FORUM

sending

SECURING THE
CYBER REALM

PLUS **The Power of Social Media and
A Holistic Approach to Security**

features

30

departments

67

ABOUT THE COVER:
This photo illustration
represents the convergence
of real- and virtual-world
threats. The artist suggests
that preventing cyber attacks
proves as critical as defending
against real-world attacks.
FORUM ILLUSTRATION

Dear Readers,

U.S. PACIFIC COMMAND

Developments associated with information technology have revolutionized the way governments, corporations, societies and ordinary citizens interact with one another. The cyber revolution has spurred globalization more than any technological development. That is why assuring the free flow of information, the protection and privacy of data, and the integrity of interconnected networks are essential to international economic prosperity, security and the promotion of universal rights. With that in mind, the United States recently published its *International Strategy for Cyberspace* to promote the innovation that not only drives the American economy but also improves lives of individuals around the globe.

The potential benefits of a secure and reliable cyberspace environment are astounding. This domain — which is every bit as important as the more traditional land, air, sea and space domains — inspires entrepreneurial innovation and interconnects individuals in all nations. More broadly, it builds better governments, safeguards fundamental freedoms, improves communications and builds understanding among people of every nationality, race, faith and educational background. When used appropriately, cyber capabilities ultimately enhance national and international security.

This is why cyberspace must be protected and why failure to do so poses such a danger to individual privacy, societal success and international security. Only by working together — as individuals and as governments — can we realize the potential for secure networks to enhance the common good. Criminal behavior in cyberspace, however, is a reality that must be contained and countered. The United States, while adhering to the principles and values of a free and open society, is committed to confronting those who dismiss international norms and standards of behavior.

The U.S. military plays a vital role in protecting the free flow of information. Indeed, the Department of Defense — including U.S. Pacific Command — contributes every day to U.S. Secretary of State Hillary Clinton's initiatives to combine defense along with diplomacy and development to enhance prosperity, security and openness, so that all can benefit from digital technology. U.S. Pacific Command depends on reliable and secure networks to underpin security throughout the Asia Pacific; therefore, we continue to strengthen our network defenses and our ability to withstand and recover from cyber disruptions, intrusions and attacks. Along with our allies and partners, U.S. Pacific Command encourages responsible behavior and opposes those who seek to disrupt networks and systems. Our collective security can only be realized when we work together to build a future for cyberspace that is open, interoperable, secure and reliable; we invite all nations and peoples to join us in that effort.

I hope that you enjoy this issue of *Asia Pacific Defense FORUM*. As usual, the magazine is full of interesting and informative articles on a wide variety of topics. For additional information or to provide comments, please contact us at **contact-apdf@apdforum.com**.

All the best,

Robert F. Willard

ROBERT F. WILLARD
Admiral, USN
Commander, U.S. Pacific Command

China's
vacation destination

Visit the Maldives, and there's a high chance the fellow vacationers at your island retreat will be from China, according to July 2011 figures that show the Asian giant as the biggest source of visitors.

The Maldives, a string of low-lying islands fringed by azure waters and white sand in the Indian Ocean, has long been popular as a luxury honeymoon destination for Europeans — but times are changing.

"China has emerged as the biggest source of tourists for the Maldives, displacing our traditional markets of Italy, the U.K. and Germany," said Simon Hawkins, an official from the Maldives tourism authority.

The Maldives welcomed 65,148 Chinese tourists in the first five months in 2011, a 56.7 percent gain over the same period in 2010, according to figures given by Hawkins. Agence France-Presse

AGENCE FRANCE-PRESSE

THAILAND

METHAMPHETAMINES *as art*

Thai authorities arrested an Iranian man who allegedly tried to smuggle more than 50 million baht (U.S. $1.68 million) worth of crystal methamphetamine into the country disguised as handicraft art.

The Customs Department said 28-year-old Safi Zadeh Hossein was carrying two plaque-shaped sculptures when he was arrested in July 2011 on arrival at Suvarnabhumi International Airport from Damascus, Syria.

Customs officials demonstrated to reporters how the sculptures were pressed and molded from the illegal stimulant. One 10-kilogram object was in the image of a yellow rose, left, and a 5-kilogram piece looked like a framed cameo.

Official Vorapat Jaovisidha said it was the first time his agency had seen this method.

The Associated Press

THE ASSOCIATED PRESS

VIETNAM

Turtle *freed*
AFTER TREATMENT

AGENCE FRANCE-PRESSE

A more than century-old giant turtle revered as a symbol of Vietnam's independence struggle won back her freedom three months after being captured for medical treatment, according to officials.

The animal, a *Rafetus swinhoei* turtle, one of only four known of its kind, was successfully treated at a special pond on an islet in central Hanoi's Hoan Kiem Lake, said Le Xuan Rao, director of Hanoi's Department of Science and Technology.

"Her health condition is good, no more ulcers on the body," he said, a day after she was released back into the lake in July 2011. "Everything went smoothly."

The soft-shell turtle, which weighs about 169 kilograms, had been injured by fish hooks and small red-eared turtles that have appeared in the lake in recent years, according to local media reports.

The animal is revered in Vietnam because a turtle from the lake guards the magical sword of 15th-century rebel Le Loi, who drove out Chinese invaders and later became emperor, and keeps it safe for future use, according to legend.   Agence France-Presse

MASSIVE URANIUM DISCOVERY

A new mine in south India could contain the largest reserves of uranium in the world, a government official said in July 2011. The find is a major boost for the energy-hungry nation, especially since Iran has threatened to halt oil supplies to India to resolve a dispute over the U.S. $12 billion annual crude trade between the two countries.

The Tumalapalli mine in Andhra Pradesh state could provide up to 150,000 tons of uranium, Srikumar Banerjee, secretary of the Department of Atomic Energy, told reporters.

"It's confirmed that the mine has 49,000 tons of ore, and there are indications that the total quantity could be three times that amount," Banerjee told *The Times of India*. "If that be the case, it will become the largest uranium mine in the world," he said. India gets less than 3 percent of its energy from atomic power, and it hopes to raise the figure to 25 percent by 2050.

Agence France-Presse
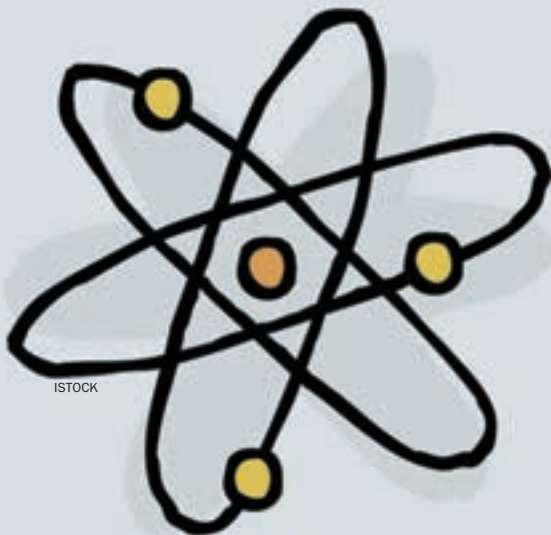
ISTOCK

AGENCE FRANCE-PRESSE

Fabled "puzzle" temple reopened

An ancient Angkor temple in northwestern Cambodia was reopened to the public in July 2011 after the completion of a decades-long renovation project described as the world's largest puzzle.

The restoration of the 11th-century Baphuon monument, one of the country's largest after Angkor Wat, was celebrated with a high-profile ceremony attended by Cambodian King Norodom Sihamoni, center, and French Prime Minister Francois Fillon, right.

The finished project is the result of half a century of painstaking efforts by restorers to take apart the crumbling tower's 300,000 sandstone blocks and then piece them back together.

"The work at Baphuon has been exceptional," Fillon said at the inauguration event in the northwestern tourist hub of Siem Reap, which drew thousands of Cambodians waving French, Cambodian and European Union flags.

King Sihamoni expressed his people's "profound gratitude to France" for completing the 10 million-euro (U.S. $14 million), French-funded undertaking. Agence France-Presse

CAMBODIAN MUSLIMS
SEEK JUSTICE

AGENCE FRANCE-PRESSE

Zakaria Bin Ahmad cannot forget the years of horror under the brutal Khmer Rouge when even praying was to risk death for Cambodia's persecuted minority Muslims.

Many others in his community did not survive the late 1970s reign of terror by the hard-line communist regime, which executed Islamic scholars, destroyed mosques, forced Muslims to eat pork and forbade headscarves.

"People tried all kinds of ways to pray. Sometimes while they were driving an ox cart … sometimes in the jungle when we asked to use the toilet, and sometimes while we were washing," the 61-year-old recalled.

But mostly, he remembers people disappearing, never to be seen again.

"Many were killed," he said quietly in July 2011 in his modest home in the shadow of a modern blue-domed mosque, a source of pride for the town of Chraing Chamres, whose earlier place of worship was destroyed by the Khmer Rouge.

Cambodian Muslims, known as Cham, hope finally to see justice as the most senior surviving Khmer Rouge leaders stand trial for genocide at Cambodia's U.N.-backed court over the treatment of the ethnic and religious minority.

"Now we can tell our story," said Sales Pin Apoutorliep, the religious leader, or hakem, of the Chraing Chamres mosque.

"We fully support the trial to tell the truth and to say what happened under the Pol Pot regime," he said, referring to the regime's main founder, who died in 1998 having escaped justice.

The high-profile genocide trial, which opened in late June 2011, carries particular poignancy for the Cham, whose bloody persecution is an often overlooked chapter of the country's "Killing Fields" era.

Before the genocide charges were filed against the former Khmer Rouge leaders, the treatment of the Muslim minority was rarely discussed.

"In the past, there was little mention about the suffering of the Cham under the Khmer Rouge regime," said Farina So, an expert at the Documentation Centre of Cambodia (DC-Cam), which researches Khmer Rouge atrocities.

"The Chams' suffering has not been investigated much," she added. "They need recognition from the people."

Nobody knows exactly how many Muslims died under the totalitarian movement, which wiped out nearly a quarter of the population.

But the DC-Cam estimates that 100,000 to 500,000 of the country's 700,000-strong Cham community died at the hands of the regime.

"It's still fresh in our eyes," Sales, who lost his parents and four of his siblings under the Khmer Rouge, said after finishing his midday prayers. "Every family has pain."

The mass killings of Muslims, along with an estimated 20,000 Vietnamese, form the basis of the genocide charges against the four Khmer Rouge defendants, who include "Brother Number Two" Nuon Chea and former head of state Khieu Samphan.

The four also face a string of other charges, including war crimes and crimes against humanity for the deaths of up to 2 million people through starvation, overwork or execution in a doomed bid to create an agrarian utopia.

Most of those deaths do not fall under the charge of genocide, which is defined by the United Nations as "acts committed with intent to destroy, in whole or in part, a national, ethnic, racial or religious group."

The indictment filed against the four elderly defendants states that "the Cham were systematically and methodically targeted and killed" and that the Khmer Rouge sought to eliminate Cham culture, traditions and language.

Today, there are about half a million Cham in Cambodia, the majority of them followers of Sunni Islam, and they enjoy full freedom of religion.

But like so many in the Southeast Asian nation, they remain haunted by the past. "They reconstructed mosques. They revived their religious and ethnic identity. They opened Islamic schools and taught Islam," Farina So said. "They are trying to recover from this trauma, but it's a slow process."

Ahmad's daughter-in-law Yakin El, wearing a traditional, long-sleeved dress with matching headscarf, said she was "shocked" when as a young girl she first learned of her relatives' ordeal under the Khmer Rouge.

"I'm pleased that they will bring up the Cham suffering during the trial," the 24-year-old said. "It's the past, but I can't forget it because most of the Muslims were killed at this time. We have to remember them."

Cambodians wait to attend a trial of former top Khmer Rouge leaders at the country's U.N.-backed war crimes court in June 2011 in Phnom Penh, Cambodia.

AGENCE FRANCE-PRESSE

Nuon Chea, left, former Khmer Rouge leader "Brother Number Two," and Khieu Samphan, right, former Khmer Rouge head of state, sit in a Phnom Penh courtroom in June 2011. They and two other regime leaders face charges of genocide, crimes against humanity and war crimes during the communist movement's brutal 1975-79 rule.

AGENCE FRANCE-PRESSE/MARKE PETERS/ECCC

SECURING THE CYBER SPHERE

RETHINKING MILITARY DOCTRINE FOR A NEW DEFENSE ERA

JOHN BUMGARNER

"One must change one's tactics every 10 years if one wishes to maintain one's superiority."

Napoleon Bonaparte, 1769-1821

Militaries have had to continually evolve over the past century to keep pace with advancements in weaponry and technology. Recent clamoring about the grave possibility of nations becoming entangled in cyber combat is once again forcing armed forces to rethink their battle plans for future conflicts. Operating in the cyber defense era, militaries will need to examine every aspect of their current doctrine to confront the challenges of the 21st century battlefield.

Many of the fundamental military strategies and tactics in use will need to be reshaped to take into consideration how technology can be applied in both conventional and asymmetric warfare. Additionally, nearly every military occupational specialty will require cyber-oriented training to meet the future challenges imposed by cyber warfare. Due to the anonymous nature, stealthiness and speed of cyber attacks, militaries will need to re-examine their decision processes linked to their customary response strategies.

Another essential part of these cyber defense era transformations will be the continual assessment of cyber threats against current weapon systems. All future weapon systems will need to be designed to limit their disruption or destruction from cyber attacks.

At a conference in February 2011, Sri Lankan Army chief Jagath Jayasuriya said the country still faces the threat of cyber war from sympathizers of the defeated Tamil Tiger rebels.

AGENCE FRANCE-PRESSE

BUILDING THE CYBER WARRIOR

During the industrial defense era, countries within the Asia-Pacific region developed their militaries to counter traditional threats in traditional spheres – air, land and sea domains. Over the past decade, several countries in this vitally important region have begun to develop capabilities to defend or advance their national interests in cyberspace, the newest domain of modern warfare. Some of the current groundwork under way in the region is the integration of cyber warfare units into existing military force structures.

For instance, the Republic of Korea established a cyber warfare unit within its military force structure in early 2010 to defend its military networks against cyber attacks and to provide offensive cyber capabilities.

In 2011, the South Korean government announced its intention to establish and fund a Cyber War Department within a prestigious university. This new department will provide a technology-rich academic curriculum interwoven with courses in cyber war tactics and psychology. Its graduates will be required to serve seven years in the Republic of Korea Armed Forces as cyber war specialists. The military expects to have a fully operational cyber command by 2012.

Over the past decade, China has made remarkable progress in developing its military capabilities in all the domains of warfare including cyberspace. Historically, the Chinese military has not publicly acknowledged the existence of cyber warriors in its ranks, but the military recently confirmed the existence of an elite cyber warfare
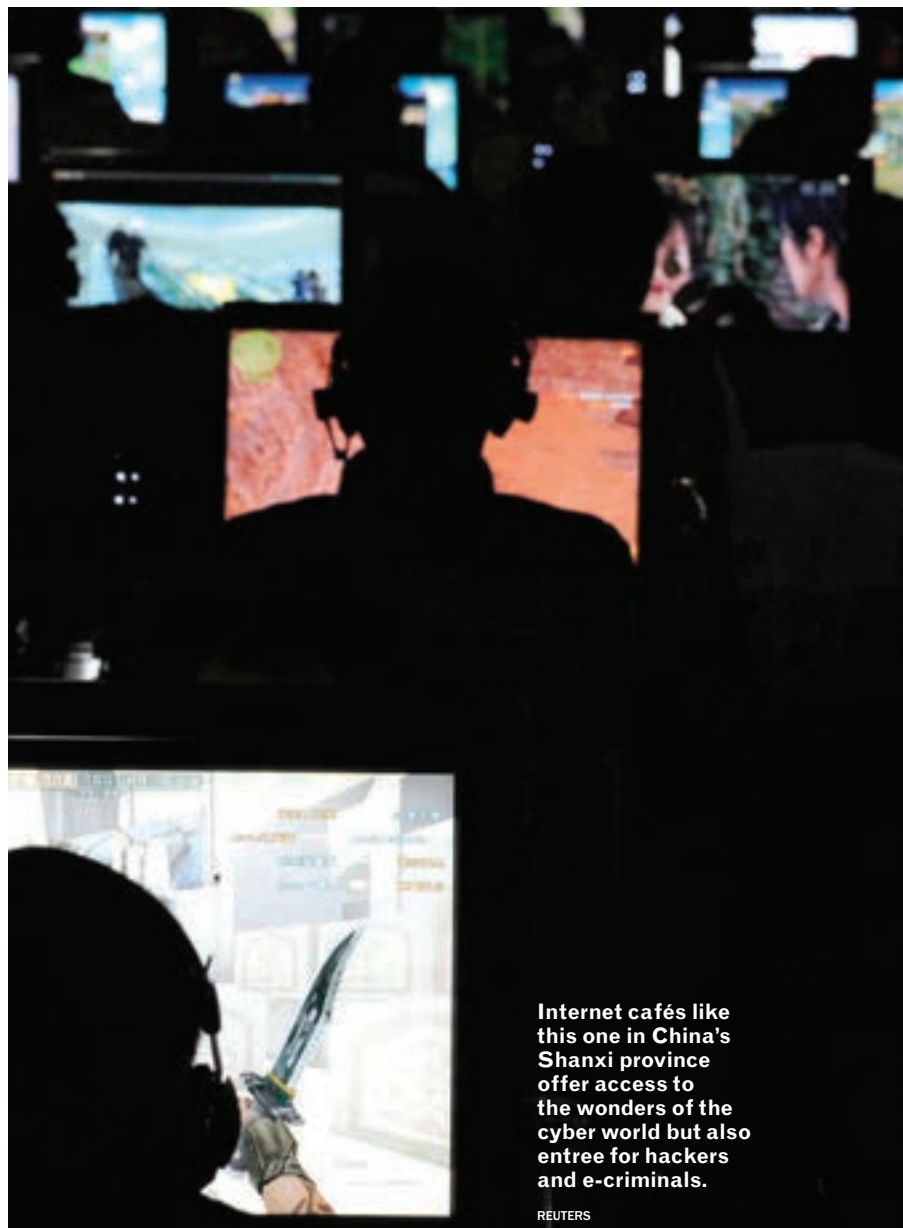
Internet cafés like this one in China's Shanxi province offer access to the wonders of the cyber world but also entree for hackers and e-criminals.

Analysts at a U.S. cyber security center use a range of tools to identify and prevent potential cyber attacks.

unit called "Blue Team." The publicly declared mission of this cyber microforce is to assess the computer networks of the People's Liberation Army to uncover vulnerabilities that could potentially undermine military readiness. For many years, the People's Liberation Army has been developing cyber warriors through rigorous academic programs in important state-sponsored schools. Similar government-funded academic programs in the United States have proven effective in developing a cadre of talented cyber warriors.

Taiwan integrated cyber warfare capabilities with traditional military operations early on, as illustrated by the Han Kuang joint-forces exercise of 2000. During this exercise, thousands of computer viruses were unleashed by opposing elements in an attempt to paralyze the military command, control and communication networks. Since that exercise, Taiwan's military has continued to expand its cyber warfare capabilities through intense training and recruitment of cyber warriors into the armed forces.

Force structure changes are also occurring within the Indian Armed Forces. The current Singh government has directed the establishment of a national Cyber Command and Control Authority to assist the government of India with addressing the cyber challenges ahead.

ENHANCING SITUATIONAL AWARENESS

For these cyber warriors to be successful in real-world operations, they need to understand how a rapid decision cycle to counter cyber events can be applied to events when every nanosecond counts.

One of the key elements to accomplishing this is the development of in-depth situational awareness architecture in cyberspace. Developing a comprehensive framework is crucial for a military seeking to react quickly to unfolding incidents that could potentially provide an opponent with an advantage. The Japan Self Defense Forces recently held cyber warfare discussions with the countries of Australia and

South Korea with the goal of developing regional cyberspace cooperation that could improve military situational awareness for all participants.

An integral component of any successful situational awareness program is the assessment of military weapon systems and other equipment (for example, tactical radios) for any known or unknown cyber-related vulnerabilities. The 21st century battlefield is littered with military equipment, such as main battle tanks, satellite communication architecture and unmanned autonomous vehicle battlefield surveillance systems that contain sophisticated electronic components that can be targeted by cyber warriors. The importance of these assessments is underscored by the discovery of various malicious computer programs in recent years. Some of these computer worms, or self-replicating malware, might have been discovered sooner if militaries had been performing regular cyber assessments. Militaries that fail to conduct these assessments

throughout the lifecycle of any defense-related component could potentially overlook critical cyber sabotage vectors that enemy forces could utilize for an attack.

FUTURE SHOCK

The cyber defense era has the world in the midst of another revolution in military affairs. Future challenges will surely include: rethinking perimeter strategies to defend our ever-shifting cyber borders, revisiting counterinsurgency strategies to handle neo-combatants such as "technopatriots," re-evaluating intelligence collection in a rapidly expanding digital world, and re-examining the thorny problem of attribution in cyberspace.

The Asia-Pacific region will likely be the world's "proving ground" for much of the cyber warfare doctrine that will be developed and tested in the cyber defense era. □

John Bumgarner is chief technology officer for the U.S. Cyber Consequences Unit. He has served as an expert source for various publications, including *Businessweek*, BBC, CNN, *Jane's Defence Weekly*, Reuters, *The Guardian* and *The Wall Street Journal*.

CYBER CRIME STOPPERS

COOPERATION IS SOUGHT TO BALANCE INDIVIDUAL
AND GROUP RIGHTS IN THE NEW FRONTIER

FORUM STAFF

Police in Indonesia, Cambodia, Malaysia, Thailand, Taiwan and China joined forces in an unprecedented operation in June 2011 and arrested nearly 600 mainly Chinese and Taiwanese nationals in a transnational Internet and fraud ring. The suspects allegedly defrauded thousands of Asia-Pacific citizens by posing as employees of a phony company that provided financial services such as selling stocks over the Internet, according to accounts in *The Jakarta Globe* newspaper.

The 177 nationals arrested at the behest of Chinese and Taiwanese police in Indonesia had rented houses with broadband Internet access and placed calls via the Internet "to many victims in China, Taiwan, the Philippines and Vietnam in which they [individually] posed as an official to extort money," Jakarta Police Chief Inspector General Sutarman told *The Jakarta Globe* in June 2011.

The criminal syndicate ran a myriad of other scams across the Asia-Pacific region. Thai police Col. Phanthana Nutchanart told reporters that "the two main tricks [were] to surprise the victim, for instance by telling them they have won the lottery, or to frighten them by saying their bank account or credit card was suspended."

Taiwan's police chief, Wang Cho-chiun, told reporters that the arrests would "help substantially reduce fraud cases." He noted that the mass bust "was also the first time Taiwan and China police jointly investigated cases in a third country, and we believe this will set an example in joint crime fighting."

The transnational investigation illustrates the scope of the emerging challenges, as well as the role of cooperation, in keeping the cyber peace. As the Internet becomes more mobile through cellphones and social networks and more widely accessible around the world, growing numbers of Internet users see the World Wide Web as a free frontier to do as they please. Balancing individual rights and civic protections has become increasingly complex given the pace at which the cyber sphere continues to evolve. Extending the laws of society to this realm become even more challenging when navigating the expanse's seemingly borderless domain.

CYBER COOPERATION

Calls for more cooperation and regulation increasingly resound in voices throughout the Asia Pacific and around the globe. In particular, "active international partnerships are central to tackling cyber crime," James Brokenshire, crime and security minister in the United Kingdom, said at the July 2011 launch of the nonprofit International Cyber Security Protection Alliance in London. The alliance formed to combat cyber crime by linking governments and the private sector around the globe. "There needs to be an international response, including international treaties, bilateral treaties and common agreements between countries," he said, according to coverage in *Computer Business Review* magazine.

As part of a transnational cyber crime operation, Indonesian officials arrested 177 Taiwanese and Chinese nationals in Jakarta, Indonesia, in June 2011 for alleged involvement in Internet-based scams. The suspects cover their faces as they wait in an immigration detention room.

British and U.S. officials meeting in June 2011 at an Asia-Pacific security conference in Singapore also emphasized the importance of partnerships. They called for countries to join together and develop a "formal, international charter to prevent serious international tensions," according to *Computer Business Review*. Then U.S. Defense Secretary Robert Gates said avoiding these tensions requires rules "that let people know what kind of acts are acceptable, what kind of acts are not, and what kind of acts may in fact be an act of war," the magazine reported.

Recognizing that cyber crime is a universal problem, an International Workshop on Cooperation against Cybercrime in South Asia, held in Colombo, Sri Lanka, in April 2011, found that preventive measures, including education, are also key, according to a post on the Marvi Memon blog. The workshop included participants from Bangladesh, India, Maldives, Pakistan and Sri Lanka.

Similarly, the Organization for Economic Cooperation and Development met in Paris in June

"As the Internet becomes more mobile through cellphones and social networks and more widely accessible around the world, growing numbers of Internet users see the World Wide Web as a free frontier to do as they please."

A Malaysian man surfs a tourism website in Kuala Lumpur on June 16, 2011. That same day hackers targeted 51 Malaysian government websites, disrupting 41 of them, according to the Malaysian Communications and Multimedia Commission, the country's Internet watchdog.

AGENCE FRANCE-PRESSE

EMERGING CYBER REGULATION

FORUM STAFF

To address potential cyber threats and suppress crime, countries are already adopting new policies with varying degrees of control. Nations seem to have universally banned child pornography from the Internet. They diverge, however, when it comes to determining where to draw the line on the freedom to post and act online.

The mobility of bloggers and hackers and the speed with which they can post — or destroy material — prompted Australia to recently tighten its cyber laws. Australia's Attorney General Robert McClelland announced Cybercrime Legislation Amendment Bill 2011 in June that will allow the country to join the Council of Europe Convention on Cybercrime, the only binding international treaty on computer offenses, according to The Australian newspaper. The law gives Australian agencies the power to access information stored overseas during cyber crime investigations.

"The increasing cyber threat means no nation alone can effectively overcome this problem, and international cooperation is essential," McClelland told *The Australian*. "Australia must have arrangements domestically and internationally to be in the best possible position to fight cyber crime and cyber security threats."

China went so far as to draft a law in 2010 that requires communications companies to monitor their clients' activity and report whether any "state secrets" are revealed through online activity.

Human Rights in China, a nongovernmental organization, reports that Internet service providers there must now cooperate with investigators and prosecutors and take "active steps" toward stopping the transmission of information deemed to be state secrets. The law defines state secrets as "information that concerns state security and interest and, if leaked, would damage state security and interests in the area of politics, economy and national defense, among others," *The Telegraph* newspaper reported. Because of the law's vagueness, that could include practically anything that the Chinese government doesn't want publicized, according to *The Telegraph*.

Retired schoolteacher Zeng Hongling experienced China's heavy hand in censoring what goes on the Internet. Zeng criticized school construction that led to the death of thousands of children in the May 2008 Sichuan earthquake, and authorities detained Zeng on charges of "inciting state subversion."

"The [Chinese] government only sees a limited role for public opinion," Nicholas Bequelin told the *Los Angeles Times* newspaper in June 2008, while doing research for Human Rights Watch in Hong Kong. "Once they take charge of a situation, they start silencing other voices, because the party is keen to present itself in a favorable light. It does not want to be accountable to any other external institutions."

Slander and libel laws are increasingly being applied in cyberspace. One man's news in Malaysia, for example, didn't sit well with a local government official who sued and won a defamation lawsuit, according to reports published in July 2011. Amizudin Ahmat must pay U.S. $100,000 in damages and U.S. $33,000 in costs after losing a defamation lawsuit filed against him by Malaysia's Minister of Information, Communications and Culture, Rais Yatim, according to Reporters Without Borders. Ahmat had posted blog entries accusing Yatim of raping his Indonesian maid.

Yatim becomes Malaysia's first senior government official to sue a blogger, according to The Associated Press. Malaysian authorities frequently blame opposition bloggers for lies spread over the Internet in an attempt to tarnish the government's image, The Associated Press reported.

Human rights proponents, however, challenge the effectiveness of overly stringent regulations. They instead promote the Internet's role in promoting transparency and accountability. World Bank blogger Tanya Gupta wrote that in countries where Internet restrictions limit what news media can produce and distribute, social media can take on the role of "watch dog" by giving another avenue to express views and disseminate information.

"Like the Lernaean Hydra from Greek mythology which grew back two heads for every head that was cut off, the Internet is very difficult to control," Gupta wrote in an April 2010 blog post about the role mobile social media plays in improving governance in developing countries. "You can always shut down the office of a newspaper and put the editor in jail. But it is very hard to shut down one website without another emerging or [to] stop people from using social networks to spread news."

A blogger named BirdAbroad released this photo in July 2011 of a customer looking at products at an allegedly fake Apple store in southwest China's Yunan Province. The blogger revealed the supposed fraud to the world. The official stores only have the word "Apple" on their signs. The phony stores were so convincing that employees actually believed they worked for Apple co-founder Steve Jobs, who died in October 2011.

2011 to discuss ways to devise a set of principles for Internet use that extend globally. "Given the increasing centrality of the Internet to modern society, the worlds' governments are increasing their regulatory attention to the Internet to address a range of concerns," Leslie Harris, president and chief executive officer of the Center for Democracy and Technology, wrote in an opinion piece about moving toward a global Internet policy on her organization's website.

Harris, however, cautioned that such practices must not be allowed to hamper the power of the technology to continue to enhance lives. "In the process, some are forgetting — or are consciously seeking to repeal or limit — the policy choices that allowed the Internet to develop into

such a powerful platform for economic activity, democratic participation, and human development. Nations are seeking to impose new obligations on Internet service providers and other Internet intermediaries to filter and block content. They are seeking additional control over the design of networks to facilitate their surveillance. They are seeking to use key resources such as the domain name system to enforce rules governing users. The resulting regulatory babble has complicated and at times impeded global data flows, as claims of jurisdiction compete and laws clash. Worse, these escalating assertions of sovereignty threaten the fundamentally open characteristics that have made the Internet what it is today," Harris wrote. □

A HOLISTIC APPROACH TO
SECURITY

Militaries, police forces, customs agents and even citizens have roles to play in protecting nations

P.C. KATOCH/VETERAN LIEUTENANT GENERAL OF THE INDIAN ARMY

C ountries such as India have faced cross-border terrorism for decades. But the attacks in the United States on September 11, 2001, changed global perspectives and approaches to the issue. After September 11, the West was willing to take the fight to the terror organizations.

Today, terrorism poses a far greater threat on a daily basis than conventional conflict. Terrorists take aim at political, military, economic, environmental, social and civil targets. Those include transportation networks, national power grids, information grids, nuclear and atomic centers, financial institutions, as well as defense installations and their networks. Unconventional targets require ever-changing security measures.

Due to its dynamic nature, security is more challenging than ever. At its core, security remains the ability of the state to protect the well-being of its people. The players, however, have expanded beyond the military and police. The security sector has a role, as well.

BEYOND MILITARIES

Militaries alone cannot cope with the multifaceted threats that have emerged with globalization. The ability to conduct integrated operations with other components of the security sector is necessary. In addition to armed forces, special forces and paramilitary forces, the security sector should include police forces, coast guards, intelligence services, elements dealing with homeland security, ministries of defense, internal affairs, law and justice, human resources, customs and immigration services, and private security services. In fact, the security sector should include almost the entire citizenry, considering the requirement to put "a billion eyes on the ground" and the vital role of citizenry for effective deradicalization programs.

Civil society, in effect, becomes an adjunct to the security sector. The importance of the civil society was very aptly summarized by Gen. V.P. Malik, the Indian Army's former chief of army staff, when he said, "My long involvement with counterterrorism … makes me believe that civil society usually contributes more to the cause of preventing and countering terrorism than encouraging terrorism. Wherever active, it generates

Indian Border Security Force Soldiers patrol the India-Bangladesh border at Fulbari, Bangladesh, on the outskirts of Siliguri, India, in April 2011.

An Indian policeman guards the India Gate monument in New Delhi in July 2011 after triple bomb blasts hit Mumbai days earlier.

WHAT IS
VIOLENT EXTREMISM?

The term "violent extremist" may need to be rethought. Can there be "good" (nonviolent) and "bad" (violent) extremists? What are cyber extremists before the actual cyber attack to cripple critical infrastructure? Learning from Japan's Fukushima, imagine the consequences of a prolonged cyber attack on the power grid of a nuclear reactor, reducing the critical function of cooling to backup generators that themselves get overheated and have to be periodically switched off. Would it not be prudent to assume extremism is extremism without playing semantics of "violent" and "nonviolent"? The line between the two is so thin and overlapping that a classically clear division may not be possible in the first place.

awareness and provides a constructive outlet for the redress of grievances. It gives voice to the marginalized and vulnerable people, including victims of terrorism, and plays a critical role in ensuring that counterterrorism measures respect human rights and the rule of law."

Nontraditional actors, such as nongovernment organizations, foundations, charities, public-private partnerships and private businesses, are capable and credible partners in local communities. However, their credentials must be verified to guard against dubious agendas.

SECURITY STRATEGY
The role of the larger security sector should be to provide citizens with a safe and resilient nation state, while protecting national security, rule of law, and social, political and economic prosperity in the process.

The strategy, both at the national and state level, should be to undertake synergized operations in rallying local populations against extremist organizations and activities, destroying extremists and blending development with education and deradicalization. The issue needs to be addressed holistically within the larger framework against both terrorism and insurgency. The above strategy implies that the security sector will need to battle simultaneously at the moral and physical levels.

The center of gravity, the population, should be the objective. Weaning them away from the extremists and promoting deradicalization should be given top priority. The citizenry must be provided necessary security and assistance while extremists are simultaneously destroyed.

A military solution alone is not the key. Operations must be dovetailed with development and education to win over the population. Threats must be dealt with to strengthen legitimate rule of law to alleviate pressures that lead to instability. Counterterrorism and counterinsurgency efforts should be integrated. Periodic assessments should be ensured to retain effectiveness of the strategy and adapt it.

At the national level, the security sector has an important role to play in formulating and executing a strategy. This includes defining and disseminating clear political aims, strategy and policy to ensure the setup of a Unified Headquarters (UHQ) and National Counter Terrorism Centre (NCTC), an intelligence network, and near real-time access to elements on the ground. It also includes coordinating development and deradicalization plans, cutting off support to extremists, and defining a strategy for employment of Special Forces and Special Operations Forces.

The security sector has an equally important role to play at the state level — both in formulation and execution. This includes developing a UHQ with all the elements of the security sector and setting up a State Counter Terrorism Centre linked to the NCTC through the National Intelligence Grid.

TECHNOLOGY'S ROLE

Given the increasing use of modern technology by extremists, fighting elements must have adequate firepower, means of day and night surveillance, state-of-the-art communications, night fighting capability, mobility and explosives handling capability. Fighting units down to the Soldier and individual weapon platform should be equipped with situational awareness and battlefield management packages. Unity of command in integrated operations must be ensured. All source intelligence must flow naturally, so that troops do not have to look over their shoulders. Clear areas of responsibilities should be defined. Extremist leadership, nerve centers and links should be priority targets.

Special Forces should be employed as high-value target teams (integrated interagency) to dislocate the extremists' center of gravity and destroy their nerve centers, in addition to spearheading psychological and intelligence operations. These options should be exploited to develop both publicized overt capabilities and deniable covert capabilities to create necessary deterrence.

Intelligence and psychological operations should be well planned. Psychological operations should include sponsored media programs for police interrogation of

INTERNATIONAL COOPERATION

A critical prerequisite for an international counterextremist strategy is a comprehensive assessment of the threat (both domestic and foreign), ideologies, motives and grievances that drive these groups to extremism, as well as a forecast of their capabilities, changing tactics and possible targets.

International cooperation is possible only if there is collective will and sincerity. Double standards in dealing with different extremist groups or selective counterextremist operations will adversely affect the overall effort, especially considering the links between various extremist groups and the fluidity with which they change their names and merge with others.

Ways must be found to create a mechanism that serves both national interests and overall requirements. If countries act only when respective national interests are affected, then the overall global war on terrorism becomes a farce. The same is true of collaborative intelligence sharing, which must be total.

Indian Defense Secretary Pradeep Kumar, right, and Pakistani Lt. Gen. Syed Athar Ali shake hands during a two-day talk between the two nations in New Delhi in May 2011.

Indian students protest in Mumbai in May 2010, seeking justice for insurgent attacks.

During a protest in New Delhi in 2011, activists demand that Pakistan hand over alleged terrorists who attacked India.

captured extremists, civilians harmed by extremists and next of kin of civilians killed by extremists. Periodic net assessment of extremist networks versus security sector operations are a must.

Troops must be educated and motivated to respect the culture, religion, way of life and women in the area of operations, and they must understand that brutalizing a population is retrograde. Collateral damage must be avoided at all costs. As part of the overall strategy, operations should have a blend with development. The security sector should launch its own quick impact development projects in consultation/conjunction with locals.

By all indications, India will have to continue contending with both terrorism and insurgencies in the foreseeable future. We should coin and adopt a holistic strategy to cope with both these forms of extremism.

We must develop both publicized overt capabilities and deniable covert capabilities in order to create the necessary deterrence. We need to aim for self-sufficiency in fighting this war. □

SHARE YOUR IDEAS

Join the Discussion
We want to hear from YOU!

Asia Pacific Defense FORUM caters to military and security personnel in the Asia-Pacific region. A product of U.S. Pacific Command, the quarterly magazine provides high-quality, in-depth content on topics that impact security efforts across the region — from counterterrorism to international cooperation and natural disasters.

FORUM provokes thoughtful discussions and encourages a healthy exchange of ideas. Submit articles, pictures, topics for discussion or other comments to us ONLINE or at:

Program Manager
Asia Pacific Defense FORUM
HQ USPACOM, Box 64013
Camp H.M. Smith, HI
96861-4013 USA

Asia Pacific Defense FORUM also offers extensive content online at
www.apdforum.com
Visitors can:

- **Access exclusive online content**
- **Browse back issues**
- **Participate in polls**
- **Send us feedback**
- **Request a subscription**
- **Learn how to submit articles**

FORUM

Exploring the issues that impact so many lives

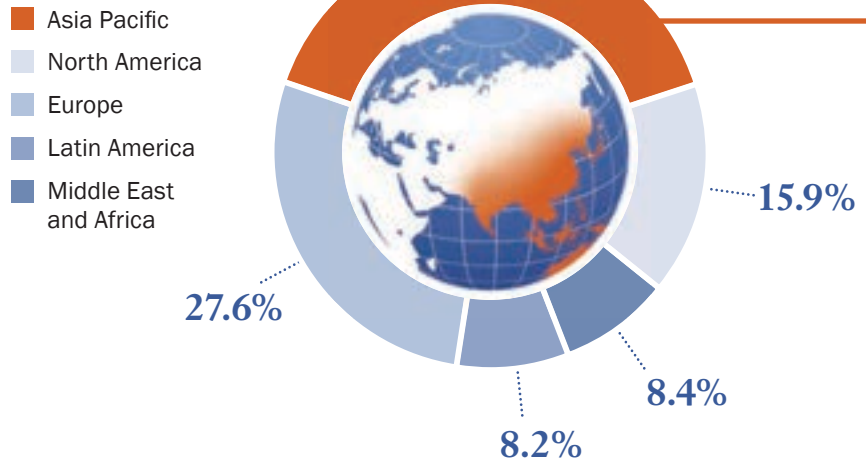Scan this image with your phone code reader to be taken to our website.

Global Breakdown

The evolution of cyber technologies has changed the way the world works. News travels faster. Money flows easier. Connections are instant. Across the Asia-Pacific region, millions of people have embraced these advances, with social networking sites exploding in popularity.

Percentage of Internet users, 2010
Source: comScore

- Asia Pacific
- North America
- Europe
- Latin America
- Middle East and Africa

39.8%

15.9%

27.6%

8.2%

8.4%

Cellphone Subscribers

Social media have flourished with the prevalence of cellphones, which many people use to access sites such as Twitter and Facebook.

Subscribers per 100 people in Asia-Pacific region
Source: International Communication Union

2005	2006	2007	2008	2009	2010
22.5	28.6	36.4	45.6	55.8	67.8

The Social Media Connection

KEY
- Social Networking*
- Photo Sharing
- Video Sharing
- Reading/Writing Blogs
- Internet Penetration

POPULAR NETWORK

- Facebook
- Twitter
- Renren
- Wretch
- Cyworld

The term "Social Networking" only includes use of social network sites such as Facebook, Wretch and Twitter. It does not include blogging, or use of photo and video sharing via other social media means.

East Asia

CHINA

0 20 40 60 80 100%

HONG KONG

0 20 40 60 80 100%

TAIWAN

0 20 40 60 80 100%

Northeast Asia

JAPAN

0 20 40 60 80 100%

SOUTH KOREA

0 20 40 60 80 100%
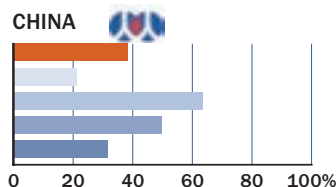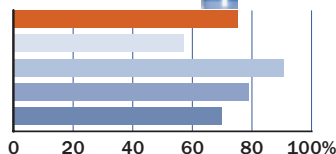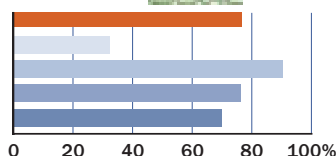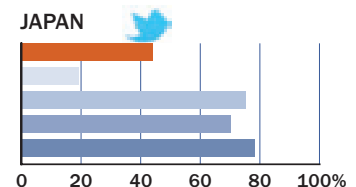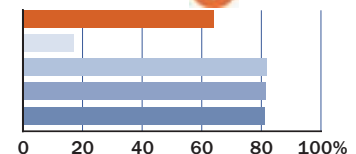
Number of Internet Users in the Asia Pacific

Low

350 THOUSAND

- 300
- 250
- 200
- 150
- 100
- 50

Timor-Leste, Marshall Islands, Micronesia, Bhutan, Maldives, Burma, Fiji, Cambodia, Macao, Brunei, Mongolia

Medium

20 MILLION

- 15
- 10
- 5

Laos, Nepal, Bangladesh, Sri Lanka, New Zealand, Singapore, Hong Kong, Taiwan, Malaysia, Australia, Thailand

High

5 HUNDRED MILLION

- 4
- 3
- 2
- 1

Vietnam, Philippines, South Korea, Indonesia, Japan, India, China
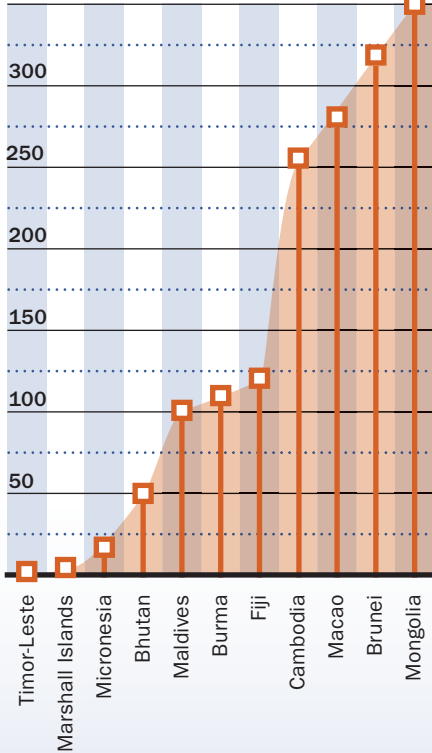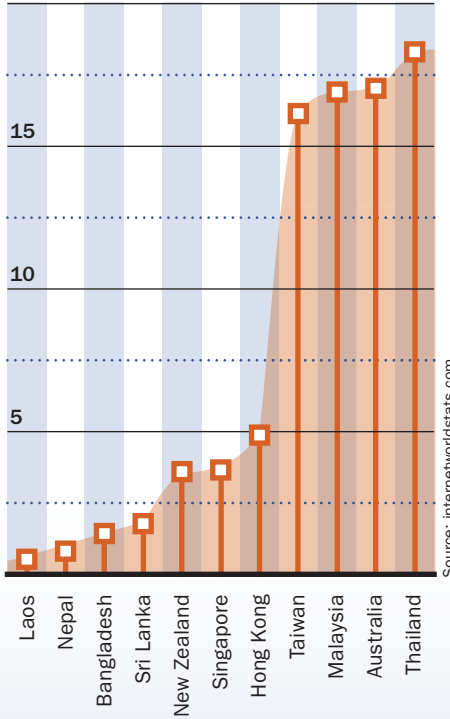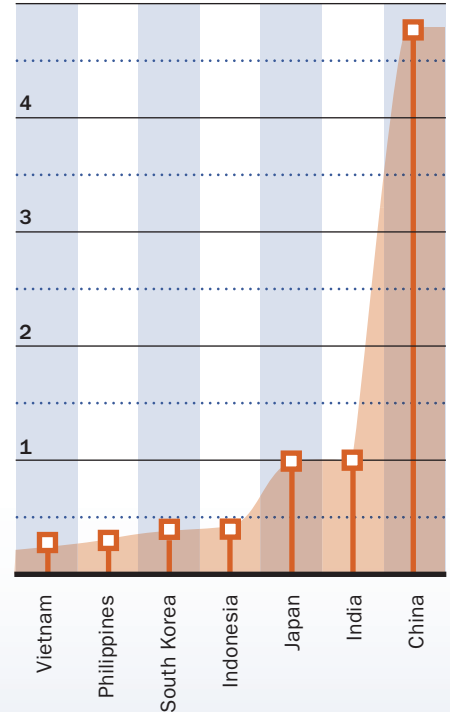
Source: internetworldstats.com

FORUM ILLUSTRATION

South/Southeast Asia

INDIA
0   20   40   60   80   100%

PHILIPPINES
0   20   40   60   80   100%

INDONESIA
0   20   40   60   80   100%
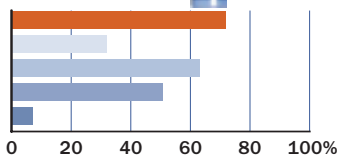
SINGAPORE
0   20   40   60   80   100%
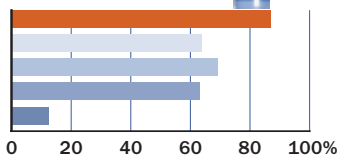
MALAYSIA
0   20   40   60   80   100%
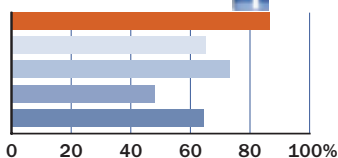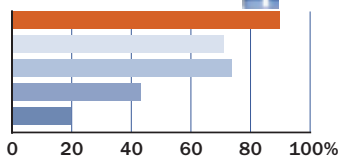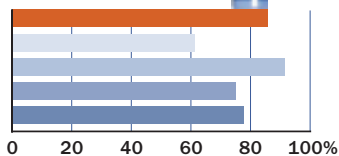
VIETNAM
0   20   40   60   80   100%
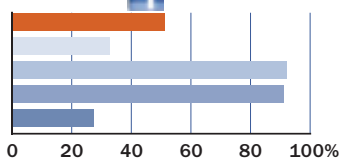
South Pacific

AUSTRALIA
0   20   40   60   80   100%
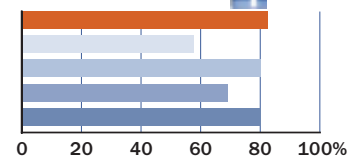
NEW ZEALAND
0   20   40   60   80   100%

Source: comScore

A massive campaign in Manila in 2001 calling for beleaguered Philippine President Joseph Estrada to resign started with a barrage of thousands of text messages demanding his impeachment.

the power of **social media**

The Role of YouTube, Facebook and Twitter in Governance

FORUM STAFF
PHOTOS BY AGENCE FRANCE-PRESSE

Incited by a text message, a mob of more than 1,000 people overran the home of a leader of a minority Islamic sect in Indonesia in west Java's Banten province in February 2011. After shoving police aside, the Islamic fanatics stoned, clubbed and macheted three members of the Ahmadiyah sect to death, one "as he knelt on the ground half naked. The bodies were then mutilated," Agence France-Presse reported.

A sect member caught the gruesome murders on video and posted the clip to the Internet. Public outcry in Indonesia, which has the second-most Facebook users and the third-largest market for Twitter in the world, expediently brought 12 suspects to stand trial in April 2011; two face the death penalty if convicted.

Although Indonesia has made "phenomenal gains" in building a democracy since the end of the Suharto era in 1998, Sidney Jones, senior advisor for International Crisis Group's Asian Program, told *FORUM*, "there would have been no action in the recent case where three Ahmadiyahese were killed, if it hadn't gone up on YouTube." Her group examines conflict and sources of violence worldwide.

In the past, such religious persecutions have largely gone unpunished in Indonesia, analysts and human rights groups contend, when perpetrated by the dominant Muslim community against minorities such as Christians and Ahmadiyah. Members of this particular Islamic sect are viewed as heretics and blasphemers by conservative Muslims, because they don't recognize Muhammad as the last prophet.

Cyber technologies, whose penetration is exploding in the Asia-Pacific region, are inherently neither good nor bad. Individuals and the public-at-large 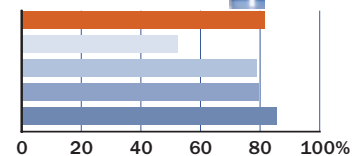are empowered to determine how such technologies are used, Clay Shirky, a new-media scholar and author based at New York University, explained in the January/February 2011 issue of *Foreign Affairs* magazine. "Internet freedom is a long game, to be conceived and supported not as a separate agenda but merely as an important input to the more fundamental political freedoms," he wrote.

Social networking's dark side

The danger is that criminals and extremists also use social media for recruiting, fundraising, training, organizing and launching attacks. Terrorist and extremist groups have developed and distributed training materials over the Internet such as The Anarchist Cookbook and the Mujahedeen Poisons Handbook. Videos posted to YouTube advertise the effectiveness of roadside bombs against coalition forces in Iraq, for example. Meanwhile, groups such as the Moro Islamic Liberation Front in the Philippines maintain Facebook pages.

As cyber extremist activities in the Asia Pacific continue to expand, countermeasures must also increase and become more sophisticated, experts say. A balance must be struck to suppress terrorism without constraining freedoms, according to Simon Bronitt, director at Griffith University's Center for Excellence in Policing and Security.

Governments are increasingly using the Internet not only to counter extremism but to help implement better policies and regulations and to keep citizens informed about issues ranging from improved health practices and disaster preparedness to crime prevention and job training programs.

Cyber advances also bring challenges for keeping the peace and maintaining democratic rule, as the Indonesian mob murders reveal. A cleric named Ujang Mohammed Arif masterminded the attack by sending a text message urging Muslim scholars, other clerics and Quranic school students to "besiege" the sect members in the village, according to prosecutors. Protections against such activities that incite violence are part of the obligations that societies and governments such as Indonesia must undertake to ensure freedom of speech, International Crisis Group's Jones told *FORUM*.

Cyber technologies, whose penetration is exploding in the Asia–Pacific region, are inherently neither good nor bad.

Authoritarian regimes can also use the Internet to further their agendas. To advance its business and propaganda goals, the Burmese government, for example,"aggressively regulates access to the Internet and digital media" by enacting shutdowns or limiting the bandwidth on which information can flow in and out of the country, according to a 2011 report by Freedom House, an independent watchdog group based in Washington, D.C.

Moreover, some attempts at cyber activism worldwide have failed, evoking heavy-handed government crackdowns, such as in the case of the 2009 Green Movement uprising in Iran. Protesters used social media avenues to contest the re-election of President Mahmoud Ahmadinejad and to communicate with foreign journalists. Ultimately, their voices were suppressed by violent military force.

The jury is still out on whether cyber tools can improve how a country is governed in the long-term and contribute to a lasting peace.

E–revolutions on the rise

The first time that social media helped force out a national leader occurred in the Philippines in January 2001. Thousands protested by sending text messages demanding that evidence be heard to impeach Philippine President Joseph Estrada. The barrage of texts sealed his downfall and constituted the world's first "e-Revolution."

Since then, many other movements in other parts of the world have adopted such strategies. Websites like Twitter, Facebook and YouTube have enabled protesters across North Africa and the Middle East to circumvent traditional gatekeepers, such as government-run media, and build alliances with other reformers.

The world media showcased the power of social networking websites in January 2011 in ousting Tunisian President Zine al-Abidine Ben Ali, an uprising that became known as the "Twitter Revolution." In Egypt, before President Hosni Mubarak's resignation in February 2011, hundreds of thousands of protesters populated Facebook pages extolling victims of Mubarak's secret police.

Later in 2011, computers and cellphones also contributed to protests in Bahrain, Yemen and Syria. Time will tell whether the cyber-sparked revolution will lead to the permanent installations of democracy in Egypt or Libya.

Social media can also improve citizen participation in government. Activists use cyber apps to disseminate campaign info, promote elections, free the press and political prisoners, counter corruption, and organize demonstrations in ways that can promote good governance.

Social media can spur governments to act. In 2008, South Koreans campaigned against beef imports by texting complaints and posting photos and videos online. In China, today's protesters similarly employ an instant-messaging service called QQ to fight corruption. "What we see is a rising role of citizen journalists" who are sometimes usurping the role of the official media, said Dr. Dona Stewart, professor at the U.S. Near East South

Members of the Ahmadiyah Islamic sect participate in the burial ceremony for two members killed by a mob incited by a text message in Indonesia's Banten province in February 2011.

Asia Center for Strategic Studies.

In turn, governments at all levels are increasingly turning to social media to improve services and get their messages out. For example, these technologies have proven invaluable in disaster relief in countries from Haiti to New Zealand. The devastating earthquake and tsunami that struck Japan in March 2011 pushed local governments and agencies there to venture onto social media to get critical information to citizens in real-time. Many municipalities such as Mitaka city in western Tokyo launched Twitter accounts after the disaster.

Some heads of state are even spreading the word. In July 2011, Indonesian President Susilo Bambang Yudhoyono encouraged the Association of Southeast Asian Nations (ASEAN) to "maximize the use of Twitter, Facebook and other social media to engage" citizens in the Southeast Asian region. ASEAN is key to facilitating stability in the Asia Pacific.

Other experts and leaders, however, caution that more regulation is needed to keep detrimental applications of social media at bay. French President Nicolas Sarkozy warned technology leaders in May 2011 that the Internet must not be "a parallel universe outside laws and morals." He purported that governments have a role in setting boundaries to limit the abuses of the Internet. "Total transparency has to be balanced by individual liberty. Do not forget that every anonymous Internet user comes from a society and has a life," he said. "Governments are the legitimate guardians of our societies and do not forget this."

Internet technologies in themselves are not a cure-all for poor governance or repression either. "The arrival of social media doesn't suddenly remove all previous forms of coordination. It's an addition to the landscape, not a replacement for it," New York University's Shirky wrote in *Foreign Affairs* magazine. "What social media does is it allows groups of people to know what other people are thinking in the country at a much wider scale, at much lower cost."

Cyber suppression

Whether cyber-incited uprisings lead to long-term stability and good governance remains to be seen. "Triumphalism about recent events in the Middle East is premature," contends Belarusian-born media expert Evgeny Morozov. "The contest is still in its early stages, and the new age of Internet-driven democratization will endure only if we learn to counter the sophisticated measures now being developed to quash it," he told *The Wall Street Journal* in February 2011.

Protesters call for the ouster of President Estrada during a protest in Manila. Estrada became the first leader impeached by Congress in the Philippines, thanks to a text messaging campaign.

Indonesian President Susilo Bambang Yudhoyono, left, has successfully implemented one of the world's leading counterterrorist programs dur–ing his tenure. Leadership, not social media in and of itself, is key to good governance.

Indonesian Islamic leaders — conservative and liberal — are turning to the Internet in the contest to win faithful followers in the world's largest Muslim-majority country. Ahmad Mustofa Birsi, an influential Muslim cleric and a prominent member of Indonesia's largest Islamic organization, the moderate Nahdlatul Ulama, checks for Twitter messages on his iPad in Jakarta.

Media analysts like Morozov fear authoritarian regimes will take the lessons from Tunisia and the Philippines and upgrade their repressive machinery to prevent similar online uprisings. When protesters "socialize" or "assemble" at a few popular websites such as Facebook or YouTube, authoritarian regimes can more easily monitor their activities and readily jam, manipulate or disrupt those sites.

When a Buddhist-led protest broke out in Burma in 2007, the country's leaders not only severed Internet service but hired roving thugs to beat up people carrying cellphones near the scene of the demonstrations. In its failed effort to contain the uprising in early 2011, Egyptian authorities pressured the country's five Internet service providers (ISPs) to shut down voluntarily, causing a huge traffic drop-off in a single day. To overcome the government's attempted security crackdown, Egyptian-based Google offered Egyptians a "speak to tweet" platform that converted voicemail to Twitter text.

In the spring of 2011, Libya's Moammar Gadhafi government, facing civil war, throttled down the nation's only ISP, effectively blocking usage for the rebellious masses but preserving online capacity for loyalist-government officials. Iran has the reputation of having the most intensive apparatus to squash social media. "They have learned their lesson from the 2009 uprising and have developed the most comprehensive Internet control strategy in the Middle East, setting up dedicated units of 'cyber-police' and experimenting with advanced Internet surveillance techniques that may even allow them to detect dissidents who are using anti-censorship tools," Morozov said.

Experts insist social media are only as good as the people who use them. That was the message of the December 2010 report "Political Change in the Digital Age" published by the School for Advanced International Studies in the U.S. In Tunisia, Internet activism led to a burst of freedom. In places such as Burma, repression gained the upper hand. "Conditions that contribute to success are likely determined not by the given technological tool," the report concluded, "but by human skill and facility in using the networks that are being mobilized."

Middle Eastern countries such as Egypt might take a cue from Indonesia, where political Islam was also suppressed for more than three decades of Suharto's reign. "The Indonesian lesson for Egypt is that when people are free from oppressive regimes, they do not embrace extremism, they reject it," according to Ann Marie Murphy, associate professor at the John C. Whitehead School of Diplomacy and International Relations at Seton Hall University.

The success of Indonesia's democracy to tame its radicals depended on its leadership, not the role of social media. In Indonesia, the new president, Susilo Bambang Yudhoyono, among other measures, installed an independent nonpartisan election commission, freed the press, released political prisoners and implemented one of the world's leading counterterrorism programs. "The willingness of Suharto's successor to take such steps in the transition was critical for Indonesian democracy. The pivotal role that social media is playing during the [Egyptian] protests shows the futility of attempting to clamp down on free speech," Murphy wrote in a CNN editorial. □

This story contains reporting from the *per Concordiam* magazine staff.

HIGH-SPEED
COUNTER
TRAFFICKING

Law enforcement harnesses
cyber technologies to beat human
traffickers at their own game

FORUM STAFF

Filipino children hold candles during a
prayer for justice and protection as part
of the annual observance of International
Day Against Human Trafficking in Manila.
The region's children are at risk of
becoming victims of online pornography and
prostitution, law enforcement officials warn.
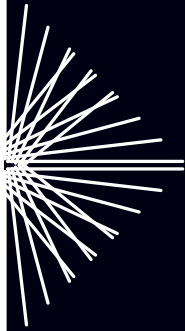
Trafficking survivors gather at the Maiti Nepal rehabilitation center in Kathmandu in April 2011.

Men in the mood for "exotic excursions" and "pleasure tours" found what they were looking for on the Wicked Adventures Travel website. There, they could arrange safe, confidential vacation packages to Thailand and the Philippines, complete with transportation, hotel and meals. What made the site's adventures so "wicked," though, was one special accommodation: children who would travel with the men for sex.

For one boat captain from the U.S. state of Florida, the site didn't offer enough. His wanderlust was focused closer to home — in Central America. Gary Evans emailed the operators of Wicked Adventures and suggested they partner with him to provide child sex tours to Honduras and Costa Rica. Through emails, instant messages and cellphone conversations, he arranged for a sampling of Honduran girls between the ages of 12 and 16. The website operators sent him U.S. $1,000 for the trip electronically via PayPal.

However, what has become a common method of arranging for sex tours, in this case, was a bust, according to an outline of the case by The Smoking Gun, a website that reports on U.S. public documents such as court records. The FBI had orchestrated the fake travel website to catch people such as Evans who use the Internet to arrange for children's exploitation.

The opportunities for human trafficking, slavery and exploitation have increased exponentially with cyber technologies. People can be bought and sold online, and criminals can share tips on how to find and take advantage of victims. However, law enforcement also has more tools to combat crime in this information age, experts say. "Rather than repressing technology, it becomes necessary to harness its potential to interfere with organized criminal activities and to combat trafficking and assist its victims," the U.N. Global Initiative to Fight Human Trafficking (UN.GIFT) reported in 2008.

LURING VICTIMS

In the underground market of sex tourism, websites like the one the FBI set up are all too real. With ease and a certain level of anonymity, travelers can arrange and pay online for sex. In addition, the reach of the Internet and related technologies has opened up greater numbers of remote areas of the world to tourists, making more naïve young people vulnerable to trafficking and exploitation, experts say.

Within developing countries, ill-intentioned tourists use technology to lure children. "Street children who have no other means of establishing contact with foreign tourists are being approached and given a mobile phone to maintain contact with the traveler," ECPAT International reported in 2010. The organization, which fights child trafficking and exploitation, also noted that offenders approach children at cyber cafés

INTERNATIONAL CHALLENGES

Because the Internet has no borders, it is an ideal conduit for transnational crimes such as human trafficking. That's why experts say international standards are needed to combat cyber crime. When law enforcement in one country identifies a website that promotes human trafficking — for example, a travel booking site that arranges for sex with children — shutting it down might not be easy. Law enforcement must work with their counterparts in the country where the site is hosted, and if the laws there are lacking, the task can be complicated.

Several international bodies have developed guidelines on responding to cyber crime. Asia-Pacific Economic Cooperation officials issued a cyber security strategy in 2002, declaring that countries must have:

· Substantive laws that criminalize attacks on networks
· Procedural laws to ensure that law enforcement officials have the necessary authorities to investigate and prosecute offenses facilitated by technology
· Laws and policies that allow for international cooperation with other parties in the struggle against computer-related crime

REUTERS

Alex Khu talks about worldwide Internet usage at the U.S. Immigration and Customs Enforcement's Cyber Crimes Center in Virginia. The agency is best known for fighting drug and human traffickers at U.S. borders, but it also works in the virtual world, combating a surge in child pornography, sex tourism and online child trafficking.

CASE STUDY:
NEPALESE POLICE GO HIGH-TECH

FORUM STAFF

For years, police in Nepal painstakingly kept track of human trafficking cases in paper logbooks housed at police headquarters. Searching through the cases quickly was difficult, if not impossible, especially when cases involved crimes in other districts.

The Nepalese police have made big improvements by developing a monitoring and tracking software system for trafficking cases. The computer system, officially launched in May 2010 and developed in conjunction with The Asia Foundation and the U.S. Department of State's Office to Monitor and Combat Trafficking in Persons, allows police to quickly search the details of trafficking cases nationwide and coordinate with district offices. They can also check suspects' criminal records.

Technological advances are crucial for law enforcement to keep pace with traffickers, and recognizing that need is the first step. "In Nepal, Internet-based anti-trafficking efforts need the full support and buy-in from the organization for which they are developed," explained Diana Fernandez of The Asia Foundation, a nonprofit, nongovernmental organization. "In the case of the Nepal police, they were fully supportive of the computer monitoring and tracking system for trafficking in persons cases and played a large part in software development. The IT [information technology]

department at police headquarters is very well trained in utilizing technology."

The software is expected to be rolled out to five more districts in the next five years. To make the most of it, law enforcement will have to remain committed. "Many district-level police officers are unfamiliar with IT and need special training and attention to properly utilize the software," Fernandez told *FORUM*. "The police will need to provide IT equipment and software training to each district office."

THE BIGGER PICTURE

The computer system is part of a larger project funded by the U.S. Department of Justice that will connect Nepalese police's digital records to international bodies such as Interpol, which will help law enforcement combat international trafficking.

On a regional scale, the system could help Nepalese and Indian law enforcement join efforts to fight trafficking. "IT can greatly assist cross-border cooperation if agencies are willing to share information with each other. This is especially important in Nepal as it shares an open border with India, a fact exploited by traffickers," Fernandez told *FORUM*. "With Web-based technology linked to Indian police databases, Nepal police would be able to track cross-border operations of traffickers and would allow for increased cooperation in information and evidence gathering."

Hana Hsin-wei Cheng and Christian P. Guth of The Asia Foundation contributed information to this report.

Traffickers have also found the Internet to be an important tool in luring victims from afar. Criminals use websites for marriage agencies and dating services to trick women into trafficking, experts say. Online job ads for waitresses, models, nannies and maids — as well as postings for agriculture and construction work — also dupe victims, according to UN.GIFT.

"Previously, press advertisements (employment, marriage, dating, etc.) were a well-known way of recruiting victims. Nowadays, with the expansion of the new technologies, these advertisements have also moved to the Internet," according to "Trafficking in Human Beings: Internet Recruitment," a report from the Council of Europe.

One joint investigation by Polish and Italian law enforcement uncovered a transnational criminal group that was using an online employment agency to recruit victims from Poland to work in Italy, according to the Council of Europe report. The criminal organization even collected fees from victims for placing them in "jobs." Once the victims arrived in Italy, they found themselves in debt bondage, living in work camps that were watched by armed guards to prevent escape. In the end, investigators arrested 27 people, and more than 100 trafficking victims were rescued.

SHARING THE EXPLOITS

Beyond the disturbing scenes that unfold in labor camps and dark brothels around the world, experts note that exploitation of trafficking victims has exploded in the form of pornography. In addition to the money made from selling actual sex, criminals have found profit in posting photos and videos in the virtual world.

In one case outlined in a report by UN.GIFT, criminals trafficked women from Japan to Hawaii, where they were forced to perform sex shows that were broadcast on the Internet for audiences back in Japan. The trafficking ring chose to illegally smuggle the women into Hawaii and broadcast the shows

Teenage girls rescued from a cyber sex den meet with a psychologist during a session at Preda Foundation in Olongapo City, Philippines.

through servers in California to get around Japan's strict laws against pornography. "This case study showcases how technology can be used to circumvent both borders and national laws," the agency reported.

Easy access to inexpensive technology has simplified production of pornography such as this. "Digital cameras and recorders enable the making of images that do not need to be professionally processed, thereby eliminating the risk of detection," Mohamed Chawki and Mohamed Wahab wrote for the Computer Crime Research Center. In areas where the Internet is not readily available, images and videos can be carried across borders in small, easily overlooked USB devices, experts say.

FIGHTING BACK

Even as criminals explore new ways to traffic, enslave and exploit victims, law enforcement officials are expanding their cyber tool kits as well. Each new arrest exposes traffickers' methods, and sharing information helps crime fighters everywhere stay on top of the trends.

International trafficking databases, in particular, have improved the information flow, experts say. Interpol's I-24/7 system allows law enforcement officials in its 188 member countries to share information on any number of crimes, including trafficking, instantly online. "As criminals and criminal organizations are typically involved in multiple activities, I-24/7 can fundamentally change the way law enforcement authorities around the world work together," Interpol explains on its website. "Pieces of seemingly unrelated information can help create a picture and solve a transnational criminal investigation."

Participation and cooperation are key, though, as the agency encourages member countries to expand the

database to include information from border police and immigration officials.

Nonprofit agencies are finding ways to share information through technology as well. The U.S.-based organization Not For Sale (NFS) has created an application called Slavery Map (slaverymap.org) that inputs reports of trafficking cases around the globe. The map — which is available to law enforcement and anti-trafficking organizations around the world — includes details on reported incidents and their outcomes. To gather as much data as possible, NFS conducts international training sessions to show workers from rescue groups and law enforcement how to contribute to the map. In the future, the organization hopes to expand the project to become an information clearinghouse for all parties involved in fighting human trafficking and helping victims, NFS board member Steve Goode told *FORUM*.

In addition to arming law enforcement and nongovernmental advocacy groups with information and technology, potential victims must be warned of the dangers. Those desperate for jobs overseas and children caught up in socializing online need to know traffickers' cyber tricks, experts say. In an effort to prevent crimes, the Child Exploitation and Online Protection Center reaches out to children on social networks such as Facebook, Twitter and YouTube to teach them safety measures.

Overall, combating trafficking will require a multifaceted approach — with law enforcement, nongovernmental groups and individuals making the most of the technology at their disposal. As Goode told *FORUM*, "This is a global movement," and stopping the flow of victims requires a coordinated international effort. □

FORUM ILLUSTRATION

Soldiers need to be trained on the responsible use of social
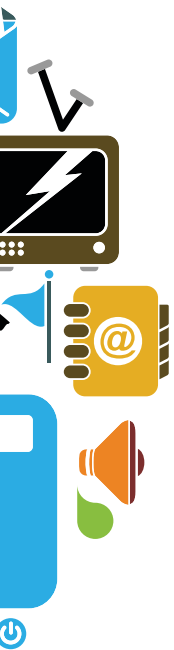
DANGER

IN THE Details

MILITARIES SEE POTENTIAL IN SOCIAL MEDIA, BUT EDUCATION IS KEY TO RESPONSIBLE USAGE

FORUM STAFF

The Soldier's mother beams with pride, ecstatic to receive a private Facebook message from her son about his tour of duty. Her smile grows more affectionate as she reads that he has posted new pictures online, appears to be doing well and is on his "best behavior," due to "VIP stuff" happening at his military base. It's the kind of good news any relative would be happy to receive — and eager to share.

The mother wastes no time toggling from the private message to update her public Facebook status with potentially sensitive details, including the location of her son's duty station. It's as if she has invited a terrorist into her home for tea and to look through her family's photo album. At least, that's the parallel drawn by the United Kingdom Ministry of Defense, which depicts this scenario in a public service announcement video released in June 2011. The ministry's mission: Warn military personnel and their families that "careless talk" on social networking websites can jeopardize a soldier's safety and cost lives.

media to avoid inadvertent disclosure of sensitive information.

AGENCE FRANCE-PRESSE

AGENCE FRANCE-PRESSE

Girls interact on Facebook at an Internet shop in Jakarta. Experts say that relatives of servicemen and women should be careful of what they post on social websites.

Cambodian bloggers, or "cloggers" as they call themselves, meet at a Phnom Penh coffee shop. Experts say social media is here to stay, so governments and businesses should learn to use it to their advantage.

Soldiers need to be trained on the responsible use of social media to avoid inadvertent disclosure of sensitive information.

The United States Army, for example, has a Social Media Handbook that guides Soldiers, personnel and families on best practices for using social media sites. Such precautions translate to any military in any country.

"There have been cases recently when people have given away details of when a ship is due home or when a plane is about to land," a U.K. Ministry of Defense spokesman told *The Guardian* newspaper in June 2011. "These things happen in the excitement of homecomings and are unintentional. But we don't want to give the enemy the edge. We're just asking servicemen and women, and their families, to be a little more circumspect when they use these sites."

The benefits of social networking — and the reality that militaries can no longer ignore the capability — dwarf the risks. As studies show the rapid and increasing rise

> ## The benefits of social networking — and the reality that militaries can no longer ignore the capability — dwarf the risks.

in popularity and use of social networking sites, militaries around the world have adjusted their response to embrace the trend and use them as a tool. Conferences that deal specifically with the military's use of social media have also emerged, such as one organized in London by the SMi Group in October 2011.

"With huge cuts to military budgets, social media has been welcomed, as it is a great cost saving tool," SMi reported in an overview of the conference, "Social Media within the Military and Defense Sector," adding that many armed forces have turned to social media to drive recruitment efforts.

Some militaries, in fact, are trailblazers in that respect. Take Singapore, for example, where the Singapore Armed Forces and Ministry of Defense (MINDEF) use social networking sites to reach out to youth. "New media platforms allow MINDEF to engage the public directly through our cyberpioneer connections on YouTube, Facebook, Flickr and Twitter," Singapore's Deputy Prime

Tips on Social Media and Security
Source: U.S. Army Social Media Handbook

Place privacy setting options on Facebook to "friends only."

Educate family and friends on what you can and cannot discuss on social media sites.

Minister Teo Chee Hean told *MIS Asia* magazine in 2010.

Within a year, Singapore's Defense Ministry saw the number of unique visitors to its YouTube channel increase from about 200,000 to 2 million, *MIS Asia* reported.

"Within six months of setting up our Facebook page, we have attracted more than 4,000 fans," Teo told the magazine. "Singaporean youths, in particular, have been very receptive to our new approaches and media platforms."

In China, however, the People's Liberation Army (PLA) has gone against the trend and banned its soldiers from using social media. The PLA announced the ban in 2010 and prohibits its soldiers from launching websites or writing blogs, Agence France-Presse reported.

Social media usage across the Asia-Pacific region has experienced unprecedented growth, according to online researcher The Nielsen Co. Nearly 75 percent of the world's Internet users have visited a social networking site and report spending an average of six hours per month on one, Nielsen reported in June 2010.

YOUTUBE

Within a year, Singapore's Defense Ministry saw the number of unique visitors to its YouTube channel increase from about 200,000 to 2 million.

"The findings we've uncovered in this social media report highlight, beyond a shadow of a doubt, that social media is here to stay and needs to be taken seriously by the broader business community," said Megan Clarken, managing director of Nielsen's online business in the Asia Pacific. "With three-quarters of the global Internet population now participating in some form of social media, businesses can no longer afford to simply observe the social media phenomenon. They need to embrace it."

Swedish military officials have done just that.

"The studies in this specific area show a clear trend: And that is that among the Internet media, the use of social media is showing the biggest increase," Sweden's Armed Forces Command Lt. Cmdr. Erik Largersten told the website DefenseNews.com in February 2011, adding, "Social media is also a valuable source of information."

Sweden's Armed Forces Command issued a directive to civilian and military personnel urging the use of social media to include Facebook, Flickr, Twitter, Wikipedia and YouTube. Guidelines dictate that personnel must abide by confidentiality rules and steer clear of sensitive information. The Swedish military anticipates the open engagement of social networking sites will "empower personnel to help develop a better understanding of the military and how it works," according to DefenseNews.com. ☐

Social Media Facts in the Asia Pacific

- Japanese bloggers post more than 1 million entries per month, more than any other country.

- By population, Korea is one of the most social media–engaged countries in the world, with the country's leading social media site, Naver, attracting 95 percent of the Korean Internet population each month.

- Close to one-third of India's social media users visit a blogging site such as Twitter at least once a day.

- Asia produced more messages on Twitter than any other continent in the world in July 2010, with a majority of tweets originating in Japan, Indonesia and South Korea.

Sources: The Nielsen Co. Report June 2010, Semiocast

Turn off the GPS functions on your smartphone to avoid geotagging.

Review all photos and videos for sensitive information before you post.

Do not post your schedule, which includes event times and locations.

Ask yourself, "What could the wrong person do with this information?" and, "Could it compromise the safety of myself, my family or my unit?"

NET SECURITY

SECURITY
WARNING

NATIONS LOOK TO MAXIMIZE SAFETY AND MINIMIZE RISK WITH BEST PRACTICES

FORUM STAFF
PHOTOS BY AGENCE FRANCE-PRESSE

*T*he key to hacking your data or disrupting your computer system could come down to something as simple as the way you sign an email. That's reportedly one way Chinese hackers targeted U.S. military personnel, by "phishing" for terms commonly used in email closings such as "very respectfully," "virtual regards" or simply "V/R," Reuters reported in April 2011.

Such tactics and attacks keep governments busy trying to secure their networks and staying one step ahead of the bad guys.

The U.S. Department of Defense announced a Strategy for Operating in Cyberspace in July 2011, outlining a plan to treat the virtual world as an operational domain. The department says it plans to work with interagency and international partners to "mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy and civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S.

prosperity and security."

A month earlier in June, India announced a task force to review its national security measures, taking more into account how the country might fare in the realm of cyber security.

"The security challenges have changed. India has moved on, our security challenges have evolved," *The Times of India* newspaper quoted an official saying in June 2011. "It is time to look at the national security situation in light of challenges ranging from cyber security to energy security."

Members of the security review task force include a former Indian Navy chief and a former Indian Air Force chief along with intelligence and nuclear

A.K. Kahn, right, police commissioner of the Indian state of Andhra Pradesh, talks with arrested computer hacker Gorantla Lathadhara Rao at a June 2010 news conference. Rao allegedly hacked a government passport application site.

FORUM ILLUSTRATION

SOUTH KOREA EXPANDS
MILITARY CYBER UNIT

AGENCE FRANCE-PRESSE

South Korea's defense ministry announced in July 2011 that it would expand its cyber warfare unit to help combat growing Internet attacks from North Korea.

The ministry said its cyber command, launched in January 2010, would increase the number of personnel from 400 to 500, after an earlier announcement that it would open a cyber warfare school next year. North Korea reportedly maintains elite hacker units.

Seoul accused Pyongyang of staging cyber attacks on websites of major South Korean government agencies and financial institutions in 2009 and 2011. Pyongyang rejected those allegations, accusing Seoul of inventing the charges to raise tensions.

In May 2011, South Korea said a North Korean cyber attack paralyzed operations at one of its largest banks. Cyber attacks on South Korean and U.S. military websites in March 2011 may have been a test by North Korea or sympathizers, according to a report by computer security firm McAfee.

"We believe this incident ... has very clear anti-Korean and anti-U.S. political motivations," McAfee said in a report titled "Ten Days of Rain."

"The combination of technical sophistication juxtaposed with relatively limited execution and myopic outcome is analogous to bringing a Lamborghini to a go-cart race," McAfee said in its findings.

"As such, the motivations appear to outweigh the attack, making this truly seem like an exercise to test and observe response capabilities," it said.

McAfee security researchers said it was 95 percent likely that the culprits behind the online assault in March 2011 were also behind the July 4, 2009, cyber attacks on U.S. and South Korean websites. Banking, military and government websites in South Korea and sites for U.S. forces in that country were hit with distributed denial of service attacks, which overwhelm websites with requests, causing them to slow down or be inaccessible.

South Korean prosecutor Kim Young-Dae details North Korean cyber attacks on the National Agricultural Cooperative Federation in May 2011.

experts. The group was given six months to prepare a report.

In the meantime, India and the United States signed an agreement in July 2011 to cooperate on cyber security. The pact establishes best practices for exchanging critical cyber security information and expertise between the two governments through the nations' computer emergency response teams and information technology departments. Any government or military that doesn't use a secure Internet connection to transmit sensitive information should find ways to improve their network.

NEED FOR SECURE NETWORKS

India's cyber review gets under way as its lack of a secure network for government business comes under public scrutiny after Prime Minister Manmohan Singh's office issued an official statement condemning a Mumbai bombing via a Hotmail.com email address.

It's a common practice for the prime minister's staff to use a free email account, such as Hotmail or Google, for official business, according to a July 2011 Bloomberg.com report.
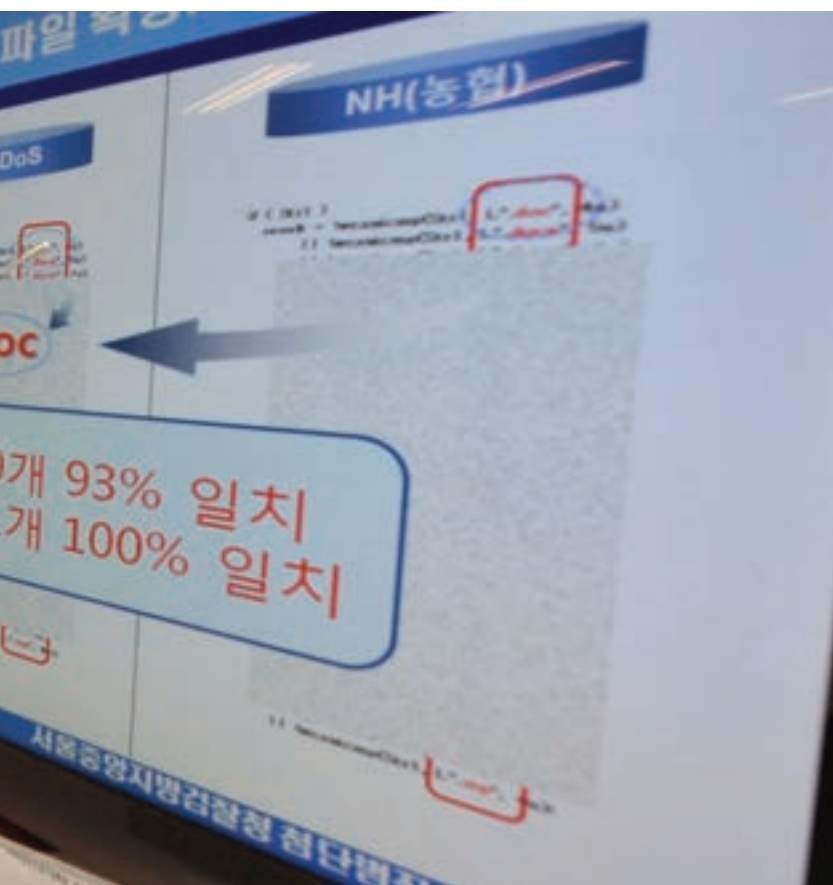
> ## 66
> *IT'S REALLY QUITE AMAZING THAT, AS A NATION, WE HAVEN'T YET WOKEN UP TO THE IDEA THAT SENSITIVE GOVERNMENT INFORMATION SHOULD BE SHARED THROUGH SECURE CHANNELS, NOT HOTMAIL OR YAHOO."*
>
> — PAWAN DUGGAL

Government officials prefer the third-party domains because they have better safety controls in place, according to Bloomberg.

"It's a recipe for disaster," Pawan Duggal, a New Delhi lawyer specializing in information technology cases, told Bloomberg. "It's really quite amazing that, as a nation, we haven't yet woken up to the idea that sensitive government information should be shared through secure channels, not Hotmail or Yahoo."

The business of global cyber crime has an estimated value of U.S. $1 trillion, "and Asia sits at the crossroads of this industry," say experts with Cyber Security for Government Asia. A conference by the same name will take place in Malaysia in February 2012, where members from the public and private sector are expected to converge and discuss cyber security laws that benefit the region.

"Cyber security is a very important component of today's national security, public safety and privacy.

With the advancement of technology, Internet usage has increased tremendously, and at the same time, we are all exposed to threats in the cyberworld," CyberSecurity Malaysia Chief Executive Officer retired Lt. Col. Datuk Husin Jazri said in a June 2011 release.

PROTECTING INDIVIDUALS

While governments work to improve their broader cyber security systems, individuals can protect themselves by practicing safer Internet surfing. Google.com offers a series of workshops intended to relay the most basic of user tips in a section called the Digital Literacy Tour, which can be accessed at www.google.com/educators/digitalliteracy.html.

The Google guide has "classroom" activities designed for students and guides designed for teachers that cover detecting lies online, playing and staying safe online, and steering clear of cyber tricks. □

HEALTHY PROGRESSION

TECHNOLOGY HAS CHANGED MEDICAL CARE DELIVERY
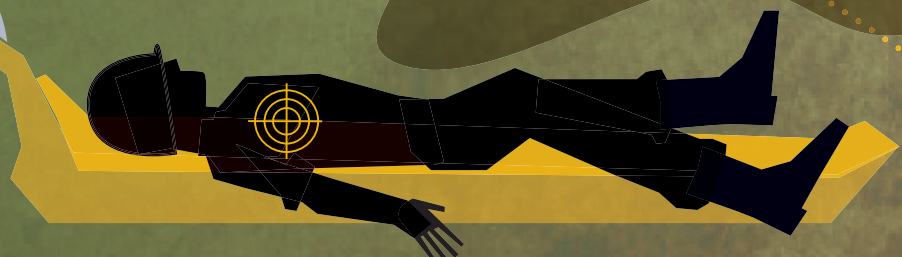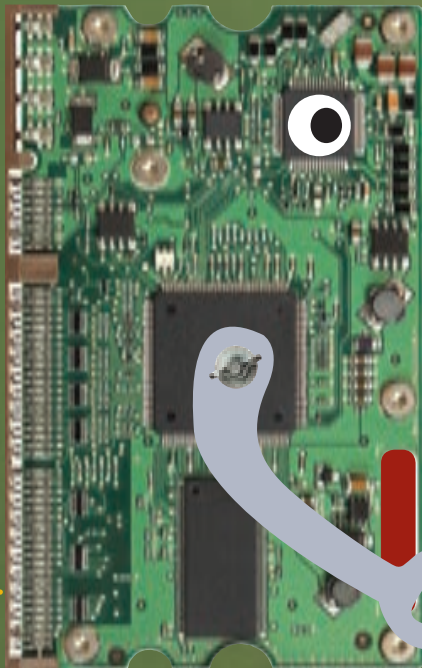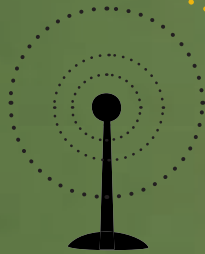
FORUM STAFF

D isguised in camouflage and face paint, a soldier and his team quietly creep through a wooded area. When they reach a clearing, the lead soldier slowly, cautiously steps into the open. A shot rings out. The soldier falls to the ground, his leg bleeding profusely. The threat posed by an unseen sniper makes reaching him too dangerous for his comrades.

Years ago, this scenario may have meant the end for a soldier. But in this case, technology is a lifesaver. Sensors in the soldier's uniform send his vital signs to a nearby medic, who uses a wireless device to request robotic assistance in extracting the wounded man. A tank-like medical vehicle responds to the request. Out of it rolls a remote-controlled robot that carries a ballistic blanket to protect the soldier. The medic also sends out a smaller robot dragging a sled. When the two robots reach the wounded man, the soldier rolls onto the sled, and the protective blanket is placed on top of him. The soldier is quickly pulled to a covered area, where the medic and fellow comrades load him into the mobile medical unit.

Guided by GPS technology and navigation systems, the autonomous mobile unit evacuates the soldier to a medical facility. En route, the vehicle provides life support and sends the soldier's vital signs to doctors awaiting his arrival. The vehicle is also equipped with a telemedicine video device, which allows the soldier to talk to a doctor while being transported.

Technology such as this, demonstrated in a video for the U.S. Telemedicine & Advanced Technology Research Center, is revolutionizing health care. From war-ravaged battlefields to peaceful farmlands, advances in medical technology connect those who need care with those who can provide it. Videoconferencing, satellite connections and mobile phone technologies are bridging the distance between specialists in big-city hospitals and medical technicians in remote locations. Patients' X-rays and sonograms can be sent from one doctor to another instantly. Health care professionals no longer have to travel to large medical centers or universities to receive specialized training.

FORUM ILLUSTRATION

HELP FOR HEALTH CARE WORKERS

Both military and civilian health care workers have benefited from these advances. Access to technology can help health care workers stay connected, particularly in countries where populations are spread out and medical workers are spread thin, experts say.

In India, the Apollo Telemedicine Networking Foundation has blazed trails in the field of telemedicine and eHealth, establishing more than 150 telemedicine centers worldwide. In the past 12 years, the organization has done 750,000 long-distance consultations using telecommunications technologies. Although teleconsultations have added to the physicians' workload, "that's a challenge which all of us enjoy," Professor K. Ganapathy, president of the foundation and the Telemedicine Society of India, told *FORUM*.

In addition to connecting India's big cities to rural areas, eHealth relationships have been forged with other countries, as well. Through a partnership with the South Asian Association for Regional Cooperation (SAARC), India provides free teleconsultations, including software and equipment, and training for health care workers in SAARC member countries. India also funds the Pan-African e-Network Project, which connects medical experts in India with their counterparts in Africa to provide teleconsultations and training.

Videoconferencing allows doctors to share patient information in real time and collaborate on a course of treatment.

This blood pressure monitor, unveiled at the 2011 International Consumer Electronics Show, allows patients to monitor their conditions at home and upload information to a website that their doctors can access.
REUTERS

PATIENT PARTICIPATION

Although health care professionals benefit from the training and guidance that come with these advances in technology, patients stand to gain the most. Active participation on their part is key.

"We are not going to train doctors to become specialists, or specialists to become super specialists," Ganapathy told *FORUM*. "We are going to make a patient take part in the decision-making process. … Why can't a patient take his own blood pressure? Why can't he take his own blood sugar?"

Many eHealth programs rely on the patient to do just that. Remote-monitoring technology allows patients to report vital signs to track their conditions without in-person visits. In China, for example, researchers are working on the Chinese Aged Diabetic Assistant (CADA), which will allow patients to track their exercise, diet and mood and send that information to physicians. Down the line, researchers hope CADA will also be used to remind patients about doctor's appointments and relay healthy living tips.

"Mobile technologies can empower elderly people to better understand diabetes, track their health indicators more closely and follow a healthier lifestyle," said Maggie Jiao Ma, one of the researchers on the project, a partnership of Microsoft, Peking University First Hospital and two U.S. universities. "Once patients are able to self-manage their diabetes, physicians and nurses can free up more time for providing advanced care."

For wounded soldiers, technological advances in prosthetics and sheer determination have made it possible for many to return to the battlefield. The United States, for example, has about 40 amputees serving in combat zones. "We realize the importance of all our Soldiers and what they can contribute to our Army," a Pentagon spokesman told *The Daily Mirror* newspaper. "Someone who loses a limb is still a very valuable asset."

BY THE NUMBERS

Access to technology has become more prevalent than access to hospitals. The World Health Organization reports that in developing countries there are:

5.3	2.3	305	11
BILLION PEOPLE	BILLION MOBILE PHONES	MILLION COMPUTERS	MILLION HOSPITAL BEDS

NATIONAL SUPPORT NEEDED

To reap the benefits of these advances in medical technologies, experts warn that governments must play an active role in building basic infrastructure, providing equipment and developing policies that promote the use of technologies.

These types of commitments can save lives in the long run. In the wake of the SARS (severe acute respiratory syndrome) outbreak in 2003, the government of Cambodia partnered with the World Health Organization to introduce Cam e-WARN, a system of monitoring 12 major infectious diseases in the country. Surveillance officers throughout the country collected data from health care workers on their mobile phones and sent the information to workers at provincial offices, who entered it into a database to track trends. The data was also sent via text message to the national office, where an alert was automatically triggered if disease cases reached concerning numbers. Once the data behind the alert was verified, a rapid response team sprang into action.

"The implementation of Cam e-Warn for the rapid detection of early stage disease outbreaks has improved the [Health] Ministry's ability to control the spread of diseases and protect the health of Cambodia's 14 million inhabitants," the World Health Organization reported in 2011.

For eHealth programs such as this to be successful, cooperation is key. Experts say nations should coordinate efforts to ensure programs are able to spread beyond borders.

"Partnerships usually facilitate change, and the telemedicine sector is no different," according to the World Health Organization's "Telemedicine:

CHALLENGES AHEAD

Although information communications technology has helped connect health care workers worldwide, challenges remain. Legal hurdles, knowledge and expertise were among the barriers cited in the World Health Organization's global survey on eHealth published in 2010. Southeast Asian nations reported the following as the main challenges to implementing programs:

1. Cost
2. Policy
3. Infrastructure
4. Culture

Opportunities and developments in member states" report. "Community leaders, health professionals, academic institutions and educators, health administrators, and policymakers represent the best alliance to make changes necessary to reflect and react to societal needs." □

Thanks to technological advances in prosthetics, an amputation no longer has to mean the end of a soldier's military career.

REUTERS

DIGITAL LIFELINES

When a disaster strikes, effective communication can mean the difference between life and death. Rapid advances in technology have opened new channels of communication, with many people turning to social media sites and text messaging technology in times of trouble.

"The public has begun to rely on social media to share information during emergencies with family, friends, and increasingly, with government and aid organizations who maintain social networking profiles," according to "The Case for Integrating Crisis Response with Social Media," published by the Red Cross. "The social web is creating a fundamental shift in disaster response that is asking emergency managers, government agencies, and aid organizations to mix their time-honored expertise with real-time input from the public."

After Haiti's deadly earthquake in 2010, victims reached out to the world through cellphone text messages — and the world responded. Using crisis-mapping software called Ushahidi, volunteers translated and plotted information sent via text message from survivors and those trapped in the rubble. Medics and relief workers were able to use the information to find victims and deliver aid.

The same technology was employed in Japan after the 2011 earthquake and tsunami left thousands dead and many more injured and stranded. Survivors were asked to send reports via Twitter, email or the Web with their location and firsthand information about evacuation centers, rescue needs, medical equipment, transportation updates and disaster areas. The public and relief workers could access all the reported information through a map on Sinsai.info.

As important as technology is in improving countries' responses to disaster, though, participation from the people involved is paramount. "Ten percent of this is the technology," Ushahidi's Patrick Meier told the website Technology Review, "and the other 90 percent is the people. That's truer and truer as the technology gets easier to use."

A SIKH AND

FAMILY PHOTO COURTESY OF SPC. SIMRAN PREET SINGH LAMBA

INGRID BARRENTINE/NORTHWEST GUARDIAN

A SOLDIER

A medic's childhood dream is realized when he enlists with the U.S. Army

MARISA PETRICH/*NORTHWEST GUARDIAN*

When U.S. Army Spc. Simran Preet Singh Lamba was a kid, he dreamed of joining the military. In the end, though, things weren't that simple. Lamba, who is in his late 20s, is a Sikh, a member of a 500-year-old religion founded in India. Sikhism asks that its followers not cut or shave their hair, so men wear turbans and full beards. As such, they are unable to join the U.S. Army without seeking case-by-case exemptions to uniform policy.

"The granting of these accommodations is very rare," said Amardeep Singh, director of programs for the Sikh Coalition.

Now serving with the 201st Battlefield Surveillance Brigade at Joint Base Lewis-McChord near Tacoma, Washington, Lamba is the first enlisted Sikh Soldier in nearly three decades. In fact, the only religious accommodations granted to Sikhs since the accommodations policy was enacted in the 1980s were granted in 2010, first to two officers and then to Lamba.

For a group with a long history of military service, this is an important step. "That's what a life of a Sikh is. ... Our ancestors were warriors," Lamba said.

With 20 million Sikhs worldwide, Sikhism is the planet's fifth largest religion. It is also one of its newest. It deeply values the principles of justice, equality and truth. The monotheistic religion also emphasizes service to others, particularly in the armed forces.

In the United States, requests for accommodations for religious practices are granted on an individual basis and are frequently denied for reasons of unit or individual readiness, unit cohesion and issues with morale or safety.

"Obviously, this has been a point of pain for our community," Singh said.

Lamba, originally from India, spent his childhood dressing up in uniforms and practicing the perfect salute. He wanted to join the Indian Air Force, but his parents told him to put his studies first. He came to the U.S. in 2006 to attend New York University, where he earned a master's degree in industrial engineering.

At the time, he thought serving in the U.S. military would be impossible. But when Capts. Kamaljeet Singh Kalsi and Tejdeep Singh Rattan were granted religious accommodations for their articles of faith, Lamba thought he would give it a try.

"When I came to the U.S., I decided to make this my home, make this my country," Lamba said. For him, there was no reason not to fight for it.

Because he was not a U.S. citizen at the time, he enlisted and was originally told an exemption would be made. When his request was formally denied, he appealed it with the help of the Sikh Coalition in New York.

> ## Lamba is aware that he is a pioneer. He isn't just a Soldier; he's representing what Sikhs can do in the U.S. military.

INGRID BARRENTINE/NORTHWEST GUARDIAN

Spc. Simran Preet Singh Lamba says it takes him seven minutes each morning to wrap his hair in a 5-meter-long turban.

SUSANNE KAPPLER/U.S. ARMY

Lamba and his fellow Soldiers point downrange at a hand grenade range in the U.S. state of Washington. Lamba's facial hair makes him stand out from his fellow Soldiers. But at the end of the day, he says, "I wear the same uniform. I do the same thing."

SIKHISM
at a glance

Sikhism is a monotheistic religion based on the teachings of 10 Sikh gurus.

The community of men and women initiated into Sikhism is called the Khalsa, which celebrated its 300th birthday in 1999.

Sikhs wear five articles of faith at all times: Kesh (uncut hair), Kara (a steel bracelet), Kanga (a wooden comb), Kaccha (cotton underwear), and Kirpan (a steel blade).

Sikh men have the middle name Singh, meaning lion, because they are brave and have hair on their faces. Sikh women have the middle name Kaur, meaning princess.

Nine months later, in August 2010, he officially joined the Army. He became a U.S. citizen the day he finished basic training at Fort Jackson, South Carolina, in November 2010. Eventually, Lamba, who speaks Hindi and Punjabi, plans to become an officer.

Now a combat medic, his challenge is to prove that he is exactly the same as any other Soldier, both for himself and for Sikh-Americans in the future.

"I wear the same uniform. I do the same thing. I get paid the same. I come to work at the same time. I do PT [physical training]," Lamba said. The only real difference is his turban, 5 meters of cloth that he wraps around his long hair each day. In garrison, he wears a black turban with a flash on the front, similar to Soldiers' berets. When he's in the field, he uses a camouflage under-turban that fits under his helmet.

He takes part in protective mask exercises just like any other Soldier, using petroleum jelly to create a seal despite his beard.

Lamba is aware that he is a pioneer. He isn't just a Soldier; he's representing what Sikhs can do in the U.S. military.

In fact, the Sikh Coalition would one day like to see a formal change to the uniform policy, enabling any Sikh-Americans to walk into a recruiting office and volunteer for their country as easily as their peers.

Singh is confident that Lamba, Kalsi and Rattan will demonstrate that Sikhs are capable of being excellent Soldiers, turbans or not. "At the end of the day, when Soldiers are out there in the field, on the ground, you're looking for a Soldier who can do their job," he said. □

THE FADING *Art of Geisha*

Despite some misconceptions, geisha are in fact highly skilled women who dance, play musical instruments and entertain their clients with games and conversation.

AGENCE FRANCE-PRESSE

A small, hot spring resort in eastern Japan plans to recruit three women to become geisha in an effort to preserve a tradition and to boost tourism, officials there said in September 2011.

Shimoda city, 130 kilometers southwest of Tokyo, has set aside 5.23 million yen (about U.S. $68,000) for a six-month geisha training project, using national subsidies available for employment programs, a city spokesman told Agence France-Presse.

The trainees will receive a daily wage of roughly 6,200 yen (U.S. $80) and will be expected to work five days a week, he said.

"Once they finish the program, they will demonstrate their art" at a local festival celebrating the life of a 19th-century geisha, he said.

Despite some misconceptions, geisha are in fact highly skilled women who dance, play musical instruments and entertain their clients with games and conversation.

Demand for geisha has steadily dropped over the years across Japan, but their presence at various tourist events delights visitors, the city official said.

Three decades ago, Shimoda boasted 200 active geisha, but only five part-timers remain, the city official said.

And they are the only people who have passed on local dance and songs — unique cultural assets that the city hopes to preserve.

"We hope that [the new geisha] will eventually join our efforts to revitalize the city's tourism" and stay employed in the tourism sector, he said.

"Our hope is that they will join our five geisha and carry on our traditional art," he said.

THE ASSOCIATED PRESS

AGENCE FRANCE-PRESSE

Why Are Newspapers Thriving in India?

TABEREZ AHMED NEYAZI

Newspaper circulation in many parts of the world continues to decline, thanks to 24/7 television and new media. Nowadays, instead of portending power, newspaper headlines often herald the demise of their own franchises, as venerable daily after venerable daily struggles to keep readers. Newspapers in the United States, United Kingdom and Japan have been hit the hardest. The Indian newspaper industry, however, is bucking this trend and witnessing unprecedented growth. The total newspaper circulation in India soared from 127 million in 2000 to 207 million in 2008.

Hindi and other vernacular papers have spearheaded this growth. Hindi newspapers lead with 85 million copies daily, while English newspapers stand a distant second with 32 million copies, according to circulation figures from 2008. How and why have newspapers in general and Hindi newspapers in particular been growing in India in an age of television and new media? Do newspapers in India have any lessons to offer newspapers in other parts of the world?

Rapidly rising literacy rates in the past few decades have created an upsurge in demand for Indian-language newspapers. Yet the growth of literacy alone does not represent the central factor: The percentage growth of newspaper circulation is higher than both the growth of literacy and the growth of the total population in India. In fact, the 1990s witnessed a phenomenal growth of daily newspaper circulation, at a pace almost double that of literacy rates. Literates

grew by 59 percent; newspaper circulation by 138 percent. Furthermore, daily newspaper circulations grew more rapidly in this period than at any time in the past.

The rise of grass-roots movements and popular mobilization since the 1980s resulted in new social groups entering the political arena. These groups needed to express their political aspirations and found companions in vernacular newspapers. The Hindi media helped such social groups by providing a platform to present an alternative discourse of democratic participation. They provided a voice to those who were marginally present in the mainstream English press.

In addition, localization has helped Indian-language newspapers retain their advertising revenue despite competition from television news channels and new media. Until the 1970s, Hindi newspapers were produced like English newspapers, mostly from urban centers where most of the English-reading audience resided. It took more than three decades for Hindi proprietors to find readers in the small towns and rural areas. Localization not only provided appealing, customized news to local societies, but also it helped Hindi newspapers compete with television for advertising.

Robin Jeffrey, in his seminal work on India's newspaper revolution, pointed to the success of *Eenadu*. The Telugu-language daily created a new base for local advertising from retailers, small businesses

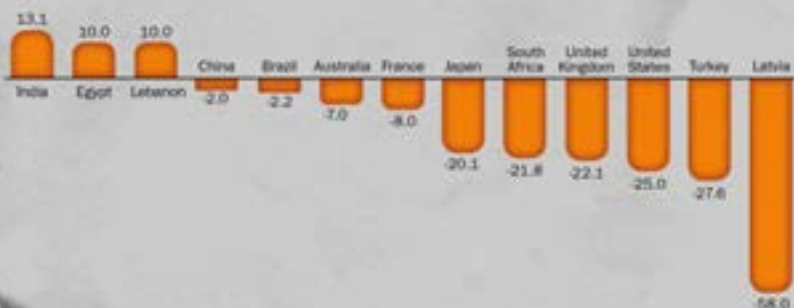and sometimes from unexpected sources such as mourning the death of prized pets and working farm animals.

Localization of news involves including local happenings, such as crimes, marriages, inauguration ceremonies and obituaries. Thus, *Dainik Jagran* and *Dainik Bhaskar*, the top two Hindi newspapers, employ large numbers of freelance writers, who need not be specialists in journalism, to send news from small towns and villages for publication in pages tailored for particular districts and towns.

Dainik Bhaskar, the second-largest-read Hindi newspaper, has 30 editions published across nine states of India. Those 30 editions have been further subdivided into various sub-editions. One edition usually has five to nine sub-editions. Currently, *Dainik Bhaskar* publishes more than 200 sub-editions daily. Only about 40 percent of the paper's content is shared across all editions, while the rest is customized to the local area and region. This helps the newspaper connect with readers by offering national news as well as highlighting regional aspirations and local sensibilities.

The expansion of Hindi newspapers into the hinterland, although directly motivated by profit, also helped create a space for marginalized groups to raise their grievances in the public arena.

Newspaper Advertising Revenues
Percentage Change 2008 to 2009

India	Egypt	Lebanon	China	Brazil	Australia	France	Japan	South Africa	United Kingdom	United States	Turkey	Latvia
13.1	10.0	10.0	-2.0	-2.2	-7.0	-8.0	-20.1	-21.8	-22.1	-25.0	-27.8	-58.0

Source: World Association of Newspapers 2010 World Press Trends annual report

FORUM ILLUSTRATION

As English newspapers concentrated in urban areas and television focused on mostly national and pan-regional coverage, Hindi newspapers targeted the local space. This localization by Hindi newspapers not only supported their survival in a competitive media environment but also earned them the reputation of being closer to the people. Hindi newspapers, thus, have become important channels to reach the masses that continue to contribute to the depth of Indian democracy.

Taberez Ahmed Neyazi is a Japan Society for the Promotion of Science postdoctoral fellow at Kyoto University.

Men turn to newspapers for information at Zaveri bazaar in Mumbai after a July 2011 bombing at the site.

THE ASSOCIATED PRESS

A Catalog of
Life

Some 8.7 million different species exist on Earth, though a tiny amount of those have actually been discovered and cataloged, researchers announced in August 2011.

The count, described by the journal *PLoS Biology*, was presented as "the most precise calculation ever offered" and replaces previous estimates that swung between 3 million and 100 million.

About 1.25 million species have been discovered and classified since Swedish scientist Carl Linnaeus standardized the taxonomy system in the mid-1700s.

The 8.7 million figure is a projection based on a mathematical analysis of currently known species.

About 86 percent of land species and 91 percent of creatures in the ocean have yet to be discovered, according to the findings by scientists at Dalhousie University in Canada and the University of Hawaii.

"Humanity has committed itself to saving species from extinction, but until now we have had little real idea of even how many there are," said co-author Boris Worm of Dalhousie University. Agence France-Presse

The birth of a rare white kiwi bird was cause for celebration in May 2011. New Zealand conservationists have been working to save the endangered species. AGENCE FRANCE-PRESSE

PHILIPPINES

Manila rice vendor
AGENCE FRANCE-PRESSE

RICE
BREAKTHROUGH
could increase harvest

Scientists expect to soon be able to remove a chalk-like part of rice, dramatically raising global harvests amid rising demand for the staple, an international research outfit said in July 2011.

The International Rice Research Institute announced the breakthrough after a 15-year study on what makes rice chalky, which causes the loss of up to a fourth of grain content in milling, said spokeswoman Sophie Clayton. The discovery follows a 2008 global crisis that saw the price of rice, the staple of half of the world, rise three-fold and pushing an estimated 100 million people into poverty.

"Until now, rice scientists did not know where in the rice genome the genes for chalkiness resided," nutrition research chief Melissa Fitzgerald said in a statement issued by the Philippines-based institute.

"Within a few years, it might be possible to breed a chalk-free grain," Clayton said, citing the research team's assessment. Agence France-Presse

POACHED IVORY
SET ABLAZE

Kenya's president set fire to more than 5 tons of elephant ivory worth U.S. $16 million in July 2011, in an act meant to focus attention on a rising tide of poaching deaths.

The bright orange flame that raced through the fuel-laden pile jumped out and nearly bit President Mwai Kibaki as he lit the mound of 335 confiscated ivory tusks and 41,000 trinkets.

"We must all appreciate the negative effects of illegal trade to our national economies. We cannot afford to sit back and allow criminal networks to destroy our common future," Kibaki told several hundred people at a rural Kenya Wildlife Service training facility in southeastern Kenya.

Africa had 1.3 million elephants in the 1970s but today has only 500,000. Kenya has 37,000 elephants, up from the 16,000 it had at the height of the crisis in 1989 but far below the country's peak. Agence France-Presse

AGENCE FRANCE-PRESSE

Spektr-R to surpass view from Hubble
AGENCE FRANCE-PRESSE

EXPLORING DEEP SPACE

Russia has launched into space its Spektr-R radio telescope, which is planned to be the most powerful ever and is the first deep-space observatory sent up by Moscow in a quarter of a century.

Spektr-R, launched in July 2011, will scour the fringes of the universe for black holes, mysterious quasar radio sources and the fast-rotating stellar remnants known as pulsars, Russian space agency Roskosmos said in a statement.

The instrument, dubbed the "Russian Hubble" after the iconic U.S. space telescope but many thousands of times more powerful, will give astronomers new opportunities for looking billions of light-years back in time to the young universe and unlocking the mysteries of black holes.

"It will allow us to look into the furthest reaches of the universe with a very sharp resolution and receive data about extra-galactic phenomena," said the project's constructor, Viktor Khartov, of the Lavochkin institute outside Moscow. Agence France-Presse

Indonesia Urges ASEAN to Harness Social Media

AGENCE FRANCE-PRESSE

The Association of Southeast Asian Nations (ASEAN) must maximize the use of Twitter, Facebook and other social media to engage the region's citizens, Indonesian President Susilo Bambang Yudhoyono said in July 2011.

Speaking to ASEAN foreign ministers on the island of Bali, Yudhoyono expressed support for the establishment of an ASEAN blogger community.

"We are facing a reality where the frequency and depth of contacts between our citizens — through cable television, email, Twitter, Facebook — far exceed the formal contacts between government officials," he said. ASEAN must "get into the act" and be "creative and open-minded in harnessing the power of technology to promote people-to-people contact," he said.

ASEAN members such as Indonesia, Malaysia, Singapore and Thailand have seen explosive growth in the use of social networks and microblogs.

Agence France-Presse

CLEANING UP
MUSIC PIRACY IN CHINA

Baidu Inc., which operates China's most popular search engine, will distribute music from three global labels. The deal, according to its partners, could help clean up China's piracy-plagued music market.

Although China is a major potential market for online music and video, rampant piracy has hampered legitimate suppliers. Music companies have sued Baidu twice, alleging it profited by maintaining "deep links" on its search engine to pirate websites.

Baidu will now distribute music from One-Stop China — a joint venture between Universal Music, Warner Music and Sony Music. Andrew Chan, One-Stop China's chief representative, hopes this commitment to legal music will cause other websites to stop using pirated copies. "They will see their big brother, Baidu, is changing to be a legal music service provider," he said. The Associated Press

AGENCE FRANCE-PRESSE

AGENCE FRANCE-PRESSE

Restaurant Puts Virtual Food Onto Diners' Plates

Want a virtual bite of what you'll eat before ordering from the menu? An Asian-themed restaurant in London's theater district is giving its customers just that, projecting images of dragon rolls, black cod and other dishes directly onto diners' plates.

Ready to place your order? Just tap the touchpad — your sashimi will be with you shortly.

Entrepreneur Noel Hunwick says he came up with the idea for the restaurant, named Inamo, several years ago while eating at a busy pizza parlor. "We were desperately trying to attract a waiter's attention," Hunwick said. "We thought: Wouldn't it be great if we could press a button and get our food?"

Having customers compose their own orders meant Inamo could cut back on staff, and it shaved about 15 minutes off the length of an average meal.

Customers waiting for their food can even play games, and those wrapping up their meals can order a taxi. The Associated Press

AGENCE FRANCE-PRESSE

Going for Greens in Thailand

Golf is big business, especially in Thailand. With 260 courses, the country has become a top golf vacation destination in Asia, according to a survey by the Tourism Authority of Thailand.

The survey, which included more than 3,000 tourists from 68 countries, showed Thailand's beaches and islands are still the biggest attraction, but golf courses were also high on the list.

Rowan Clark, senior writer for Australia's *Golf Digest* magazine, expressed excitement about a course he visited in the Khao Yai National Park. "I have never seen an elephant walking along the road to a golf course before!" he said in a news release. "The countryside there was very lush and uninhabited, which was wonderful. … I was very impressed." *FORUM* staff

JAPAN'S OLYMPIC DREAMS

AGENCE FRANCE-PRESSE

In a sign of confidence in the country's recovery, the Japanese Olympic Committee formally asked Tokyo to bid for the 2020 Summer Games.

In July 2011, Committee chief Tsunekazu Takeda met with Tokyo Gov. Shintaro Ishihara (left), who had voiced support for the city hosting of the 2020 Olympics. Ishihara was also the driving force behind the bid to host the 2016 games, which Tokyo lost out to Rio de Janeiro.

Ishihara said he wants to bring the Olympics to Tokyo as a symbol of Japan's recovery from the March 2011 earthquake and tsunami, which left about 23,000 people dead or missing in northeastern Japan.

The Associated Press

MIXED MARTIAL ARTS MADNESS

AGENCE FRANCE-PRESSE

Despite a few false starts, Asia, the home of martial arts, seems ready to take on the best in the world of modern mixed combat.

When Bae Myung Ho raised the Legend Fighting Championship welterweight title belt in July 2011, he showed it to his fans. Then the South Korean mixed martial artist went straight for the cameras. Bae fought in front of about 1,500 people in a Macau casino — but an estimated 150 million households worldwide watched on TV.

Mixed martial arts incorporates everything from Brazilian jiu-jitsu to judo, wrestling, karate and Muay Thai kickboxing. There are rules, of course, including no eye gouging or blows below the belt. Pretty much everything else goes.

"It's a sport where athletes can draw on the best from so many sports from this region, and they now have a chance to show them to the world," said Legend co-founder Chris Pollak. Agence France-Presse

A big
wedding party

Thousands of underprivileged Indonesian newlyweds from various faiths joined a mass reception in July 2011 to receive free marriage certificates that they otherwise could not afford.

About 15,000 people, including Jakarta city officials, friends and family members of the 4,541 couples, attended the reception in at the Senayan Sports Palace.

The couples included 3,112 Muslims, 1,248 Christians, Buddhists and Hindus from across the Indonesian capital.

The couples from low-income families were married in separate mass ceremonies during three months in 2011. The last 200 couples were married in July.

The Associated Press

SNORE
PATROL
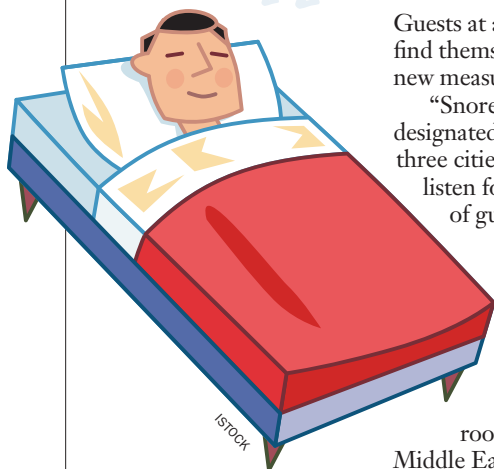
Guests at an international hotel chain may find themselves sleeping more soundly due to new measures.

"Snore monitors" patrol corridors in the designated quiet zones of Crowne Plaza hotels in three cities in the United Kingdom. Their job is to listen for offensive noises and knock on the door of guests who snore too loudly.

"We have quiet zones on two floors of the hotel. As Snore Monitor, I conduct floor walks to check for noise disruptions, paying particular attention to the quiet zone rooms," said Laura Simpson of Leeds Crowne Plaza hotel.

In Crowne Plaza's snore absorption rooms at 10 hotels in Europe and the Middle East, guests can expect soundproofing on the walls and headboards, anti-snoring pillows and white-noise machines. Reuters

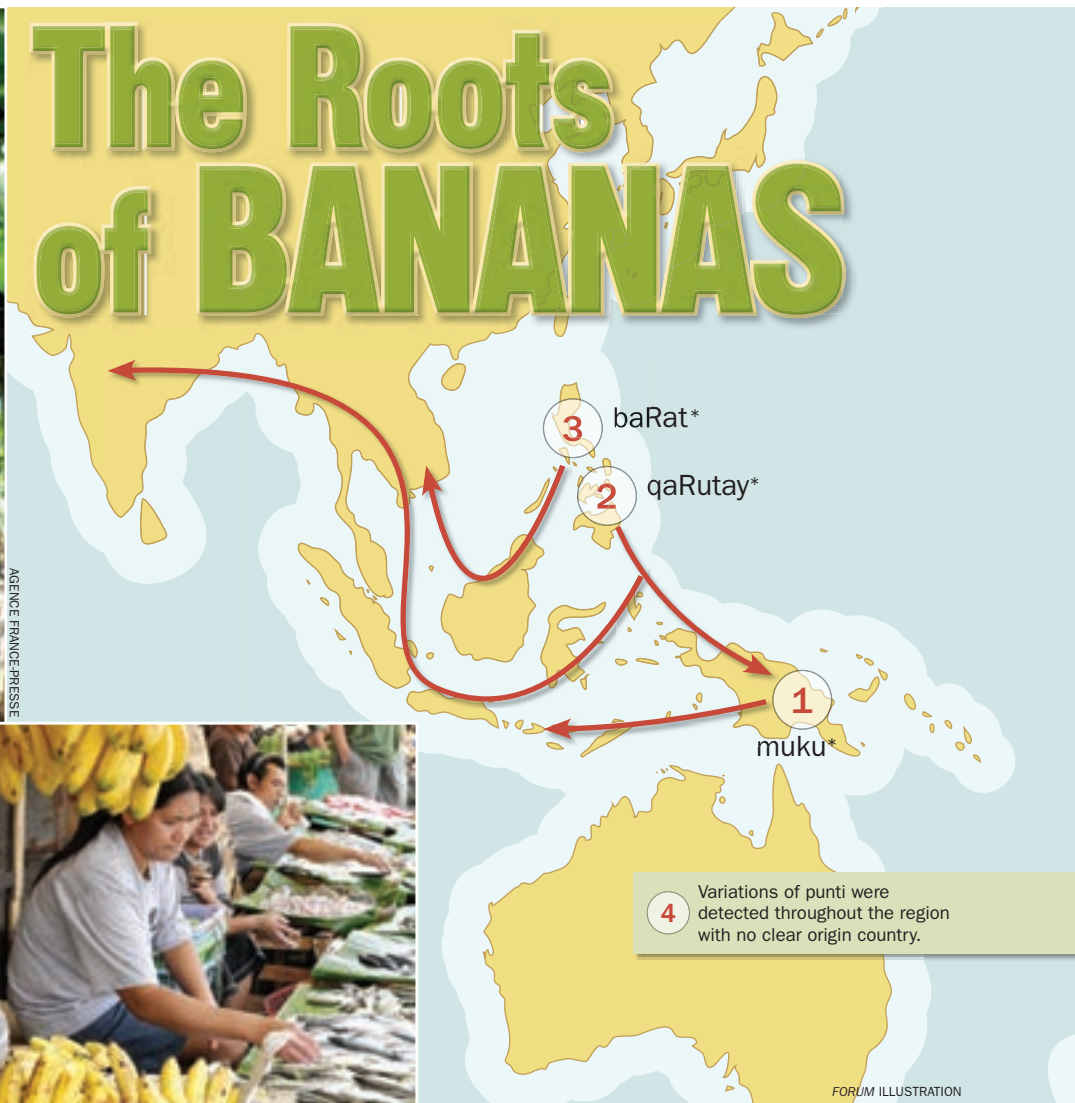ISTOCK

WORLD'S STEEPEST
ROLLER
COASTER

Fuji-Q Highland Amusement Park in Yamanashi, Japan, unveiled the world's steepest roller coaster, the Takabisha, in July 2011.

The thrilling new ride, with scenic views of Mount Fuji, lasts for just 112 seconds but is packed with jaw-dropping features, including seven twists, blackened tunnels and a 43-meter peak.

The most impressive thing about Takabisha is the free fall at 121 degrees, so steep that it has been recognized by the Guinness World Records as the steepest roller coaster made from steel. The record is the 14th set by Fuji-Q, which is one of the leading amusement parks in the world for thrill seekers. Agence France-Presse

AGENCE FRANCE-PRESSE

The Roots of BANANAS

AGENCE FRANCE-PRESSE

3 baRat*

2 qaRutay*

1

muku*

4 Variations of punti were detected throughout the region with no clear origin country.

FORUM ILLUSTRATION

AGENCE FRANCE-PRESSE

* Route for linguistic terms
Source: *Proceedings of the National Academy of Sciences*

A NEW STUDY TRACES THE HISTORY OF THE POPULAR FRUIT THROUGH SOUTHEAST ASIA

FORUM STAFF

Bananas are big business in tropical climates around the world, providing a major source of revenue and food for millions of people. Throughout history, the plants have been used for cooking, medicine, clothing, paper and even construction materials. Now domestication of the important cash crop has been traced through the ancient cultures of Southeast Asia.

Researchers used genetic testing, archaeological findings and linguistic data to outline the modern-day banana's roots. Their findings were published in July 2011 by the journal *Proceedings of the National Academy of Sciences*.

Genetic data from the bananas of today reveal a hybridization of varieties that could not have happened without the intervention of people, according to the study. Exchanges among cultures

in the island nations of Asia and the Pacific, including relocating banana plants, led to the hybridization.

Researchers determined the origin of the domesticated fruit is the island of New Guinea, where remains of banana seeds and leaves were found at archaeological sites. From there, linguists helped paint a picture of the fruit's travels. Across Southeast Asia and Melanesia, the researchers found 1,100 words for the popular fruit. However, they discovered these terms could be traced to four root words: muku, punti, qaRutay and baRat.

"A cultivated plant often migrates with its name," the researchers explained, "and when this plant is culturally innovative, its name is often retained in the receiving language." For example, the term "muku" sprouted in New Guinea, and variations spread west

across Indonesia. The term "qaRutay," on the other hand, stemmed from the Philippines, then spread south into Indonesia, west into mainland Asia and east toward New Guinea.

The trail of bananas that researchers followed from east to west also points to a migration of culture, Mark Donohue, a linguist at the Australian National University who was involved in the study, told *The Telegraph* of India.

"We know that the inhabitants of Madagascar are at least in part the descendants of an east-to-west movement about 1,200 years ago. We also have some records of people from Java and Malaysia trading with India about 2,000 years ago," Donohue told *The Telegraph*. "It could have been a minor movement in terms of the number of people, but a big transformation in terms of culture."