As police monitoring of physical spaces makes it harder for extremist groups to operate in the open, they're turning to cyberspace. And the internet offers a vast battleground where 'female fighters' are able to join the ranks at the front line, without restrictions.

Understanding and countering online radicalization must be one of the main pillars of the fight against regional terrorism. Therefore, national and regional plans need to be put in place to combat terrorists' use of the internet.

To date, regional governments and national law enforcement agencies have done little to stop the rise of online radicalization. Compared to territorial security or economic management, the possible threat from a handful of people radicalizing themselves by spending long hours in front of computer screens has not been seen as a priority. The many legal factors involved in attempts to regulate cyberspace have also been a political minefield for many regional governments.

Although websites that incite violence are subject to criminal laws in some countries, there are often no specific regulations covering the internet. Some governments don't want to appear un-Islamic by coming down hard on Islamist groups, and some don't want to appear undemocratic by seeming to rein in freedom of expression in cyberspace.

In general terms, there are three broad policy approaches that governments could adopt:

- *zero tolerance* (blocking sites, prosecuting site administrators, using internet filters)
- a softer strategy of *encouraging internet end users to directly challenge the extremist narrative* (including creating websites to promote tolerance)
- an intelligence-led strategy of *monitoring leading to targeting, disruption and arrest*.

These broad approaches can, and probably should, be pursued simultaneously. In most cases, regional countries should not adopt one approach to the absolute exclusion of the others. Also, while the focus here is on countering online radicalization, the offline elements of terrorist networks are equally important.

A range of stakeholder interests must be balanced in countermeasures to combat online radicalization. Law enforcement and security (government); the internet industry, such as site administrators, domain hosts and internet service providers (ISPs); the community of online users; business (e-commerce); and the media all have an interest in access to information.

Each approach will have advantages and drawbacks in its security consequences, its economic impacts (on public authorities, ISPs and consumers) and its broader human rights implications (such as freedom of expression, access to information and privacy).

For example, hard-line approaches using censorship and filtering might not be effective for technical and legal reasons, while softer approaches might be too slow to show real results and in the long run might not deter the extremists. Intelligence gathering and monitoring will be part of any sensible approach. However, in many cases, it won't be easy to apprehend those responsible for maintaining websites deemed illegal.

There is a growing debate among terrorism experts about the appropriate next steps in the counter-radicalization debate. Restricting user access to extremist material is considered by some analysts as crude, expensive and counterproductive. But as access to this type of material increases, the radicalizing influence will become more pronounced. And an environment where extremist and hateful material has become commonplace only fuels the climate of violence that terrorists seek. The problem of internet radicalization crosses national borders and will require a concerted international response. Domestic political considerations will influence the choice of policy options available to governments in Southeast Asia. But developing comprehensive strategies to counter the rise of online radicalization is likely to be an increasingly important part of the counter-terrorism agenda in the future. ●

# India's elections and the Maoist threat

Bibhu Routray



Despite fears that month-long exercise to elect a new lower house of Indian Parliament would be marked by large-scale Maoist violence, the first two phases of the five-phase election process have passed off relatively peacefully.

On April 16, the first day of the polling, between 58 and 62 per cent of 143 million voters exercised their franchise in 124 constituencies across 15 States and two Union Territories. Considering the fact that this phase of polling covered much of the territory that is significantly affected by Communist Party of India-Maoist violence, attacks were inevitable. However, the toll—eighteen dead—was lower than most experts had anticipated.

The second phase on April 23, held in Maoist affected States such as Andhra Pradesh, Bihar, Jharkhand, Maharashtra and Orissa saw a dramatic. Stray incidents apart, there was no significant violence; no fatalities were reported. Over 55 percent polling was recorded on that day.

CPI-Maoist' activities affect 195 of India's 630 districts, in 16 states. With a cadre strength of nearly 20,000 armed cadres and another 100,000 militia and overground workers backing it up, this left-wing extremist movement has often been described as India's biggest internal security challenge. An heir to the radical left-wing extremist movements which were born in the state of West Bengal in the 1960s, the CPI-Maoist aims at capturing power by waging a people's war—a war that made up of a relentless onslaught on every symbol and institution of the state. Unlike its ancestors in West Bengal, the CPI-Maoist has proved resilient. With the exception of Andhra Pradesh, where police have inflicted serious reverses on the movement over the past five years, none of the states affected by the extremists have been able to put together an effective response. An average of 800 fatalities have been reported across the country in left-wing extremist violence during each of past four years.

Prior to the elections, the CPI-Maoist had not only called for a boycott of the poll process but, in the words of Union Home Minister P. Chidambaram, had "done all it could do to disrupt the elections." However, Maoist violence on April 16 succeeded in impacting less than one percent of the 76,000 polling stations that had been identified as vulnerable to Maoist attack. Moreover, the killings remained confined to just three states—Bihar, Jharkhand and Chhattisgarh. Jharkhand, in India's east, alone accounted for nine fatalities. In the neighbouring state of Chhattisgarh, five poll management staff became unintended victims of a Maoist improvised explosive device. The CPI-Maoist later apologized to the family members of the victims, explaining that its cadre had mistaken the dead civilians to be security force personnel.

Significantly, though, no killings occurred either in the eastern state of Orissa, which is gradually emerging as the new hotbed of Maoist violence, or in neighbouring state of Andhra Pradesh, the erstwhile extremist citadel. The lack of violence was also reflected in a reasonable to high turnout of voters in states like Chhattisgarh which recorded 51 percent voting and Andhra Pradesh where 65 percent voters cast their ballot in the first phase. Apart from a few areas, where local grievance against the government combined with Maoist ban on elections to record zero polling, the voting process, across the Maoists were unable to enforce their call for an election boycott.

The 18 deaths, on April 16, however, were sufficient recipe for media outcry. Declaring it the "most violent election" prominent newspapers ran headlines such as "India votes amid bullets, blasts", "It began with a bang" and "8 cops among 16 dead in Red Rampage". Little attention, however, was given to the fact that the CPI-Maoist had suffered losses in the run-up to the elections, significantly degrading its capabilities. In two incidents in the state of Bihar, for example, security forces had managed to kill several CPI-Maoist cadre who were involved in attempts to abduct political activists. Moreover, the CPI-Maoist had been unable to execute significant anti-election violence in the build-up to April 16. Bar the killing of a candidate belonging to a non-significant party in Orissa and the detonation of bombs in buildings that were to be used to house poll security personnel, no major attacks took place. Again, on April 22, some 200 Maoist insurgents seized a train for few hours in Bihar. However, they released the train and its passengers some hours before voting began. The 'train hijack' incident attracted significant international media attention, but did nothing to deter voters from exercising their franchise.

1

Despite media hype, Maoist violence in the Indian elections has been limited.

2

Both pro-active policing and cooption by political parties helped defend the democratic process

3

However, the new government will have to place the growing Maoist threat high on its agenda.



### **Tactical Challenges**

The polls were held in extremely challenging circumstances, with poll parties often required to trek kilometers inside Maoist-dominated forest areas constantly exposed to attack. The elaborate security cover laid out by the India's Ministry of Home Affairs and the Election Commission included an alert to the Indian Air Force in central and eastern India, which deployed 25 helicopters for emergency operations; deployment of an additional 50,000 paramilitary forces; and intensified patrols in all sensitive areas.

But the fact that elections were being held in several Maoist violence-hit areas at the same time stretched the security forces available for the task to the limit. The Election Commission later justified holding the polls in all the Maoist affected areas in the first phase, saying that the decision gave the security forces at least three weeks' time for "area domination" in those areas, a luxury that would not be available if polls in these areas were to be held in separate phases.

In practice, though, the desired level of area domination was not possible because of the non-availability of adequate number of security forces. Not long ago, in November 2008, presence of 300 paramilitary companies had ensured near zero-violence during the State Assembly elections in Chhattisgarh, the State worst affected by Maoist violence. This time around, Chhattisgarh was allotted only 160 additional companies. In Jharkhand, 96 paramilitary companies were provided against a request of about 220 companies. Bihar received 130 companies while it had asked for 260 companies.

The two major military attacks by the Maoists before the elections—on April 10, they killed 10 paramilitary personnel in Chhattisgarh and five more on April 11 in Jharkhand—were, as the Indian Ministry of Home Affairs argued, the consequence of a "pro-active approach adopted by the security forces to foil the designs to disrupt the poll process". Given the scale of the threat, India's security forces did reasonably well in defeating the CPI-Maoist's efforts to sabotage the elections. However, better security planning and management would likely have further reduced the levels of violence.

### **Cooption and Collusion**

The relatively low levels of violence and disruption were, also at least in some cases, the result of need-based political collusion between various candidates and the Maoists, which ensured the absence of attacks in a number of vulnerable polling stations. In remote constituencies of Orissa, Jharkhand and Bihar, political parties had entered into agreements with the Maoists for a time-bound peace.

Little, however, can be read into the gains made by the state or the deliverance of the promise made by the Indian Home Minister P Chidambaram to hold a "peaceful election". The temporary peace that particular political formations may have purchased during the elections is bound to lapse in quick time. The large-scale mobilization of paramilitary companies for the areas going to the polls will not be available to these States after the elections.

The limited disorders during the polls, thus, are not accurate indices of any significant reverses inflicted on the Maoists by the Indian state in areas where their influence has been the maximum. There has been no dramatic augmentation of capacities on the part of the state and its agencies vis-à-vis the Maoists. Most of the worst affected States continue to dither and squirm at putting together an effective response to the threat of left-wing extremism, despite the striking example of Andhra Pradesh, which five years ago was the worst Maoist affected state, but managed to force the Maoists out of its territory through effective Police action.

Policing in most of the left-wing extremism affected states remains poor and highly inadequate to take on the rampaging extremists. As a result, states remain over-dependent on the paramilitary whose unavailability affects the counter-extremism efforts of the states. The efforts to modernize the police remains tardy and marked by myopic implementation. For example, states have not been able even to spend the funds made available by the central government for police modernization. According to a recent performance audit review of Police modernization across 16 States released by the Comptroller and Auditor General of India, Maoist-affected States like Orissa, Andhra Pradesh and Jharkhand not only kept 30 to 60 percent of available funds unutilized, but on occasions, diverted them to incur expenses that in no way added to the capacities of their police force.

A new government will assume power in New Delhi in May. It is bound to discover that in spite of the peaceful elections, the threat of the Maoists remains a reality and also a growing challenge that it cannot afford to close its eyes to.

# The Philippines' counter-terrorism approach

Carlos Quita



The Philippines' rich counter-insurgency experience with confronting rebel groups with disparate affiliations and objectives, spans more than five decades. The country's whole-of-government approach to addressing the long-drawn out internal security problem has influenced some of the new approaches in counter-insurgency, counter-terrorism and counter-radicalization. In the context of radicalization and de-radicalization, the Philippine case is replete with lessons, particularly on the many factors that influenced ordinary citizens to embrace the dangerous and tumultuous life of a rebel or terrorist and why they revert back to mainstream society.

The Philippine government confronts security threats from three major groups. The first is the Maoist-Leninist-Marxist-inspired communist terrorists movement (CTM) composed of the Communist Party of the Philippines (CPP), the New Peoples Army (NPA), and the National Democratic Front (NDF). From its peak strength of more than 25,000 in 1988, it has dwindled to around 4,800 red fighters. The second threat is the Southern Philippines Secessionist Groups (SPSG), principally the Moro Islamic Liberation Front (MILF) which grew to its present strength of 11,500 fighters when an estimated 1,500 rebels affiliated with the Moro National Liberation Front (MNLF) defected to the MILF when the MNLF signed a peace agreement with the government in September 1996. The third is the Abu Sayaff Group with about 400 terrorists in Sulu archipelago and Basilan Island. It is notoriously known for its kidnap-for-ransom activities and beheading of captives and has been a willing host to Jemaah Islamiyah elements.

## The Roads to Radicalization.

**The CTM's Arouse-Organize-Mobilize Methodology:** With lessons from the long-drawn out insurgency, the resilient CTM has evolved into what it is now. Its approach to organizational expansion and wielding power are firmly anchored in the use of terrorism and co-optation of its target audiences, usually by sectors, through the Arouse-Organize-Mobilize methodology. In the arousal stage, the insurgents agitate using issues such as poverty, injustice, and human rights abuses that relate to the masses. The people are then enticed to join in a specific group. Once organized, members are enjoined to actively participate in the group's mobilization for mass action. Lasting for months and even years, the course is punctuated by continuing education on communism, rights of indigenous people, communist values, and military tactics. At the same time, targets for recruitment are screened in the process and those with potential to be hardcore members undergo separate indoctrination sessions. Most of those who advanced ahead of their contemporaries become cadres, party members, and even politicians who can participate in the CTM's parliamentary struggle. The rest may end up as militia members, regular fighters, or runners.

**The Moro Ethno-Cultural Methodology:** The Moro rebellion is claimed to be a struggle to defend Islam and preserve the Moro people's identity. To achieve its objective of an independent Islamic State that is based on the doctrine of Allah's sovereignty, the MILF has a four-point program, namely: Islamization, Organizational Strengthening, Military Build-up, and Self-Reliance.

In carrying out the process, Islamization is incorporated in all aspects of life at the level of the individual, community and the revolutionary movement. The need to Islamize the environment before independence is achieved has been the main driver for recruitment of its principal adherents. Radicalization may start in any of the following ways:

- Exploitation of seminaries to promote the secessionist cause.
- Conversion of non-Muslim recruits to the Islamic faith and radicalizing them in the process.
- Establishment of combined military bases and mosques, to promote the MILF's interpretation of Muslim culture.
- Use of legal fronts such as Islamic NGOs funded by some Middle East countries to propagate Islamic militancy.

1

The Philippines 'whole-government' counter-terrorism doctrine is replete with lessons

2

Cultural education has been a key component of the Philippines' counter-terrorism efforts

3

Counter-radicalization programs work best when all arms of the government are involved

⇒



### **The National Intervention Programs for Counter- Radicalization**

Just as the insurgents and terrorists continue to adapt to their environment for survival, so has the government's counter-insurgency approach evolved. The government's policy for achieving peace is underscored in the Six Paths to Peace defined in Executive Order Number 3, 2001: (1) Pursuit of Social, Economic and Political Reforms; (2) Consensus-Building and Empowerment for Peace; (3) Peaceful Negotiated Settlement with Different Rebel Groups; (4) Programs for Reconciliation, Reintegration into Mainstream Society and Rehabilitation; (5) Addressing Concerns arising From Continuing Armed Hostilities; and (6) Building and Nurturing a Climate Conducive to Peace.

All peace accords have a humanitarian and rehabilitation aspect such as those concluded with the MNLF, and the former Cordillera People's Liberation Army (CPLA). Towards this end, integration of former rebels into the mainstream of society started in 1994 under the National Reconciliation Development Program which was renamed the National Program for Unity and Development (NPUD) in 2004. A total of 39,975 former rebels of different affiliations benefited from this program.

In March 2007, the President issued Administrative Order 172 declaring the Social Integration Program as an enhanced amnesty, reintegration and reconciliation program to integrate former rebels into the mainstream of society. Some 445 members of the CPP/NPA/NDF had benefited from this program since its implementation in 2008.

The reformation of surrendered, captured and convicted rebels and terrorists who fall under the rehabilitation program is being carried out by various government agencies and institutions. The military and police re-indoctrinate these radicals to get their cooperation for future operations. Some of them are active in the ongoing government campaign to inform the public of the large-scale deception being waged by threat groups.

### **Cultural Education as a Tool to Counter-Radicalization**

Since radicalization entails conditioning the mind to extreme and aggressive behavior largely through cultural mechanisms, it is only logical that cultural education be one of the major tools for counter-radicalization programs.

The government's Madrasah Education Program addresses the needs of the Muslim youths for quality basic education that is compatible with the tenets of Islam. In line with this program is the increase in government-accredited Madaris from 633 in 2007 to more than a thousand. Different donor countries provided funds for the training of *asatidz* (teachers), printing of textbooks, construction of madaris, and the information drive.

Promotion of inter-faith dialogue to build mutual trust among various religions and cultural groups is one of the comprehensive initiatives of the Philippines. The Armed Forces of the Philippines also conducts the following pro-active initiatives which resulted to the surrender of hundreds of insurgents:

- The Special Advocacy on Literacy/Livelihood and Development for Muslims which emphasizes cultural awareness and understanding among the Muslims, Christians and indigenous peoples to promote social harmony and socio-economic alleviation through literacy and livelihood programs.
- The Army Literacy Patrol System which aims to provide elementary education to children in conflict-affected areas; and
- The Special Operations Team concept which harnesses the cooperation of the local government units, the community and other stakeholders to neutralize the AOM methodology of the CTM and win the insurgents and the masses to the side of the government.

### **Some Findings on Disengagement.**

A survey on the disengagement of 230 communist rebels (out of the 767 who availed of the NPUD from 2000 to 2003) revealed the following findings:

- 73 % of the respondents fall within illiterate to elementary education level.
- 77 % joined the movement due to CTM's agitation/propaganda through AOM
- 32% surrendered due to government's program; 26% due to hardship, 23% for family reasons, and the rest for various reasons.
- Propaganda themes that affected them most: 56 % - poverty; 33 % - disillusionment with the government; and 11 % - human rights abuses.

In conclusion, it is clear that counter-radicalization of rebels, terrorists and militants can be best achieved through a holistic program involving the entire government machinery, the people, and other key players. Moreover, the approach should include pro-active measures to be able to immunize the citizens from recruitment long before the seed of radicalization is implanted •

# Asian Conflicts Reports

## Council For Asian Terrorism Research

### Editors

Dr. Caroline Ziemke | Institute for Defense Analysis, Washington, D.C.  
Praveen Swami | Associate Editor, *The Hindu*, New Delhi.  
Shanaka Jayasekara | Macquarie University, Australia

### About the Authors

KATSUHISA FURUKAWA is Fellow at the Research Institute of Science and Technology for Society, Tokyo

\* Based on ANTHONY BERGIN, SULASTRI BRE OSMAN, CARL UNGERER and NUR AZLIN MOHAMMED YASIN co-authored research report published jointly by the S. Rajaratnam School of International Studies in Singapore and the Australian Strategic Policy Institute in Canberra.

BIBHU PRASAD ROU TRAY is Fellow at the Institute for Conflict Management, New Delhi.

CARLOS F. QUITA is a member of the Strategic and Integrative Studies Center and the concurrent Chief of Operations of the Philippine Army.

The opinions expressed in Asian Conflicts Reports are those of the individual authors and do not necessarily reflect the views of the Council on Asian Terrorism Research Executive Board or its member institutions.

The Council on Asian Terrorism Research includes as its members:

Afghanistan: Centre for Conflict and Peace Studies | Australia: Centre for Policing, Intelligence and Counter Terrorism, Macquarie University | Bangladesh: Bangladesh Institute of International and Strategic Studies | Bangladesh: Bangladesh Institute for Peace & Security Studies | India: Institute of Conflict Management | Indonesia: Center for the Study of Islam and Society, State Islamic University of Indonesia | Japan: Research Institute of Science and Technology | Malaysia: Southeast Asia Regional Centre for Counter Terrorism | Pakistan: Pakistan Institute for Peace Studies | Philippines: Strategic and Integrative Studies Center | Philippines: Philippine Institute for Political Violence and Terrorism Research | Singapore: International Centre for Political Violence and Terrorism Research, Nanyang Technological University | Sri Lanka: Sri Lanka International Centre for Terrorism Research and Conflict Management | USA: Institute for Defense Analyses |

For inquiries about CATR or Asian Conflicts Reports:

Dr. Caroline Ziemke,  
SFRD, Institute for Defense Analyses,  
4850 Mark Center Drive,  
Alexandria VA, 22311, USA.  
E-mail: [cziemke@ida.org](mailto:cziemke@ida.org)

