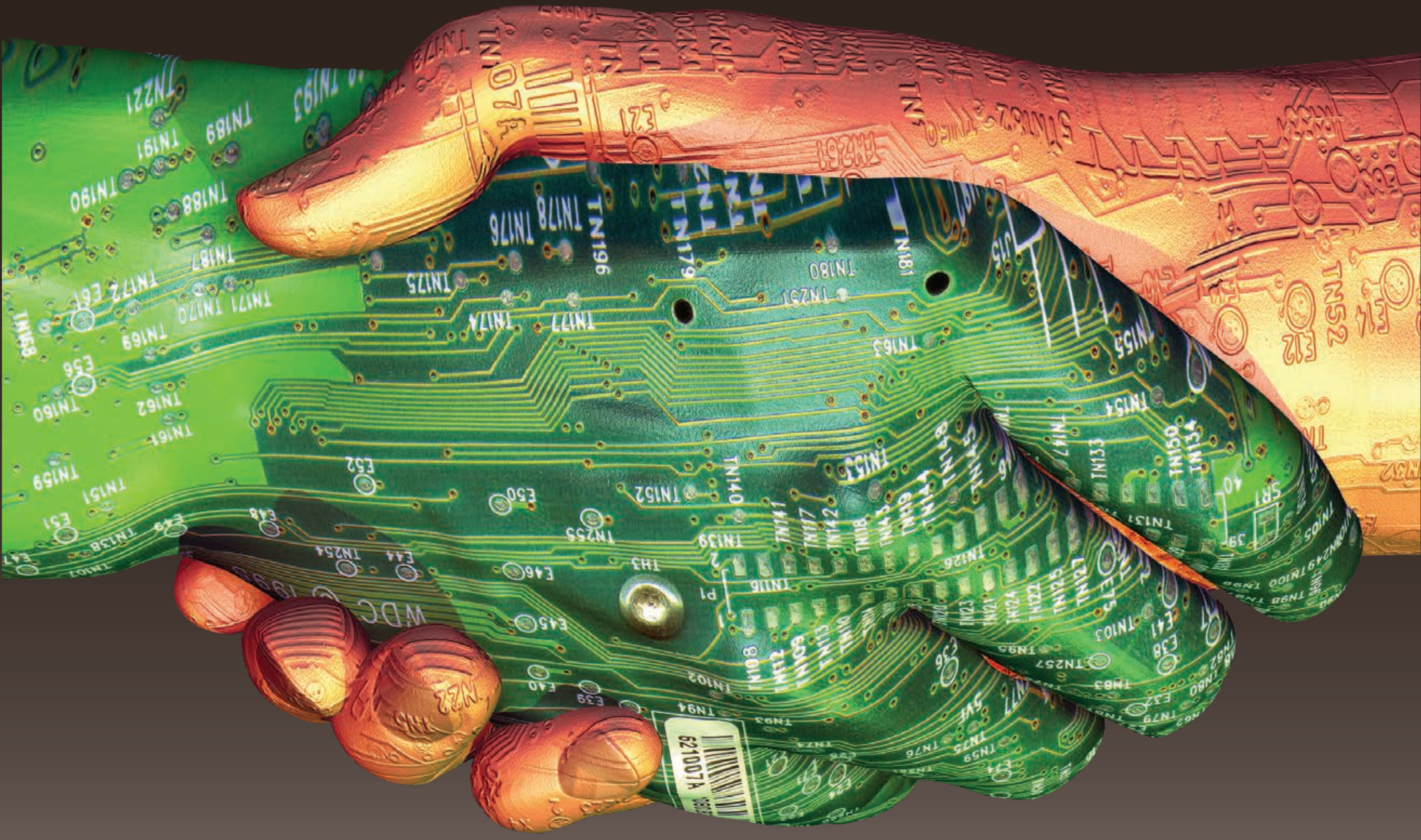
INDO-ASIA-PACIFIC DEFENSE

FORUM

VOLUME 41, ISSUE 3, 2016

Cooperating on CYBER SECURITY

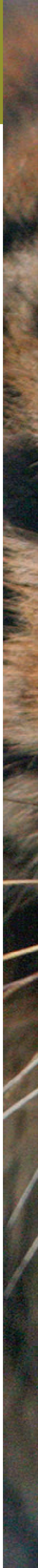


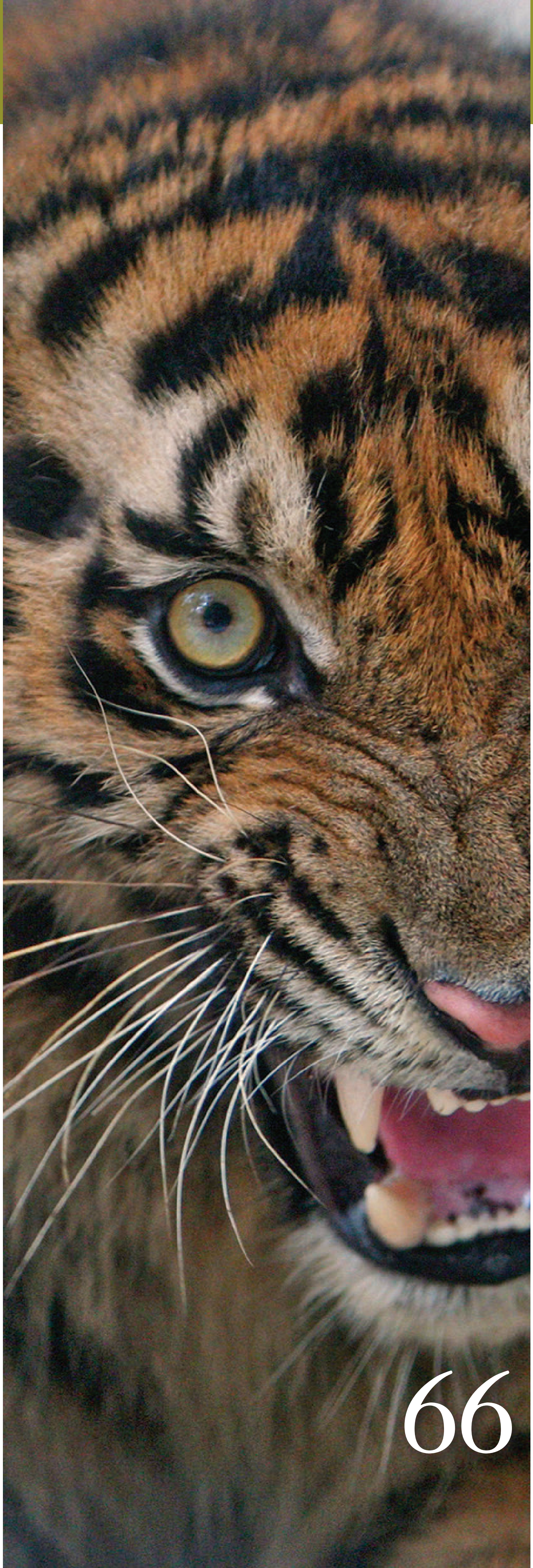
PLUS

Decoding the Enemy Online

26

features





departments

ABOUT THE COVER: This cover design emphasizes working with allies and partner nations to protect cyberspace.

FORUM ILLUSTRATION

U.S. PACIFIC COMMAND

Dear Readers,

Welcome to *Indo-Asia-Pacific Defense FORUM's* third-quarter edition for 2016, which focuses on the importance of securing cyberspace.

This issue explores common threats that Indo-Asia-Pacific nations face in the domain of cyberspace and how our global interdependence can inspire innovation, improve communication, build better institutions and safeguard fundamental freedoms. Cyber capabilities can enhance understanding among nations and boost national, regional and international security.

Building stronger partnerships and fostering a spirit of cooperation are key to understanding and addressing threats in this realm. Authorities must work to contain criminal behavior and terrorist activities in cyberspace and to suppress and counter efforts by adversaries to exploit essential information infrastructure. Failure to protect the cyber domain places individual privacy, social structures, key critical infrastructures and security at risk.

By working together, we can realize the potential for secure networks to enhance common goals for everyone's prosperity. Information sharing and continued collaboration among partner nations remain central to forging a stronger digital defense. Together, we must operate and protect our critical information technology infrastructures and promote international norms and standards for responsible behavior in this domain. Cyber security cooperation also entails sharing best practices and strengthening bilateral and multilateral engagements and partnerships. Relationships with industry and academia are also important to keep up with the latest technologies and maintain the agility needed to adapt to the rapidly evolving environment of cyberspace.

The U.S. Pacific Command is committed to working with our allies and partners to strengthen our network defenses and improve our ability to withstand and recover from cyber disruptions, intrusions and attacks. To enhance our collective security, we must work together with our allies and partners to build a future for cyberspace that is open, interoperable, secure and reliable. Assuring the free flow of information, the protection and privacy of data, and the integrity of interconnected networks is essential to international economic prosperity, security and the promotion of universal rights.

As always, I hope this edition creates dialogue about these important security challenges, and I welcome your comments. Please contact me at **iapdf@iapdforum.com** with your perspectives.

All the best,

Harry Harris

HARRY B. HARRIS, JR.
Admiral, USN
Commander, U.S. Pacific Command

IAPD **FORUM**

Cyber Awakening
Volume 41, Issue 3, 2016

USPACOM LEADERSHIP

HARRY B. HARRIS, JR.
Admiral, USN
Commander

ANTHONY G. CRUTCHFIELD
Lieutenant General, USA
Deputy Commander

MARK C. MONTGOMERY
Rear Admiral, USN
Director of Operations

PROGRAM OFFICER

MICHAEL W. CHRISTENSEN
Lieutenant Colonel, USA
IAPD FORUM Manager

CONTACT US

IAPD **FORUM**

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

www.iapdforum.com
email:
iapdf@iapdforum.com

Indo-Asia-Pacific Defense FORUM is a professional military magazine published quarterly by the commander of the U.S. Pacific Command to provide an international forum for military personnel of the Indo, Asian and Pacific areas. The opinions expressed in this magazine do not necessarily represent the policies or points of view of this command or any other agency of the U.S. government. All articles are written by *FORUM* staff unless otherwise noted. The secretary of defense has determined that the publication of this magazine is necessary for conducting public business as required by the Department of Defense.

ISSN 2333-1593 (print)
ISSN 2333-1607 (online)

COL. (RET.) ARTHUR N. TULAK is on the research faculty of Georgia Tech Research Institute, working in the Pearl City Field Office for U.S. Pacific Command J81. He is the vice president of the Hawaii chapter of the Association of Old Crows, a professional association for electronic warfare and information operations (IO). His military career included 15 years working in IO, in doctrine development and in the field as a staff officer supporting operations in Bosnia, Kosovo and Afghanistan. He has served in various Army, joint and allied headquarters in the European, Afghanistan and Pacific theaters. Featured on Page 18

DR. ALEXANDER L. VUVING is a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies. Prior to joining the center in 2008, he was an assistant professor at Tulane University and a postdoctoral fellow and associate of Harvard University's Belfer Center for Science and International Affairs at the Kennedy School of Government. His major areas of research include Asian security, the rise of China, Chinese strategy, Vietnamese politics, Southeast Asian foreign policies, the South China Sea dispute and soft power. He holds a doctorate in political science from the Johannes Gutenberg University, Germany, and has been a recipient of prestigious scholarships from the German National Academic Foundation and the Konrad Adenauer Foundation. Featured on Page 26

DR. CHING CHANG and **JACOB DOYLE** write about cyber security relations for this issue of *FORUM.* Chang, a research fellow at the Society for Strategic Studies, Taiwan, is an expert in security affairs around the Indo-Asia-Pacific region, particularly on mainland China military issues. Doyle is a regular contributor to *FORUM.* A veteran journalist with over two decades experience, he has written for publications such as the *Budapest Business Journal*, *Czech Business Weekly*, *Construction and Investment Journal* and *City Newspaper* of Rochester, New York. He is based in Turkey. Featured on Page 40

JUSTIN PUMMELL is a geographer with the U.S. Army Corps of Engineers. He supports U.S. Pacific Command, U.S. Army Pacific, partner nations and others in designing capacity development projects and exercises that enhance readiness and response to all hazards. Featured on Page 44

Join the Discussion

We want to hear from YOU!

Indo-Asia-Pacific Defense FORUM caters to military and security personnel in the Indo-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
Indo-Asia-Pacific Defense FORUM
HQ USPACOM, Box 64013
Camp H.M. Smith, HI
96861-4013 USA

Indo-Asia-Pacific Defense FORUM offers extensive content online, with new articles posted daily, at **www.iapdforum.com**

Visitors can:

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

FORUM

Exploring the issues that impact so many lives

CHINA

REUTERS

FEARING POLLUTION, FAMILIES BUILD 'BUBBLES'

Liu Nanfeng has five air purifiers, two air quality monitors and a water purification system in his Beijing apartment. He buys organic. Still, he worries for his toddler daughter's health.

"I feel safe at home, but when we go out to the mall, the indoor and outdoor air are the same," the 30-something screenwriter said. "It feels hopeless."

China's persistent pollution and regular product safety scandals are driving an increasing number of consumers to build bubbles of clean air, purified water and safe products at home and in their cars.

Twice in January 2016 alone, Beijing's city government issued pollution "red alerts," the first time it had triggered its most severe smog warning.

While there is no official data on their numbers, market analysts say Liu's tastes reflect the concerns of a large and growing group of well-heeled urban consumers.

Foreign and domestic companies are starting to take notice of what could be called "bubble families," a demographic whose emergence has been fueled by new technologies and the rapid spread of e-commerce.

Websites such as Alibaba's Taobao.com have made it easier to find products from overseas that are perceived as safer.

Among upper-middle-class parents in China's bigger cities, buying toys and skin care products for children from overseas is common.

Reuters

BURMA

Fossilized lizard is clue to 'lost ecosystem'

A fossilized lizard found preserved in amber in Southeast Asia dates back 99 million years, scientists have determined, making it the oldest specimen of its kind and a "missing link" for reptile researchers.

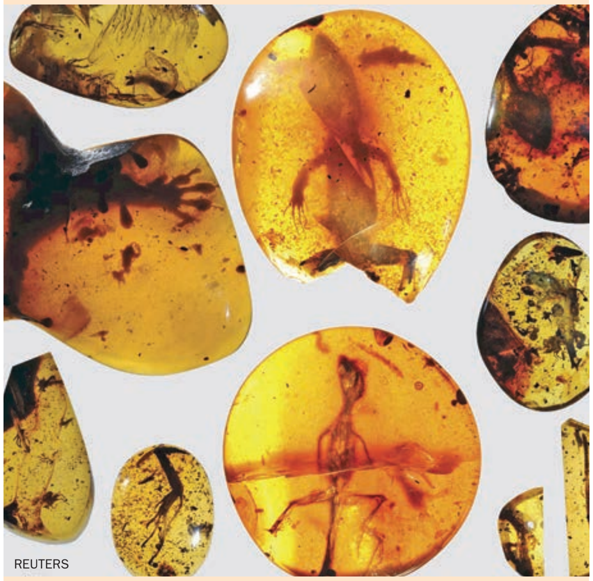
The lizard is 75 million years older than the previous record holder, according to researchers at the Florida Museum of Natural History, who announced the finding in March 2016.

It was found decades ago in a mine along with other ancient, well-preserved reptile fossils, but the scientists were able to analyze the finds only recently.

"It was incredibly exciting to see these animals for the first time," said Edward Stanley, a member of the research team. "It was exciting and startling, actually, how well they were preserved."

Scientists believe the chameleonlike creature was an infant when it was trapped in a gush of sticky resin while darting through a tropical forest in what is now Burma.

Small reptiles have delicate bodies and typically deteriorate quickly, he said. Being encased in solid amber helped to protect the specimen.


REUTERS

Stanley and other researchers used high-resolution digital X-ray technology to examine the creatures and estimate the age of the amber without breaking it.

The discovery will help researchers learn more about the "lost ecosystem, the lost world" to which the creatures belonged, Stanley said, and it may help researchers learn more about the creatures' modern relatives.

"It's kind of a missing link," Stanley said. Reuters

THAILAND

OFFICIALS STRUGGLING TO MOVE RICE MOUNTAINS BY 2017

Thailand's military government will struggle to offload by a 2017 deadline some 14 million tons of rice in state warehouses left over from a policy of the civilian government it ousted, traders and exporters said.

The government inherited 18.7 million tons of rice built up under the previous government's rice subsidy scheme and has since held 12 auctions, offloading about 5 million tons of rice worth U.S. $1.39 billion.

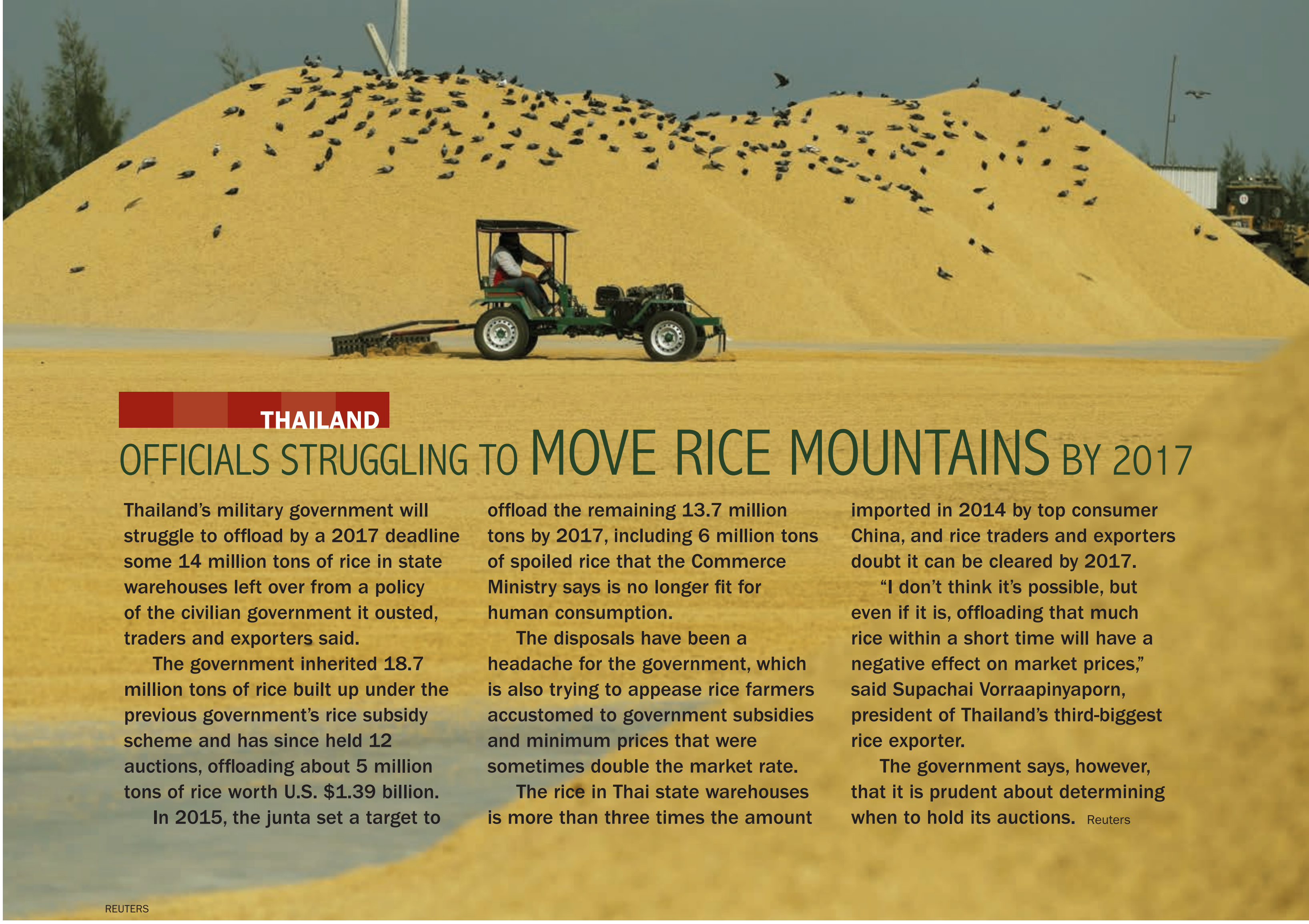
In 2015, the junta set a target to offload the remaining 13.7 million tons by 2017, including 6 million tons of spoiled rice that the Commerce Ministry says is no longer fit for human consumption.

The disposals have been a headache for the government, which is also trying to appease rice farmers accustomed to government subsidies and minimum prices that were sometimes double the market rate.

The rice in Thai state warehouses is more than three times the amount imported in 2014 by top consumer China, and rice traders and exporters doubt it can be cleared by 2017.

"I don't think it's possible, but even if it is, offloading that much rice within a short time will have a negative effect on market prices," said Supachai Vorraapinyaporn, president of Thailand's third-biggest rice exporter.

The government says, however, that it is prudent about determining when to hold its auctions. Reuters



REUTERS

LARGE HAULS OF BLACK-MARKET *ivory seized*

VIETNAM, THAILAND

AFP/GETTY IMAGES

Nearly 3 tons of ivory seized in Vietnam and Thailand show that the black market trade for illegal animal parts is still thriving in Southeast Asia.

Vietnamese officials said 2.2 tons of tusks, originating from Mozambique, were discovered in December 2015 buried among sacks of beans.

In Thailand, wildlife officials displayed more than 700 kilograms of ivory items that were seized around the same time on the island of Koh Samui.

A customs official said the tusks were found in a cargo container that was marked as carrying hair wigs, adding that the shipment had been sent from Singapore and was on its way to Laos.

Tusks and other body parts of elephants are prized for decoration as talismans and for use in traditional medicine across parts of the Indo-Asia-Pacific region, with China being a major market for such products.

The international trade in ivory, with rare exceptions, has been outlawed since 1989 following a drop in the population of African elephants from millions in the mid-20th century to just 600,000 by the end of the 1980s.

That has not stopped criminal gangs, however, seeking to exploit the continued demand for the material. Agence France-Presse

China passes CONTROVERSIAL Counterterrorism Law

REUTERS AND THE ASSOCIATED PRESS

China's parliament passed a controversial new anti-terrorism law in December 2015 that requires technology firms to hand over sensitive information such as encryption keys to the government and allows the military to venture overseas on counterterror operations.

Chinese officials say their country faces a growing threat from militants and separatists, especially in its unruly Western region of Xinjiang, where hundreds have died in violence in the past few years.

An Weixing, head of the Chinese Public Security Ministry's counterterrorism division, speaks at a news conference after the parliament passed a controversial new anti-terrorism law in late December 2015. REUTERS

The law has attracted deep concern in Western capitals not only because of worries that it could violate human rights such as freedom of speech but also because of the law's cyber provisions. U.S. President Barack Obama raised concerns about the law directly with Chinese President Xi Jinping.

While a provision in an initial draft that would require companies to keep servers and user data within China was removed from the final law, technology companies will still have to provide help with sensitive encryption information if law enforcement authorities demand it.

Speaking after China's largely rubber-stamp parliament passed the law, Li Shouwei, deputy head of the parliament's criminal law division under the legislative affairs committee, said China was simply doing what other Western nations already do in asking technology firms to help fight terror.

This will not affect the normal operation of tech companies, and they have nothing to fear in terms of having "back doors" installed or losing intellectual property rights, Li added.

Officials in Washington have argued that the law, combined with new draft banking and insurance rules and a slew of anti-trust investigations, amounts to unfair regulatory pressure targeting foreign companies.

Left: Anti-terrorism paramilitary police take part in a drill in Changsha, Hunan province, in December 2015.
REUTERS

China's national security law adopted in July 2015 requires all key network infrastructure and information systems to be "secure and controllable."

The anti-terrorism law also permits the People's Liberation Army to get involved in anti-terrorism operations overseas, though experts have said China faces major practical and diplomatic problems if it ever wants to do this.

An Weixing, head of the Public Security Ministry's counterterrorism division, said China faced a serious threat from terrorists, especially "East Turkestan" forces, China's general term for Islamist separatists it says operate in Xinjiang.

"Terrorism is the public enemy of mankind, and the Chinese government will oppose all forms of terrorism," An said.

Rights groups, though, doubt the existence of a cohesive militant group in Xinjiang and say the unrest mostly stems from anger among the region's Muslim Uighur people over restrictions on their religion and culture.

The new law also restricts the right of media to report on details of terror attacks, including a provision that media and social media cannot report on details of terror activities that might lead to imitation, nor show scenes that are "cruel and inhuman."

The National People's Congress said its standing committee adopted the law with a unanimous vote. The law went into effect January 1, 2016.

Rights advocates and foreign governments have expressed concerns about the law's likely impact on tech businesses and freedom of speech.

They say it is troublesome that telecommunications companies and Internet service providers are required to share encryption keys and back door access with the police and state security agents seeking to prevent terrorist activities or investigating terror acts.

Chinese officials said in late December 2015 that the requirements for the tech firms are necessary because terrorists are increasingly turning to cyberspace.

They said lawmakers balanced the needs to fight terrorism and to protect business interests and public rights.

"Relevant regulations in the anti-terrorism law will not affect the normal business operation of companies, and we do not use the law to set up 'back doors' to violate the intellectual property rights of companies," Li said,

"The law will not damage people's freedom of speech or religion," Li said.

Beijing has asserted that China is a victim of global terrorism following violent ethnic clashes involving members of the Muslim minority Uighur community in the far northwest region of Xinjiang. Foreign experts, however, have argued that there is no proof of foreign ties and that the violence in Xinjiang might be homegrown.

China has accused the West of adopting double standards. Beijing recently refused to renew the press credentials of a French journalist, effectively expelling her, for questioning Beijing's equating of ethnic conflicts with global terrorism.

Li said at a news conference that China's anti-terrorism law targets no specific region, ethnicity or religion.

FORUM ILLUSTRATION

DECODING NORTH KOREA'S CYBER WARRIORS

FORUM STAFF

Governments are combating the threat by scrutinizing the nation's cyber operations and sharing information on attacks

Monday, November 24, 2014. Employees at Sony Pictures Entertainment headquarters receive a flashing image on their computer screens of a skull, long skeletal fingers and a message: "This is just a beginning. We've obtained all your internal data." Then comes a warning to obey demands or risk having "top secrets" exposed. A week later — amid prerelease publicity for a Sony film called *The Interview* that mocks North Korean leader Kim Jong Un in a plot calling for his assassination — hackers leak the salaries of studio executives and other proprietary company information.

Wednesday, March 20, 2013. Malware known as "DarkSeoul" spreads across South Korea, crippling computers, news broadcasting servers and financial institutions. The affected broadcasters had previously been identified by North Korea as targets when Kim threatened to destroy government installations in the South.

In March 2011, hackers launched a distributed denial of service (DDoS) attack — dubbed "Ten Days of Rain" by computer security firm McAfee — against South Korean government websites and the United States Forces Korea network. The attack lasted 10 days, after which it stopped, self-destructing itself and the systems it had infected.

North Korea maintains it had zero involvement with the attacks. Digital forensic investigators suggest otherwise.

U.S. Federal Bureau of Investigation Director James B. Comey said that in the Sony case, the hackers unwittingly helped reveal themselves when they got "sloppy."

"Several times, either because they forgot or they had a technical problem, they connected directly and we could see them. And we could see that the IP [Internet protocol] addresses that were being used to post and to send the emails were coming from IPs that were exclusively used by the North Koreans," Comey said about threatening emails sent by hackers to Sony employees, according to a January 2015 report by the *Financial Times* newspaper.

North Korean leader Kim Jong Un REUTERS

Despite this hacker blunder in the Sony attack, experts say North Korea's cyber operations have advanced — though detailing to what extent remains a challenge.

"It is difficult to pinpoint exactly how advanced North Korea's technical capabilities are, given the paucity of available open source analysis," according to a research report titled "What Do We Know About Past North Korean Cyber Attacks and Their

The cyber army North Korea has amassed, along with its budding capabilities, can seem inconceivable, particularly when most North Koreans have never seen the Internet.

Capabilities?" by independent consultants Jenny Jun, Scott LaFoy and Ethan Sohn. "Certainly, they have evolved beyond rudimentary DDoS attacks against websites they have often resorted to in the past decade, into more targeted, complex and well-organized operations involving several stages of exploitation of a target system or network. They are capable of social engineering, extended advanced persistent threat campaigns and employment of less sophisticated but sufficiently effective malware," said the December 2014 report, published by the Washington, D.C.-based Center for Strategic and International Studies (CSIS). "Given the rapid rate of improvement in their operational capability, in the future, we may see them trying to work on the types of attacks more destructive and permanent in effect, such as attacks through compromise of supply chains or compromising supervisory control and data acquisition networks."

A map at the Cyber Terror Response Center in South Korea shows how cyber warfare would be waged on the Korean Peninsula. THE ASSOCIATED PRESS

At least one expert speculates that North Korea's cyber operations could rank among the top 10 in the world. That doesn't mean they have what it takes to execute a sophisticated computer virus, according to James Lewis, director and senior fellow for CSIS' Strategic Technologies Program. "They're not going to be able to do the most damaging kind of cyber attack," Lewis told *The Christian Science Monitor* newspaper in February 2015.

Governments shouldn't underestimate them, though. Lewis also noted that North Korea has created a network of state-sponsored black market operations in places such as Japan, Singapore and Malta.

"This gives North Korea another pipeline into the tech world," Lewis told *The Christian Science Monitor*. "They have an ability to use Japan, China and this black market."

The cyber army North Korea has amassed, along with its budding capabilities, can seem inconceivable, particularly when most North Koreans have never seen the Internet, according to experts. Several sources say professional hackers in the North number between 1,000 and 3,000.

"North Korea is emerging as a significant actor in cyberspace with both its military and clandestine organizations gaining the ability to conduct cyber operations," Jun, LaFoy and Sohn wrote in a September 2015 executive summary published by CSIS and titled, "North Korea's Cyber Operations: Strategy and Responses."

The trio of researchers sought to create a comprehensive open source reference material because, in their analysis, little unclassified information existed on North Korea's cyber operations. They also want to change the public's perception about attacks linked to North Korea.

"Think about North Korea cyber attacks as not merely isolated incidents but a series of deliberate choices the North Korean government made as part of its larger strategies," Jun said at CSIS during a discussion of her team's research. "When we look at how cyber operations are organized, they're unlikely to be abandoned by the regime in the near future."

The cyber operations report describes North Korea's Reconnaissance General Bureau and General Staff Department, the two organizations charged with planning and executing the North's cyber strategy. Here's what the report says about each:

Reconnaissance General Bureau (RGB): "The RGB is the primary intelligence and clandestine operations organ known within the North Korean government and is historically associated with peacetime commando raids, infiltrations, disruptions and other clandestine operations, including the 2014 Sony Pictures Entertainment attack. The RGB controls the bulk of known DPRK [Democratic People's Republic of Korea] cyber capabilities, mainly under Bureau 121 or its potential successor, the Cyber Warfare Guidance Bureau. There may be a recent or ongoing reorganization within the RGB that promoted Bureau 121 to a higher rank or even established it as the centralized entity for cyber operations. RGB cyber capabilities are likely to be in direct support of the RGB's aforementioned missions. In peacetime, it is also likely to be the more important or active of the two main organizations with cyber capabilities in the DPRK."

General Staff Department (GSD): "The General Staff Department of the KPA [Korean People's Army] oversees military operations and units, including the DPRK's growing conventional military cyber capabilities. It is tasked with operational planning and ensuring the readiness of the KPA should war break out on the Korean Peninsula. It is not currently associated with direct cyber provocations in the same way that the RGB is, but its cyber units may be tasked with preparing disruptive attacks and cyber operations in support of conventional military operations. North Korea's emphasis on combined arms and joint operations suggests that cyber units will be incorporated as elements within larger conventional military formations."

LaFoy, one of the cyber operation report's co-authors, said understanding the inner workings of the North's organizations from what information has become publicly available proves a valuable resource.

"The North Koreans don't publish their strategies, so we're left to deduce what they're planning or opting to do," LaFoy said. "Looking at organizations like the RGB to see what they've been previously associated with, and what they're associated with now."

LaFoy said North Korea's cyber attacks do just enough to upset the natural flow on the Korean Peninsula but stop short of anything that would cause an actual war: "A violent conflict that the North Koreans can neither control nor win," he said. "Cyber gives them a low risk, low means of chipping away at the status quo without reaching an armed provocation or an armed attack."

Han Hui, a professor at Seoul Media Institute of Technology, claimed in November 2015 that the North had a cyber attack strategy to paralyze as much as 50 percent of South Korea's information technology infrastructure.

"North Korea's goal is to destroy the South Korean leadership by physical, psychological attacks, tying it to cyberattacks, then bringing about wide-scale panic," Han said, according to news agency United Press International (UPI).

Addressing the threat, Han said, means the South must go beyond creating new institutions or expanding existing ones. It must train South Korean cyber personnel in new skills, he told UPI.

Beyond equipping personnel with training to detect and deter cyber attacks, the CSIS cyber operations report listed four main policy objectives for managing the emerging North Korean cyber threat:

- Prepare a graduated series of direct responses targeting North Korea's cyber organizations.
- Curb North Korea's operational freedom in cyberspace.
- Identify and leverage North Korea's vulnerabilities to maintain strategic balance.
- Adopt damage mitigation and resiliency measures to ensure that critical systems and networks maintain operational continuity despite suffering an attack.

A man walks by a gate at the Cyber Terror Response Center of National Police Agency in Seoul. THE ASSOCIATED PRESS

Jun stressed that a critical recommendation for all governments calls for continuous cyber defense dialogues regarding North Korea's cyber capabilities. Open information sharing also has an added benefit, according to Jun and her team. It forces North Korea to change its tactics, techniques and procedures, increasing the cost and risk of each cyber operation.

"Information sharing is real important here," she said. "The more we share amongst each other what North Korea's attack methods and tools are, that prepares each defender because it provides a more comprehensive view to the threat and that allows each [nation] to reduce [its] own vulnerabilities themselves." □

CYBER

CRIME WAVE

FORUM ILLUSTRATION

THE INDO-ASIA-PACIFIC IS A GLOBAL HUB OF DIGITAL CRIME, WHICH HAS BECOME ONE OF THE FASTEST-GROWING ILLICIT ACTIVITIES ON THE PLANET

FORUM STAFF

The luxurious mansion was supposed to be vacant. When Indonesian police investigators burst inside at 6 a.m. in late July 2015, however, they uncovered a bustling cell of an international cyber crime network.

A syndicate believed to be organized by a Chinese citizen living in Hong Kong recruited the 31 young Chinese and Taiwan nationals found inside. They had been operating for a month in the upscale residence in the Indonesian port city of Medan before the raid, according to an account in *The Jakarta Post* newspaper.

"They suddenly moved quickly to burn the evidence as we entered the house," North Sumatra Police special crimes director Ahmad Haydar told the newspaper. Nevertheless, authorities seized 65 cellphones as well as laptops, routers, walkie-talkies and banknotes in five currencies.

Just a month later, in August 2015, a team of Jakarta, Taipei City and Chinese police broke up another cyber crime nexus of more than 90 Chinese and Taiwan nationals operating out of low-key offices around Jakarta. The scammers posed as public officials when they contacted businesspeople in China, promising to allocate projects to them in exchange for payment, Jakarta Police crime directorate head Krishna Murti told *The Jakarta Post.*

"The victims are mostly from China and Taiwan. The network itself was protected by big [criminal] organizations in Japan such as the Yakuza," Krishna said. "The crime involves four countries."

That's a leading challenge posed by digital crime: It often involves many countries. Hackers operate in a borderless Internet where geographic and political boundaries have little meaning.

This is an especially acute problem for the Indo-Asia-Pacific region, which has become a global hub of cyber crime for a number of reasons, including the rapid pace of the region's economic and technological advancement and its ready adoption of the Internet.

"As one of the fastest-growing criminal activities on the planet, cyber crime is moving higher up the agenda of countries around the globe," the United Nations Office on Drugs and Crime (UNODC) reported during a 2011 conference in Seoul that brought together cyber security experts from more than 20 Indo-Asia-Pacific nations.

"The easy access and widespread use of the Internet has attracted a range of criminal activities," UNODC affirmed. "From computer data theft and fraud-like phishing to content-related offenses, including copyright issues and online child pornography, the Internet offers criminals an increasingly lucrative sphere in which to operate."

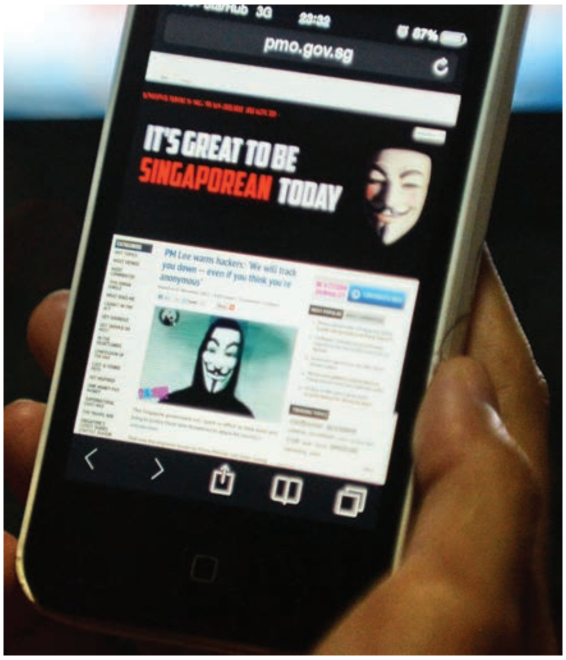
Investigating across multiple jurisdictions makes dealing with digital crime a complicated task. The borderless nature of such crimes has prompted increasing calls for more transnational cooperation and regulation of cyberspace.

"Cyber borders are blurring with cyber criminals located worldwide, making it increasingly challenging for any one organization to fight cyber crime alone," Microsoft said in a statement in 2015 as it launched its new Cybercrime Satellite Center in Singapore. "Rising sophistication in cyber crime and its devastating impact on governments, industry and individuals has also made the sharing of cyber threat intelligence key to an effective cyber security ecosystem."

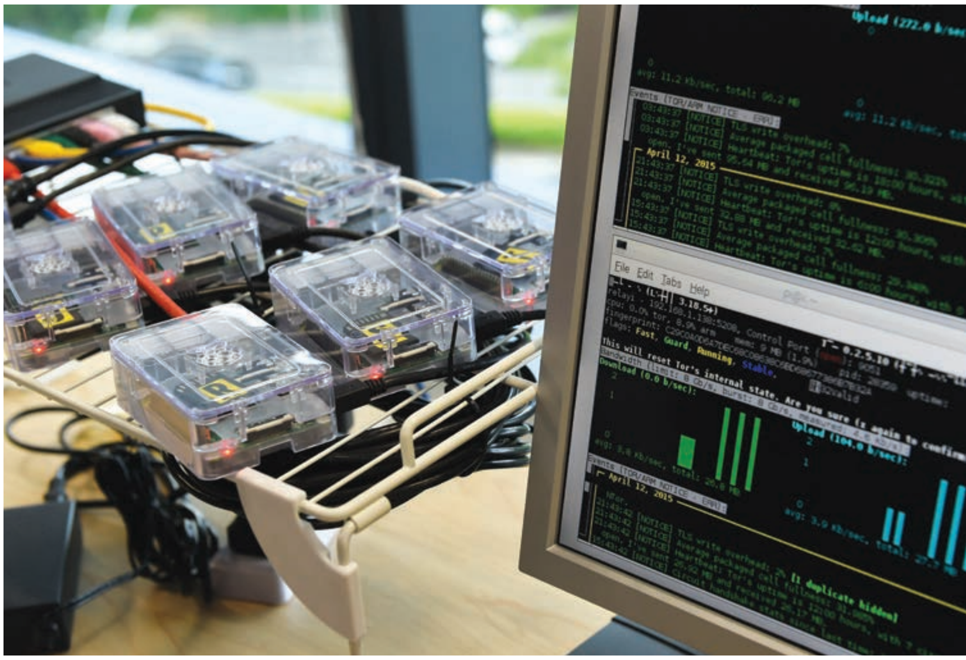
EMERGING COUNTERMEASURES

The Indo-Asia-Pacific region's governments and various cyber crime-fighting authorities are addressing the problem:

- Interpol, a network of police forces from 190 countries all over the world, opened a state-of-the-art cyber crime center in 2015 in Singapore. The Interpol Global Complex for Innovation (IGCI) provides high-tech assistance and training to member countries' law enforcement agencies on digital security, capacity building and training, and operational and investigation support.
- In 2015, Microsoft opened its fifth Cybercrime Satellite Center in the financial hub of Singapore. It serves as a regional command post for the software giant to undertake cyber security initiatives throughout Southeast Asia. Microsoft's other cyber crime satellite facilities are located in Beijing, Tokyo, Washington and Berlin.
- Senior diplomats from China, Japan and South Korea met for cyber security conferences in 2014 in Beijing and in 2015 in Seoul — the first meetings of their kind, according to China's Xinhua News Agency. They discussed possibilities for trilateral cooperation in fighting cyber crime and terrorism. They established a cyber crime directors workshop involving the three nations and Hong Kong.
- The U.S. Justice Department in late 2015 stationed a new "cyber prosecutor" — a legal advisor — in Malaysia to help Southeast Asian nations establish the laws and tools needed to fight hackers, according to The Associated Press. "The position is intended to shore up international partnerships against a type of crime that's without



AFP/GETTY IMAGES



AFP/GETTY IMAGES

geographic borders and is often carried out by overseas hackers," The Associated Press reported.

- In response to a growing number of cyber offenses in Indonesia, the Australian Federal Police and Indonesian National Police combined forces to open a pair of joint cyber crime offices in 2014 and 2015 — one at the Indonesian National Police headquarters and the other at the Jakarta Police headquarters, according to the *Jakarta Globe* newspaper. "We will also expand partnerships with other countries, not just Australia," Cmdr. Gen. Nanan Sukarna, a (former) National Police deputy chief, told the newspaper.

MYSTIQUE, SECRECY SHROUD ENFORCEMENT

What is digital crime? The definition is continually evolving with the technology.

"Cyber crime is increasingly conducted by a highly specialized chain of software break-in experts, underground market-makers and fraudsters who convert stolen passwords and identities into financial gains," said a 2014 Reuters report on the issue. "Criminals can keep data for months or even years before using it to defraud victims."

Hackers can target corporations, individuals and governments, experts say.

It's a booming business. A 2014 study by market research firm International Data Corp. and the National University of Singapore found that businesses worldwide were spending about U.S. $500 billion per year to deal with malware — software designed to disrupt or gain access to their computer systems. The study called malware "a lucrative vector for cyber crime." Businesses in the Indo-Asia-Pacific region were spending U.S. $230 billion, nearly half of the total amount.

A July 2015 *Bloomberg Business* article asserted that a "veil of secrecy" was helping to feed a surge of cyber attacks in the region. Cyber security analysts lamented that, in most cases, Indo-Asia-Pacific companies that get hacked are rarely required to report it to the authorities.

"In an era where more and more data is stored online and attacks are discovered with alarming regularity, the lack of reporting mechanisms means there's no telling how often or how much personal information is taken from databases in Asia," *Bloomberg Business* reported. It further noted that companies in the Indo-Asia-Pacific get targeted by hackers up to 40 percent more frequently than the global average.

If security breaches aren't made public, then hackers are given the leeway to simply use the same strategies over and over again. "The culture of silence regarding cyberattacks in Asia serves as fuel to the guild of thieves who operate with impunity in the region," Tom Kellermann, chief cyber security officer at software developer Trend Micro Inc., told *Bloomberg Business.*

This dynamic is what's leading to calls for more cross-border collaboration in the fight against digital crime.

"In order to effectively address issues related to multijurisdictional cooperation in cyber crime investigations, there is a need for countries to have bilateral, regional and international agreements specifically tailored to meet the requirements of the cyber domain," Noboru Nakatani, executive director of the Interpol Global Complex for Innovation (IGCI) in Singapore, told *FORUM*. (See "Key Leader Profile" on Page 58.)

LEFT: Signs of the activist hacker group Anonymous appear on the website of Singapore Prime Minister Lee Hsien Loong on November 7, 2013, after he vowed to hunt down anyone who attacked the city-state's technology network.

Devices to simulate cyber crime sit at the Interpol Global Complex for Innovation during its opening ceremony in Singapore in April 2015.

> **"As Asian countries become wealthier, fraud and extortion committed over the Internet will increase."**
>
> — "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia"

The gleaming new Interpol complex, equipped with a digital forensics laboratory, assists law enforcement throughout the region with cyber crime investigations.

Bradley Marden, the IGCI's coordinator for digital crime investigative support, told the technology news website ZDNet in September 2015 that criminal hackers were broadening their targets beyond banks. "Now they're being more creative in monetizing the compromise and not limiting themselves to banks and financial institutions, where previously they would target just bank accounts and credit card information," he told ZDNet.

Eric Chan, regional technical director for Southeast Asia and Hong Kong for the network security company Fortinet, told ZDNet that hackers routinely use email to intrude into computer systems. About 30 percent of cyber attacks are launched via email, with recipients clicking on roughly 25 percent of the illicit emails, Chan added.

Governments also remain at risk from cyber attacks. In January 2016, for example, the international hacking network called Anonymous targeted Thai police and government websites. Hackers temporarily shut down the sites to protest the death sentences that two Burmese migrant workers received in connection with the 2014 slayings of two British tourists, Reuters reported.

MOUNTING RISKS

Which countries in the region are most at risk from cyber crime? The answer depends on which experts you ask.

"Computer security experts say developed, technology-rich Asian countries like Japan, South Korea and Taiwan are particularly vulnerable to attacks," Reuters reported.

Microsoft, however, came to a somewhat different conclusion. The software giant noted that its most recent Security Intelligence Report found that emerging economies in the Indo-Asia-Pacific region were particularly vulnerable to malware: "The study revealed that out of the top five locations across the globe most at risk of infection, a total of four are from the Asia Pacific — Pakistan, Indonesia, Bangladesh and Nepal, topping the rankings at first, second, fourth and fifth places respectively in terms of computers encountering malware."

The Australian Strategic Policy Institute and the International Cyber Policy Centre analyzed the so-called "cyber maturity" of 20 countries that make up a wide geographical and economic cross section of the region in a study titled "Cyber Maturity in the Asia Pacific Region 2015." Analysts reviewed the implementation and operation of cyber-related structures, policies, legislation and organizations.

"South Korea, Singapore and Japan are noteworthy for the breadth of their cyber policy governance frameworks and the effectiveness of their implementation," the study said. "In contrast, other states are still working to develop the necessary telecommunications infrastructure to increase digital access for their citizens. These states, including Laos, Cambodia, Papua New Guinea and Fiji, tend to place responsibility for cyber policy and security in the hands of their telecommunications-related agencies."

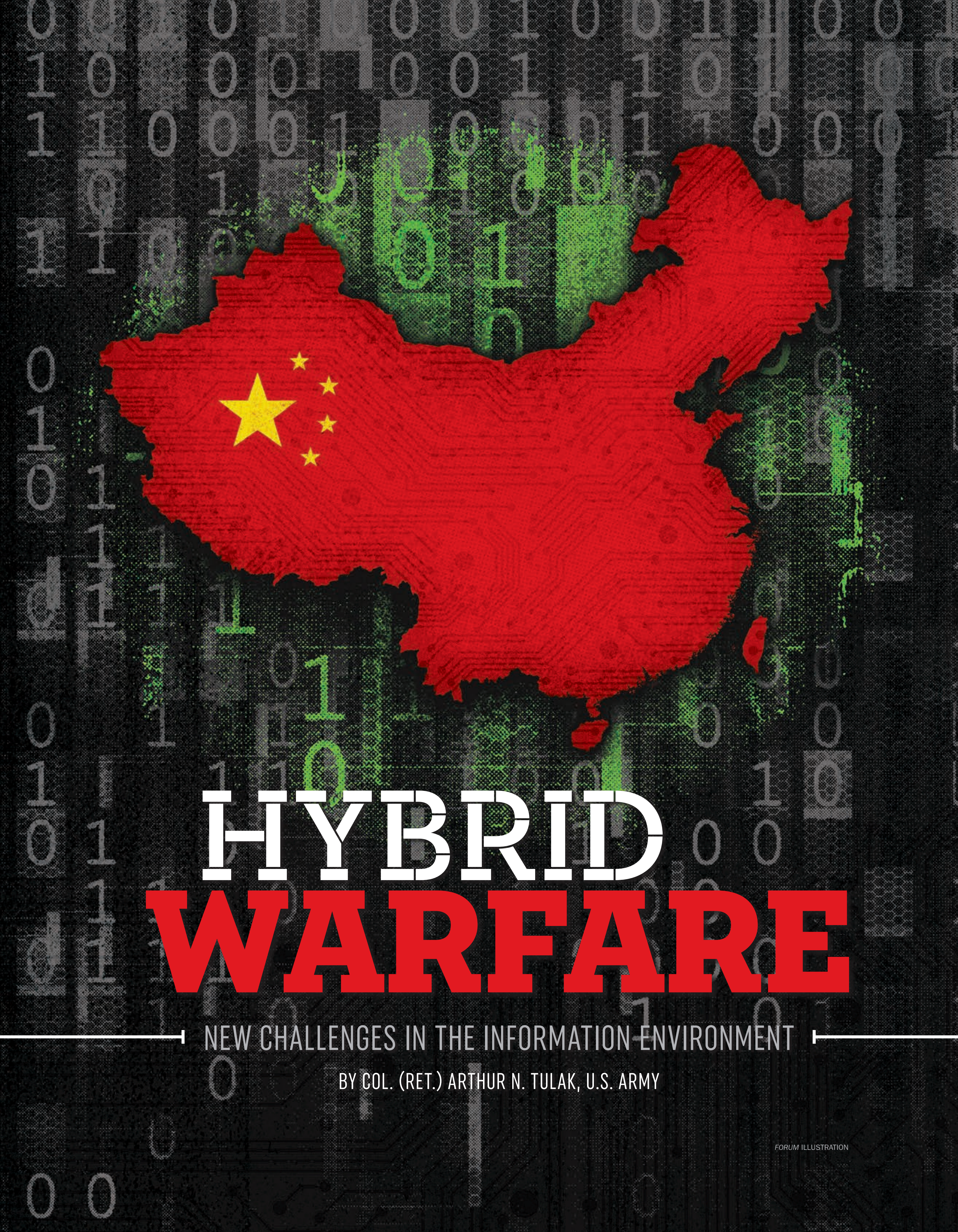
Cyber crime will almost certainly persist as a significant problem in the Indo-Asia-Pacific, where more than 1 billion people are on the Internet and where the World Wide Web is inextricably linked with global business, experts say.

"Asian societies have been enthusiastic adopters of the Internet," noted a study titled "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia," published by the Lowy Institute for International Policy, a nonpartisan think tank in Australia.

The study asserted that the level of cyber crime is only likely to rise in the region.

"Cyber criminals go where there is money," the report concluded. "As Asian countries become wealthier, fraud and extortion committed over the Internet will increase."

Governments and cyber security experts in the Indo-Asia-Pacific will need to increase transregional cooperation as well as development, regulation and enforcement of cyber laws to keep pace with these burgeoning criminal enterprises that increasingly operate online as nefarious predators of the digital realm. □



HYBRID WARFARE

NEW CHALLENGES IN THE INFORMATION ENVIRONMENT

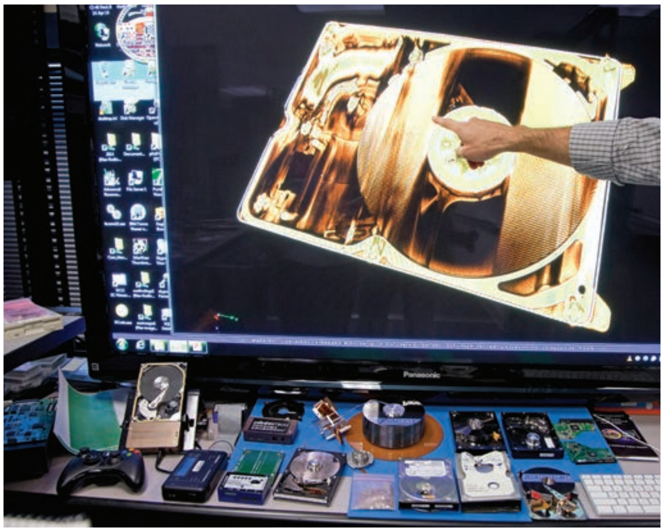
BY COL. (RET.) ARTHUR N. TULAK, U.S. ARMY

FORUM ILLUSTRATION

The nature of the military threat environment has changed as our adversaries and potential adversaries increasingly use nonmilitary and paramilitary means to achieve strategic and operational objectives that were previously considered a purely military task. The trend toward nonmilitary operations and capabilities substituting for military force, as well as a convergence of conventional and irregular approaches, has been acknowledged for many years by military scholars and writers. These tactics, carried out during peacetime competition, may generate lasting negative outcomes that directly affect security, economics and international law.

These trends have recently accelerated as great power states attempt to achieve military objectives short of open interstate conflict. The "blending" approach to modern warfare has been given many names, including "new generation warfare," "asymmetric warfare," "compound warfare," "hybrid warfare," and more recently has been described as actions conducted in the "gray zone" between classic diplomacy and open military conflict. Of these, the term hybrid warfare has gained the greatest currency as a way to understand current events. Among NATO circles, the term is used to describe the new operational attributes of the Russian offensive against Ukraine. Russia's use of military forces and equipment under the guise of indigenous, separatist forces in the Ukraine is the starkest example of hybrid warfare that includes the use of lethal force. China's version in the South China Sea has so far remained nonlethal, even as lethal means such as fighter aircraft, air defense missiles and artillery are being deployed on contested islands.

Hybrid warfare employs a combination of military and nonmilitary means in peacetime to achieve traditional military objectives (for example, territorial control or conquest), and thereby change the "facts on the ground" short of actual conflict. In his recently published work, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Michael Mazarr, a political scientist and former associate dean of the National War College, reveals that peacetime hybrid warfare accomplishes military objectives of battlespace control. He asserts that "the purpose of hybrid warfare is either to win a conclusive campaign through the use of force and some level of violence, or else to set the stage for some sort of decisive military action."



Cyber evidence is displayed at the Defense Computer Forensics Laboratory in Linthicum, Maryland. The United States spends U.S. $10 billion annually to protect sensitive government data. THE ASSOCIATED PRESS

Seizing ground via peacetime hybrid warfare can be seen as shaping the theater for future military operations by expanding military control over contested terrain or operational space to better employ offensive and defensive capabilities in the event of actual conflict. Both the Russian and Chinese versions of hybrid warfare use measures short of direct state-on-state military confrontation that would cross treaty red lines. The Russian version features “unorthodox and varied techniques” that combine a mixture of special forces, information campaigns, proxy forces and criminal activities, according to a 2015 *Jane’s Defence Weekly* report. A common feature of this new form of warfare is the precise strategic management of troops and operations, down to the tactical level, in order to achieve ambiguity about whether the forces and means employed are actually under national command authority, and to achieve the desired influence effects and strategic communication messaging across all media.

> “RUSSIA HAS ADOPTED THIS APPROACH, AND IT IS A MIX OF VERY WELL-KNOWN CONVENTIONAL WARFARE AND NEW, MORE SOPHISTICATED PROPAGANDA AND DISINFORMATION CAMPAIGNS.” — FORMER NATO SECRETARY-GENERAL ANDERS FOGH RASMUSSEN

The U.S. Army has acknowledged the challenges posed by hybrid warfare and examined the hybrid threat capabilities of China, Russia and Iran in *The U.S. Army Operating Concept: Win in a Complex World*, published in October 2014. In examining these potential threats, we find that traditional information operations, electronic warfare (EW) and cyber warfare are important components of hybrid warfare.

INFORMATION OPERATIONS IN HYBRID WARFARE: EUROPEAN THEATER

Classic hybrid warfare operations were demonstrated in the Crimean campaign in 2014, when Russian forces successfully employed psychological warfare, deception operations, skillful internal communications, intimidation, bribery and Internet/media propaganda “to undermine resistance, thus avoiding the use of firepower,” according to a 2014 analysis published by the National Defense Academy of Latvia. More recently, Russia’s military offensive in the eastern Ukraine prompted former NATO Secretary-General Anders Fogh Rasmussen to declare that “Russia has adopted this approach [hybrid warfare], and it is a mix of very well-known conventional warfare and new, more sophisticated propaganda and disinformation campaigns including Russian efforts to influence public opinion through financial links with political parties within NATO and engagement in NGOs [nongovernmental organizations],” *Newsweek* magazine reported in April 2015.

In both campaigns, Russia employed its own land forces wearing military camouflage uniforms (and often with face masks), but without insignia that would clearly identify them as Russian military. This had the effect of creating ambiguity, because the Russians claimed the well-equipped and well-trained soldiers were merely homegrown separatists. The press referred to these mysterious forces as “little green men” who appeared in numbers far too large and with capabilities far too sophisticated to fit the Kremlin’s description as locally formed separatist groups. Nevertheless, the strategy achieved ambiguity and plausible deniability long enough to change the facts on the ground. NATO officials estimated in March 2015 that 1,000 Russian military and intelligence personnel were deployed in the eastern Ukraine. These personnel likely operated or supervised the operation of sophisticated weapons systems, including tanks, artillery, air defense and command, control, and communications networks supporting separatist forces, as reported by *Jane’s Defence Weekly*.

Russia’s hybrid warfare, abundantly demonstrated in operations, is now part of Russia’s new military doctrine, which emphasizes information operations, disinformation campaigns, and exploiting the target populations’ “potential for protest,” as well as using special operations forces and proxies to remain below the threshold of conventional military operations, *Jane's Defence Weekly* reported.

U.S. Air Force Gen. Philip Breedlove, NATO's supreme commander in Europe, testified before the U.S. Senate Armed Services Committee that this doctrine is being put into practice. He described Russian influence efforts in Eastern Europe as a "dedicated, capable and very lively information campaign," according to the *Defense News* newspaper. Gen. Breedlove estimated that this information campaign was fueled by the equivalent of U.S. $350 million and was disseminated by print, Internet and television media "in a dedicated, capable way."

INFORMATION OPERATIONS IN HYBRID WARFARE: INDO-ASIA-PACIFIC THEATER

In step with the Russian military, China's People's Liberation Army (PLA) has integrated hybrid warfare principles into its military doctrine, which calls for "combining conventional and unconventional actions," according to the U.S. Army Training and Doctrine Command. An example of hybrid warfare in the Indo-Asia-Pacific is exhibited by China's use of nonmilitary and paramilitary forces, such as its Coast Guard and fisheries enforcement vessels, oil exploration ships, oil drilling platforms, and Chinese-registered commercial ships and fishing boats to exert influence and assert China's dubious territorial and maritime claims in the South China Sea. As reported by *Defense News*, China has demonstrated that it can surge large numbers of fishing ships into a "maritime militia." The tactic was employed effectively against Taiwan in the 1990s with swarms encircling Taiwan's outer islands during periods of political tension and more recently against the Philippines in the Scarborough Shoal stand-off and against Japan near the Senkaku Islands in 2012. According to *Defense News*, China uses swarms of fishing vessels to encircle a disputed area to bar access for a rival state's coast guard or navy without using overt military force.

In testimony before the U.S. House Armed Services Committee in April 2015, U.S. Navy Adm. Samuel J. Locklear III, then commander of U.S. Pacific Command, acknowledged with concern these various nonmilitary and paramilitary operations, as well as a corresponding increase in military operations in the South China Sea. He remarked that while China's reliance on the use of "maritime law enforcement vessels to enforce their claims has largely kept these issues out of the military sphere," they were also accompanied by "a steady increase in military air and sea patrols."

China's use of what is likely the world's largest seagoing fleet of dredgers to create a string of artificial islands atop submerged shoals and reefs in the South China Sea and West Philippine Sea is yet another example, *The Diplomat* magazine reported in February 2015. Adm. Harry B. Harris Jr., while in command of the U.S. Pacific Fleet, commented on the PLA's hybrid warfare techniques, saying that "China is creating a 'Great Wall of sand' with dredges and bulldozers over the course of months," *The Washington Post* newspaper reported in April 2014.

FROM LEFT: FBI Director James Comey, CIA Director John Brennan, Director of National Intelligence James Clapper, Director of the National Security Agency Adm. Michael Rogers, and Defense Intelligence Agency Director Lt. Gen. Vincent Stewart appear before the U.S. House Intelligence Committee hearing on cyber threats in Washington, D.C., in September 2015. THE ASSOCIATED PRESS

U.S. Military Academy cadet Kiefer Ragay participates in an annual cyber defense exercise at the Cyber Research Center at the U.S. Military Academy at West Point, New York, in April 2014.

THE ASSOCIATED PRESS

China has used its maritime militia on commercial and nonmilitary ships to harass U.S. Navy ships transiting the South China Sea, including the confrontation by Chinese fishing vessels harassing the USNS Impeccable in March 2009 and another by Chinese merchant vessels harassing the USS Lassen in October 2015. More recently, China used its naval militia personnel, disguised as fishermen, to conduct landings on Japan's Senkaku islands as reported in *Defense News* in March 2016. As noted in a series of articles by Dr. Andrew Erickson and Conor Kennedy of the China Maritime Studies Institute of the U.S. Naval War College, China's maritime militia is a subset of China's militia organization under PLA and state control. As reported in *Defense News* in November 2015, the use of these paramilitary forces, referred to as "little blue men," for their maritime militia uniforms, has been compared to Russia's "little green men," the mysterious military forces posing as local separatists in Crimea and eastern Ukraine. The intent of such hybrid warfare tactics is to achieve military objectives short of conflict, while confounding and delaying Western military decision-making.

Acts of hybrid warfare carried out in peacetime can result in long-term threats to regional security. In a speech at the Center for a New American Security, U.S. Deputy Secretary of State Antony Blinken compared China's large-scale land creation projects in the South China Sea to Russian seizures of Crimea and portions of eastern Ukraine, and called them "a threat to peace and stability." The establishment of military-capable operating bases in the South China Sea in disputed waters on artificially created islands, and the seizure of Crimea and portions of eastern Ukraine were hybrid warfare operations carried out below the threshold of military conflict, but these actions may in fact make such conventional military force-on-force conflict more likely in the future. Addressing this threat, Blinken issued a stern warning:

"In both eastern Ukraine and the South China Sea, we're witnessing efforts to unilaterally and coercively change the status quo — transgressions that the United States and our allies stand united against."

As China carries out hybrid warfare to accomplish territorial acquisition via nonmilitary and paramilitary means, it is following the Russian example in Ukraine by implementing a coordinated supporting “information campaign” that is planned at the strategic level and is transmitted globally. This information campaign conforms to the PLA’s “Three Warfares” doctrine with actions, activities and messaging to support psychological, media and legal warfare. The messages have promoted China’s “historical claims,” peaceful intentions, and the concept of “indisputable territorial sovereignty” of its artificial island bases. At a news conference in April 2015 (during the fever-pitch dredging operations overseen by the PLA Navy), the Chinese Ministry of Foreign Affairs offered nonmilitary justifications for occupation of the many contested reefs, shoals and islets, extolling the many supposed benefits to the international community that would result from Chinese administration and control. These messages were intended to create information “cover” to allow China to continue the march to complete the construction of the artificial islands.

A month later, Ouyang Yujing of the Chinese Ministry of Foreign Affairs asserted “that China has every right to deploy on relevant islands and reefs facilities necessary for military defense” as reported by *China Daily* newspaper. U.S. intelligence found that China made good on this claim, when it identified heavy artillery vehicles on an artificial island built atop Fiery Cross Reef, The Associated Press reported in May 2015.

The recent deployment of PLA J-11BH/BS jet fighters (as reported on Chinese language websites) to Woody Island in the Paracels serves to highlight the likely purpose of the airstrips being constructed on the artificial islands, such as the 3,000-meter airstrip constructed on top of Fiery Cross Reef. Finally, the deployment of HQ-9 air defense missiles to Woody Island in February 2016 proves that the ultimate objective of hybrid warfare is to achieve military conquest short of open military conflict. In short, China employs its “Three Warfares” doctrine to carry out hybrid warfare offensive actions against adversaries whose militaries are on a peacetime footing.

“POTENTIAL ADVERSARIES HAVE INVESTED SIGNIFICANTLY IN CYBER AS IT PROVIDES THEM WITH A VIABLE, PLAUSIBLY DENIABLE CAPABILITY TO TARGET THE U.S. HOMELAND AND DAMAGE U.S. INTERESTS.” — U.S. DEPARTMENT OF DEFENSE CYBER STRATEGY

ELECTRONIC WARFARE, CYBER THREAT ENVIRONMENT AND HYBRID WARFARE

Another aspect of hybrid warfare as practiced by the Russians and Chinese is the important role assigned to their military cyber and EW units, which bring another set of new challenges as these capabilities are applied to hybrid warfare.

As Deputy Defense Secretary Robert Work has observed, “our competitors are trying to win in the EW competition,” *Defense News* reported. The Russian Army’s use of EW as a component of hybrid warfare during its offensive operations in the Ukraine was evidence of this. It employed advanced Russian military EW systems such as high-power microwave systems to jam Ukrainian military communication and reconnaissance and to disable unmanned aerial vehicle surveillance operated by the Organization for Security and Co-operation in Europe cease-fire monitoring teams, *Jane’s Defence Weekly* reported.

The PLA also takes EW very seriously, as evidenced by military writings that stress “obtaining electromagnetic dominance is a precondition to winning modern war,” according to China Radio. In a report published by the U.S.-China Economic and Security Review Commission in February 2015, analysts assessed that “the PLA sees space, cyber, and EW capabilities as increasingly vital aspects of its ability to deter or, if necessary, defeat a technologically advanced adversary in a future informatized local war, whether over Taiwan or the Senkaku/Diaoyu Islands, maritime territorial disputes in the South China Sea, or elsewhere.”

On the cyber front, as is the case with EW, our competitors and potential adversaries are increasingly investing in these capabilities and putting them to use in peacetime hybrid warfare.

In his 2015 testimony to the U.S. House Armed Services Committee, Adm. Locklear expressed concern about the “risk posed by persistent cyber threats” as well as “increased cyber capacity and use, especially by China, North Korea, and Russia.” He specifically

mentioned North Korea's cyber attack on Sony Pictures as an example of the country's cyber capabilities being applied against the military and civilian networks of our ally, South Korea. These threats represent the most capable top two tiers in the five-tier threat matrix developed by the U.S. Defense Science Board Task Force focused on understanding the advanced cyber threat facing the nation.

China's cyber capabilities continue to grow, mature and expand. The PLA established its first information warfare units in 2003. They were tasked "to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly systems and networks," according to a 2007 edition of *Security Bulletin*. The PLA began incorporating offensive computer network operations into its exercises in 2005 to build its proficiency. After years of official denials,the PLA acknowledged the existence of dedicated cyber warfare units in the 2013 edition of *The Science of Military Strategy*, published by the PLA's Academy of Military Sciences, as reported in *The Diplomat*. This acknowledgment followed a well-known 2013 report published by the commercial computer security firm Mandiant, which identified Unit 61398 of the Second Bureau of the PLA General Staff Department's Third Department as the source of many computer network intrusions emanating from China.

Of importance to hybrid warfare was the acknowledgment that many of China's cyber capabilities and cyber warriors are outside the military, such as patriotic hackers and university students. The Science of Campaigns therefore calls for a mobilization of these assets for cyber war. Putting these capabilities under military control in peacetime would be a "Peoples War" in cyberspace and would provide plausible deniability for cyber attacks that would likely accompany hybrid warfare. As explained by Franz-Stefan Gady, writing in *The Diplomat* in March 2015, "This approach may, perhaps more effectively than in Western countries, put civilian and nonstate actor capabilities in the hands of senior military decision-makers who can more effectively channel and direct these resources for a variety of operations in cyberspace." The U.S. Department of Defense Cyber Strategy published in April 2015 addressed external threats directly: "Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests. Russia and China have developed advanced cyber capabilities and strategies." The plausible deniability of cyber attacks has made them a viable and favored component of hybrid warfare.

China now fully considers cyber as a component of military operations, as revealed in its 2015 Defense White Paper, which stated that "China will expedite the development of a cyberforce," *Stars and Stripes* newspaper reported in May 2015. More recently, in October 2015, Bloomberg News carried the PLA's announcement that it was consolidating the nation's various cyber warfare capabilities and units into a single military command reporting to the Central Military Commission. The PLA's actions in establishing a cyber command come more than a year after the Russian military's February 2014 announcement of its own cyber command. Russian Maj. Gen. Yuri Kuznetso said the goal of having it fully operational by 2017 was "to defend Russian armed forces' critical infrastructure from computer attacks," the website Tripwire.com reported.

Cyber warfare was a major characteristic of the Russian invasion of the Republic of Georgia in 2008, and such tactics were again employed in the invasion of Crimea in 2014. During the Russian invasion and annexation of Crimea, Ukraine suffered "sophisticated and coordinated cyber attacks which crippled communications networks and overwhelmed government websites," as reported by the United Kingdom's *Channel 4 News* in May 2014. Most recently, hackers based in Russia carried out sophisticated attacks on Ukraine's power grid in December 2015, knocking out power to tens of thousands of customers in central and western Ukraine. Ukraine's SBU state security service blamed Russian security services for the malware used to attack, as reported by Reuters. Later, a U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team investigation confirmed that this was a cyber attack, which cyber security experts have linked to to the Russian Black Energy hacking group, as reported by Reuters in February 2016.

Cyber attacks are increasing across the globe, and most alarmingly so in the Indo-Asia-Pacific. In February 2015, *Jane's Defence Weekly* reported statistics showing that during 2013-14, the percentage of the world's cyber attacks emanating from the Indo-Asia-Pacific region ranged from 64 percent to 70 percent, with a foreboding assessment that "the scope of the cyber threat … [and] the threat of cyberattack remains at an alarmingly high level."

In response, governments across the Indo-Asia-Pacific region are "pushing forward to enhance cyber security, with defense and military agencies taking center stage" with investments

U.S. Secretary of State John Kerry speaks about cyber security and Internet freedom at Korea University in Seoul in May 2015.

AFP/GETTY IMAGES

from U.S. Pacific allies and security partners valued at U.S. $17 billion in 2014, according to *Jane's Defence Weekly*. The possibility of cyber attacks, a key component of hybrid warfare, leading to open armed conflict is now a serious concern. NATO Secretary-General Jens Stoltenberg, speaking at a key alliance planning summit in March 2015, said: "NATO has made clear that cyber attacks can potentially trigger an Article 5 [collective security, military] response," *Defense News* reported in March 2015.

MOVING FORWARD

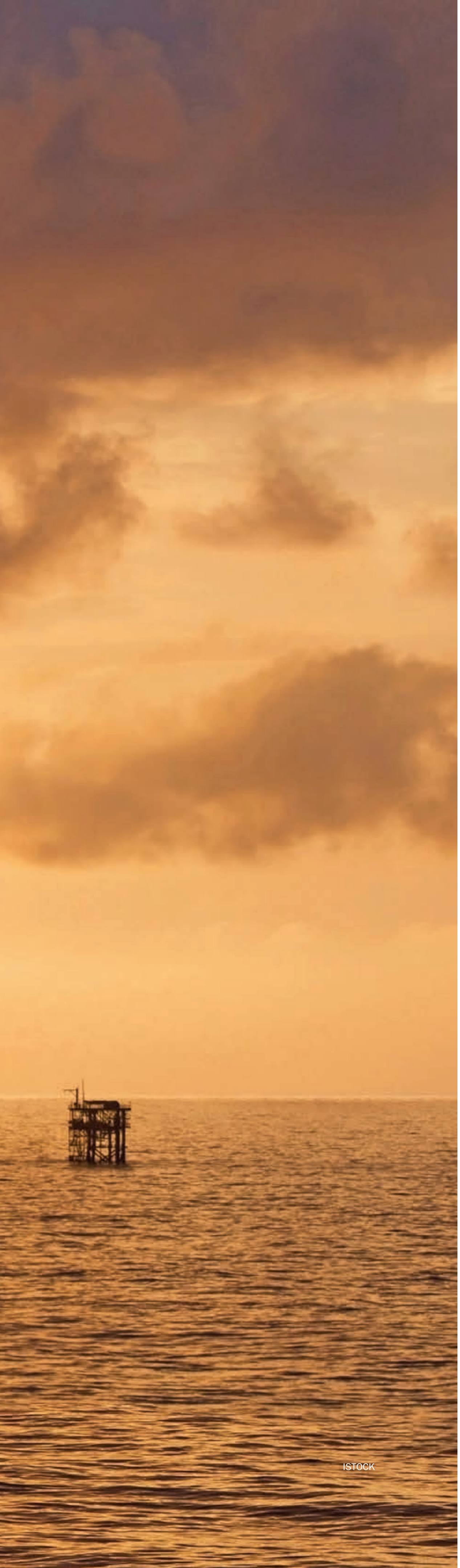
Hybrid warfare is taking place during "peacetime" with dramatic results reflected in redrawn boundaries in Europe and new artificial islands created inside "dashed lines" drawn on maps in the Pacific. As the Russian and Chinese examples show, information operations are a key component to conducting warfare against an adversary on a peacetime footing, without triggering a shooting war. Competitors and potential adversaries have adapted traditional information operations to suit hybrid warfare, designed to delay and confound military and government decision-making and responses, creating new challenges to the U.S. and our military allies and security partners. Likewise, EW and cyber have been proven as viable components of hybrid warfare that can achieve disruption and destruction of command and control, communications, and infrastructure. EW and cyber are firmly established as a priority area for development by China and Russia, which are aggressively pursuing and fielding new capabilities and establishing new units and commands to employ them. Hybrid warfare is founded on successful operations in the information environment, which provide the necessary camouflage, concealment and cover for what are essentially military operations to achieve objectives and effects in the physical environment. Meeting this threat will require more agile military organizations, capabilities and specialized military personnel in order to prevent information operations, EW and cyber actions in peacetime hybrid warfare from sparking military conflict. □

SOUTH CHINA SEA

STRATEGIES

Determining China's next move in the region

DR. ALEXANDER L. VUVING


ISTOCK

Since 2014, the Spratly Islands have remained a large and unique construction site. Workers aboard dozens of Chinese vessels have been cutting coral and dredging sand to turn previously submerged reefs into artificial islands. In less than a year, they created more than 10 square kilometers of new land on seven sites across an archipelago whose total land area had originally been approximately 4 square kilometers. Fiery Cross Reef, which was submerged at high tide when occupied by China in 1988, now boasts a land mass of 2.74 square kilometers and is large enough to host a 3,100-meter-long airstrip and a 63-hectare harbor. Nearly six times larger than Itu Aba, the largest natural island in the Spratly group, Fiery Cross Reef is still smaller than two other artificial islands. By June 2015, China had created 4 square kilometers and 5.6 square kilometers at Subi Reef and Mischief Reef, respectively, and these numbers were still growing at publication time, according to the Asia Maritime Transparency Initiative website http://amti.csis.org/island-tracker.

What is the endgame of this island building? The roles of China's man-made islands in wartime and in maritime law seem extremely doubtful. Too small and isolated to sustain major attacks, these assets can easily become liabilities in times of war. Being completely artificial, they are not entitled to a 12-nautical-mile territorial sea or 200-nautical-mile exclusive economic zone. Why is China investing a huge amount of resources to create these artificial islands?

The conventional perspectives that focus on military and legal implications of these activities are ill-suited to answer the questions. China is pursuing a strategy that is based upon principles very different from the conventional thinking, as outlined in the author's comments in a March 2015 article on the IR.Asia website. The philosophy behind this strategy can be found in Sun Tzu's *Art of War*. The key idea is "winning without fighting." The overall objective is to gain control of the South China Sea, but the main way to achieve this is not through large battles. Rather, China wants to achieve its objective through activities that create new facts on the ground (and the water), set up the playing field and psychologically change the strategic calculus of other nations. The underlying logic of this strategy is to shift the propensity of things in favor of Chinese dominance by maneuvering the strategic configurations of the region.

Three imperatives are required to pursue this strategy of opportunistic and gray-zone expansion, and Beijing's sixdecadelong involvement in the South China Sea has neatly followed these requirements. (Author Alexander L. Vuving first published this theory in December 2014 in "China's Grand-Strategy Challenge: Creating Its Own Islands in the South China Sea," in *The National Interest* magazine. The article correctly predicted China's building programs at Subi Reef and Mischief Reef.)

Three Imperatives

The first imperative is to avoid large battles as much as possible; clashes can be initiated, but only to exploit an existing favorable situation. This imperative served as the mainstay of China's approach when it seized the Paracel Islands from South Vietnam in 1974 and when it clashed with Vietnam in the Spratly Islands in 1988.

The second imperative is to control the most strategic positions in the area; if not already in possession, these positions must be seized stealthily if possible and in a limited conflict if necessary. This imperative was most visible when China took control of the seven reefs it now occupies in the Spratly Islands and of Scarborough Shoal in 2012.

The third imperative is to develop these positions into strong points of control, robust hubs of logistics and effective bases of power projection. This is precisely what China is now doing in the South China Sea.

These activities are to serve the dual goal of establishing Chinese supremacy and sovereignty in this domain. Due to their strategic locations and their logistic support, the islands in China's hands will be robust platforms from which a myriad of fishing boats, law enforcement vessels, warships and aircraft, manned or unmanned, can dominate the waters and the skies of the South China Sea.

The key points of control include Woody Island in the Paracel Islands; Fiery Cross Reef, Subi Reef and Mischief Reef in the Spratly Islands; and Scarborough Shoal in the northeastern part of the South China Sea. Woody Island, Fiery Cross Reef, Mischief Reef and Scarborough Shoal form a four-point constellation from which, with a radius of only 250 nautical miles, the entire main body of the South China Sea can be kept under intense watch. Within the Spratly group, Subi Reef, Mischief Reef and Fiery Cross Reef make a perfect triangle to cover the archipelago.

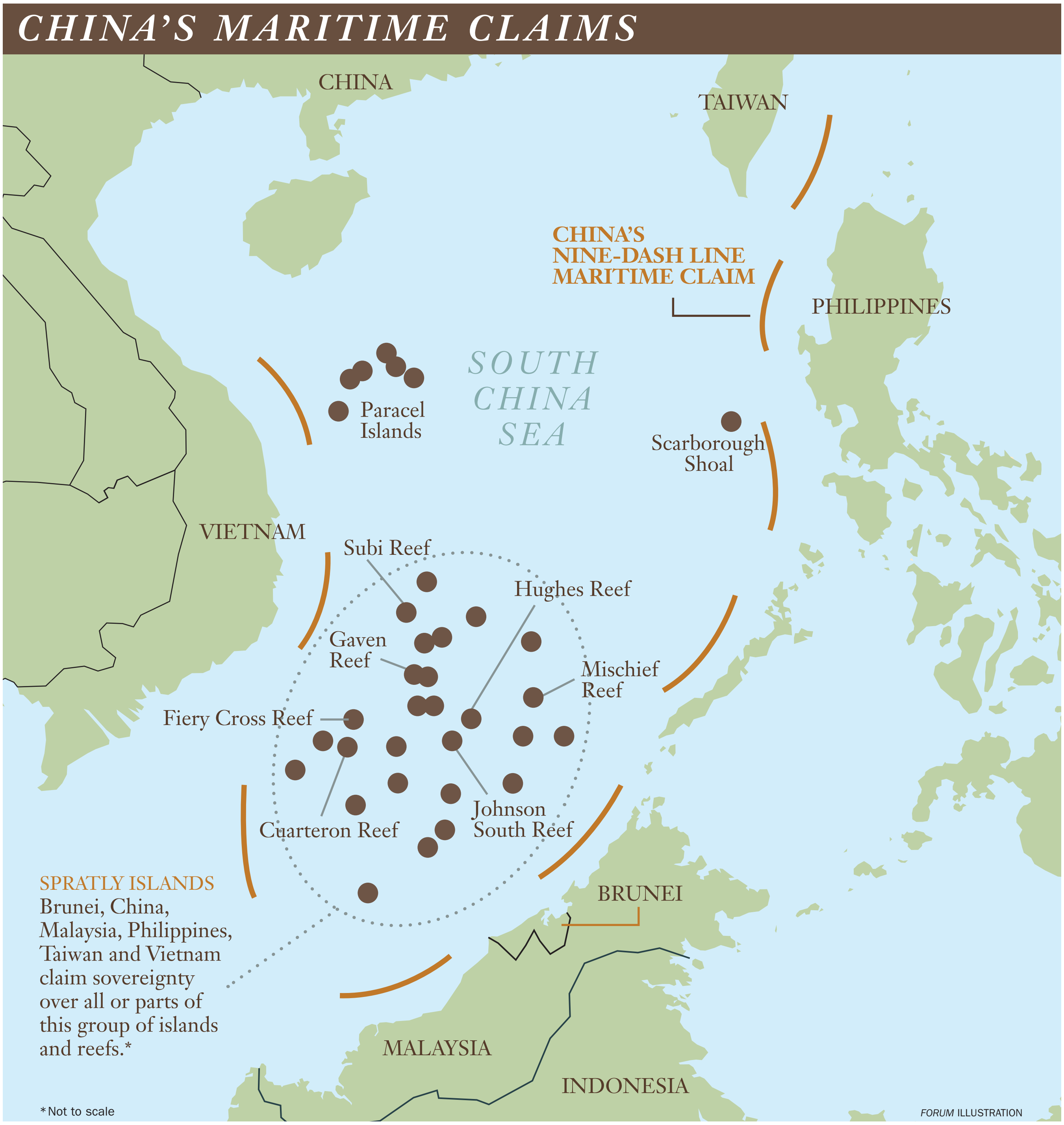
On Woody Island, China has recently installed anti-aircraft missiles and upgraded a 3,000-meter-long airstrip and a 1,000-meter deep-water port. The airfield is capable of handling eight or more fourth-generation aircraft such as Su-30MKK fighters and JH-7 bombers, while the harbor can accommodate vessels of 5,000 tons or more. An airstrip and a harbor of similar sizes are under construction at Fiery Cross Reef. The land creation at Subi Reef and Mischief Reef suggests that each of the two artificial islands will also have an airstrip and a harbor of these sizes. Although Beijing had not started large-scale construction at Scarborough Shoal as of early spring 2016, it would not be surprising if it will also build an airstrip and a deep-water port at this site in the future.

The expanded areas gained through land creation will enable China to install significant military and dual-use facilities on its outposts. The four smaller Chinese outposts in the Spratly Islands now are about the size of the largest Vietnamese outpost there. Spratly Island, the largest feature occupied by Vietnam in the archipelago, covers 15 hectares. The four Chinese outposts, Cuarteron Reef, Johnson South Reef, Gaven Reef and Hughes Reef, now measure 23.1 hectares, 10.9 hectares, 13.6 hectares and 7.6 hectares, respectively.

Chinese dredging vessels are seen in the waters around Mischief Reef in the disputed Spratly Islands in the South China Sea in this image taken by a P-8A Poseidon surveillance aircraft.

REUTERS

CHINA'S MARITIME CLAIMS



SPRATLY ISLANDS
Brunei, China, Malaysia, Philippines, Taiwan and Vietnam claim sovereignty over all or parts of this group of islands and reefs.*

*Not to scale

FORUM ILLUSTRATION

China will put radar stations, power and water plants of various sizes, and other storage and service infrastructure on the islands it occupies. Its facilities in the Paracel and Spratly islands will be capable of supporting thousands of fishing boats and hundreds of patrol vessels, warships and aircraft to operate in the waters and skies located hundreds of kilometers from the Chinese coasts. China will also populate these islands with thousands of civilians and military personnel. With several enlarged islands in the Paracels and seven artificial islands in the Spratlys as staging and resupply bases, China can deploy tens of thousands of fishing boats and hundreds of law enforcement vessels to push the Vietnamese, Filipinos, Malaysians and Indonesians out of the waters Beijing considers its own.

De Facto Control

China may not attack the features already occupied by other claimants, but it will increase efforts to surreptitiously take control of some strategically located but unoccupied features. Eldad Reef and Whitsun Reef in the central groups, as well as several features in the eastern part of the Spratly Islands closer to the Philippines, continue to be the targets of these efforts.

China may not formally declare an air defense identification zone in the South China Sea since such

REUTERS

Members of China's People's Liberation Army Navy patrol in the Spratly Islands in February 2016.

an act may trigger a major crisis and turn many of the Southeast Asian nations against China. But Beijing will impose several air defense zones in the areas surrounding the Paracel and Spratly islands. It will also quietly assert that the sky within the U-shaped line belongs to it.

With substantially more facilities in the Paracel and Spratly islands, China will occasionally declare several security, fishing and environmental zones in the South China Sea. Although these maritime zones may not be in accordance with international law, China will refuse to go to the court, and as the most powerful actor in the region, Beijing can enforce whatever it regards as lawful.

Can China achieve air and naval superiority in the South China Sea? As previously mentioned, the airfields and harbors in the Paracel and Spratly islands are too isolated and too exposed to sustain major attacks in wartime. China's only aircraft carrier, the Liaoning, is no match for even a single aircraft carrier of the U.S. Pacific Fleet. While the Liaoning will be equipped with 30 J-15 multirole fighters and multiple antisubmarine warfare helicopters, a Nimitz-class U.S. carrier has twice that capacity.

Beijing's goal appears to be air and sea superiority in times when the United States is not militarily involved. Vietnam's ability to attack Chinese outposts in the South China Sea is heavily limited by the possibility of China's retaliation along the countries' 1,450-kilometer land border. Four airfields at the Paracel and Spratly islands will be able to add 30 to 40 more to the number of fourth-generation aircraft that China can operate at the same time in the South China Sea. This will enable China to gain air superiority over Vietnam and Malaysia, the largest air forces among its Southeast Asian rivals. Vietnam enjoys a long coastline on the South China Sea but has only 35 fourth-generation aircraft for the entire country. Malaysia lies far to the south and has no more than 44 fourth-generation aircraft for the entire country.

In addition to aircraft and warships, China may also deploy more missiles to the sites it occupies in the Paracel and Spratly islands. The deployment of more missiles will likely trigger vehement protests by Vietnam, the Philippines, the United States and some other governments, but China will justify its deployment as an act of self-defense. China's military assets there will be highly vulnerable in wartime, but their main functions appear to be peacetime patrolling and psychological intimidation.

AFP/GETTY IMAGES

At a news briefing in Manila in April 2015, Philippine military chief Gen. Gregorio Pio Catapang points to aerial photos of Chinese construction on reefs and shoals in the Spratly archipelago.

A Coercive Blend

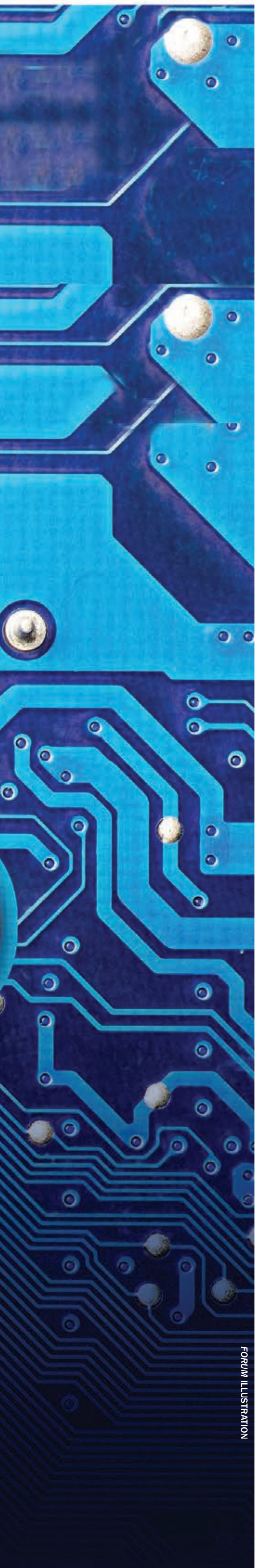
China's approach mixes coercive elements with cooperative ones, using the latter to lure and trap others in the former. China may offer its facilities on the artificial islands as a global public good. In May 2015, Adm. Wu Shengli, commander of the Chinese Navy, told Adm. Jonathan Greenert, chief of U.S. naval operations, that the facilities on China's artificial islands might be used for joint rescue and disaster-relief operations. Although the United States did not buy China's pitch, China will certainly use its disputed assets as staging bases for high-profile humanitarian or cooperative operations that involve other states in the region. For countries with no territorial or maritime disputes with Beijing in the South China Sea, this will be another incentive for acquiescence in Chinese domination.

It is unlikely that China will disrupt the commercial air and sea traffic in the region, but it will be no surprise if China occasionally tries to intercept some vessels and aircraft, military or civilian, of countries that oppose its bid for regional hegemony. The main effects of such acts are designed to be psychological rather than physical.

China's activities in the South China Sea fit into a larger and long-term strategy whose central tenet is to gain control of this strategically pivotal location in ways that would prevent others from responding in kind. This strategy in turn is part of a larger effort to realize the China Dream, to restore what China perceives as its rightful place at the top of a hierarchy of nations. The fate of belligerent rising powers in the past and the vulnerability of China's trading routes suggest that war is not the way for China to achieve this ambition. Equipped with a strategic tradition that favors indirect approaches, China has opted for a strategy of opportunistic and gray-zone expansion that tries to shape the playing field rather than directly attack the enemy. Intimidation is a major element of this strategy, but it is to result from an overwhelming configuration or selective overpunishment rather than indiscriminate assaults.

If China's rivals are unable to counter this strategy, China will emerge, at least in the perception of most regional countries, as the overlord of the South China Sea. Given the fact that the lifeline of Asia's economy runs through the South China Sea, and the fact that the center of world economic gravitation has shifted to Asia, preserving free access for all to the South China Sea is increasingly important. □

MASTER MANIPULATORS


FORUM ILLUSTRATION

NATIONS USE INFORMATION CONTROL TO LIMIT OUTSIDE INFLUENCE AND OFTEN PORTRAY A DISTORTED IMAGE OF WHAT'S HAPPENING WITHIN THEIR BORDERS

FORUM STAFF

Countries have long recognized that their most porous border isn't the one shared with a feuding neighbor but a virtual one.

Cyberspace has allowed friends and enemies to be as close as the click of a mouse. Yet agreeing upon international cyber standards to protect the valuable content and sites and police the harmful ones remains a challenge among nations. This lack of internationally enforceable rules creates spaces for nefarious groups to operate and leaves countries to make individual decisions on how to regulate this virtual space. Such diverse policies have led to tensions in the Indo-Asia-Pacific and elsewhere, with unlawful actors taking advantage of the gaps in standards to hack government and private networks.

Nations such as China, Russia and North Korea have a history of self-imposed restrictions regarding their virtual borders. As recently as December 2015, China had no interest in any plans that would change the status quo.

"We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation, and participate in international cyberspace governance on an equal footing," Chinese President Xi Jinping said during China's second-annual World Internet Conference. "No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security."

China blocks foreign social media sites including Facebook and Twitter. "The Chinese government has long kept tight reins on both traditional and new media to avoid potential subversion of its authority," according to an April 2015 report titled "Media Censorship in China" by the Council on Foreign Relations. "Its tactics often entail strict media controls using monitoring systems and firewalls, shuttering publications or websites, and jailing dissident journalists, bloggers and activists."

Critics say a recently enacted anti-terrorism law in China allows authorities greater reach to censor and gives the state access to sensitive commercial data. The law requires companies to provide technical information and decrypt documents when police request it as part of an investigation to prevent a terrorist attack, according to a December 2015 *New York Times* newspaper report.

"While the Chinese authorities do have a legitimate duty in safeguarding their citizens from violent attacks, passing this law will have some negative repercussions for human rights," William Nee, a Hong Kong-based researcher on China for Amnesty International, told *The New York Times*. "Essentially, this law could give the authorities even more tools in censoring unwelcome information and crafting their own narrative in how the 'war on terror' is being waged."

Zhang Xuezhong, a lawyer and former professor at East China University of Political Science and Law, called the law "more an ideological declaration" that will lead to more censorship.

"A good security law should state who on what conditions gets what punishment, but this law doesn't," Zhang told the BBC in July 2015, when the law was still in draft form and was being debated. "Technically speaking, the law is awful, as it is difficult to enforce it on individuals and companies."

China has proposed that the United Nations adopt an Internet code of conduct, with a Chinese official pledging that China "will continue to commit itself to establishing a peaceful, secure, open and cooperative cyberspace."

Backing China in its quest for what it sees as the future of Internet conduct is Russia. The two countries agreed in May 2015 not to spy on each other.

"No country can call itself the only country that has the right to govern cyberspace, so we call on the international community to play a more important role in cyberspace governance," Russian Prime Minister Dmitry Medvedev said in a speech, echoing Xi's remarks during the Internet conference, according to *The Wall Street Journal* newspaper.

MEDIA RESTRICTIONS

For countries with strict controls on information, restrictions aren't only placed on what comes into the country, but also on what gets out. Worldwide, several countries limit what independent journalists can produce inside their borders. Those found breaking the rules routinely face imprisonment, with China imprisoning more journalists than any other country in the world, according to the Committee to Protect Journalists (CPJ), a New York City-based nonprofit organization that promotes freedom of the press worldwide.

Annually, the CPJ ranks the 10 most censored countries, taking into account media laws, punishments for journalists and Internet restrictions. Four Indo-Asia-Pacific countries made CPJ's 2015 list, with North Korea ranked No. 2, Vietnam ranked No. 6, China ranked No. 8 and Burma ranked No. 9.

"In North Korea, 9.7 percent of the population has cell phones, a number that excludes access to phones smuggled in from China. In place of the global Internet, to which only a select few powerful individuals have access, some schools and other institutions have access

INFORMATION CONTROL

The Committee to Protect Journalists, a New York City-based nonprofit that promotes freedom of the press worldwide, compiles an annual list of the 10 most censored countries. Countries are rated on the basis of a series of benchmarks, including the absence of privately owned or independent media, blocking of websites, restrictions on electronic recording and dissemination, license requirements to conduct journalism, restrictions on journalists' movements, monitoring of journalists by authorities, jamming of foreign broadcasts and blocking of foreign correspondents.

Four Indo-Asia-Pacific countries made the 2015 list. The full ranking included:

1. Eritrea
2. North Korea
3. Saudi Arabia
4. Ethiopia
5. Azerbaijan
6. Vietnam
7. Iran
8. China
9. Burma
10. Cuba

Below are more details from the report on the four Indo-Asia-Pacific rankings.

NORTH KOREA

Leadership: Kim Jong Un

How censorship works: Article 53 of the country's constitution calls for freedom of the press, but even with an Associated Press (AP) bureau — staffed by North Koreans and located in the Pyongyang headquarters of the state-run Korean Central News Agency — and a small foreign press corps from politically sympathetic countries, access to independent news sources is extremely limited. Nearly all the content of North Korea's 12 main newspapers, 20 periodicals, and broadcasts comes from the official Korean Central News Agency, which focuses on the political leadership's statements and activities. Internet is restricted to the political elite, but some schools and state institutions have access to a tightly controlled intranet called Kwangmyong, according to the AP.

VIETNAM

Leadership: Prime Minister Nguyen Tan Dung

How censorship works: Vietnam's Communist Party-run government allows no privately held print or broadcast outlets. Under the 1999 Media Law (Article 1, Chapter 1), all media working in Vietnam must serve as "the mouthpiece of Party organizations." The Central Propaganda Department holds mandatory weekly meetings with local newspaper, radio and TV editors to hand down directives on which topics should be emphasized or censored in their news coverage. Forbidden topics include the activities of political dissidents and activists; factional divisions inside the Communist Party; human rights issues; and any mention of ethnic differences between the country's once-divided northern and southern regions. Independent bloggers who report on sensitive issues have faced persecution through street-level attacks, arbitrary arrests, surveillance and harsh prison sentences for anti-state charges.

CHINA

Leadership: President Xi Jinping

How censorship works: For more than a decade, China has been among the top three jailers of journalists in the world — a distinction that it is unlikely to lose any time soon. Document 9, a secret white paper dated April 22, 2014, which was widely leaked online and to the international press, included the directive to "combat seven political perils" and reject the concept of "universal values" and the promotion of "the West's view of media." Document 9 made it clear that the role of the media is to support the party's unilateral rule. The paper reasserted the necessity for China's technological and human censors to be ever more vigilant when keeping watch over the country's 642 million Internet users — about 22 percent of the world's online population.

BURMA

Leadership: President Thein Sein

How censorship works: Despite an end to more than four decades of prepublication censorship in 2012, Burma's media remains tightly controlled. The Printers and Publishers Registration Law — enacted in March 2014 — bans news that could be considered insulting to religion, disturbing to the rule of law or harmful to ethnic unity. Publications must be registered under the law, and those found in violation of its vague provisions risk de-registration. National security-related laws, including the colonial-era 1923 Official Secrets Act, are used to threaten and imprison journalists who report on sensitive military matters.

SOURCE: Committee to Protect Journalists

In this photo illustration, a man in a Shanghai office building holds an iPad with a Facebook application. China has banned foreign social media sites and applications, including Facebook and Twitter.
REUTERS

to a tightly controlled intranet," the CPJ report said. "And despite the arrival of an Associated Press bureau in Pyongyang in 2012, the state has such a tight grip on the news agenda that newsreel was re-edited to remove Kim Jong Un's disgraced uncle from the archives after his execution."

North Koreans wanting outside information seek it through the porous border with China, where they can obtain smuggled foreign DVDs.

"To keep their grip on power, repressive regimes use a combination of media monopoly, harassment, spying, threats of journalist imprisonment and restriction of journalists' entry into or movements within their countries," the CPJ report said.

CREATING THE STORY

Russia recently ramped up its state media machine, increasing the budget for its RT (formerly known as Russia Today) international news channel, according to a September 2015 report by the BBC. It has relied heavily on RT to win the hearts and minds of viewers for years.

"In general, the Russian media portrays anything going on from the point of view of [Russian President] Vladimir Putin," Nataliya Rostova, a visiting scholar at the University of Berkeley's Graduate School of Journalism and a senior correspondent at Moscow-based online magazine Slon.ru, told The WorldPost news website in October 2015. "He has unlimited access to the media, and they explain everything that's going on according to his official statement. It doesn't really matter if it's a war in Syria or any other topic."

She explained that when Putin took power in 2000, he assumed control over Russia's three main television stations and later brought two more under his purview.

"When it comes to so-called independent media, which are smaller and not owned by the state, there's often an agreement between the Kremlin, the owner and the editor-in-chief. Even Aleksey Venediktov, the editor-in-chief of Echo Moskvy, which is sometimes called the last remaining independent radio station in Russia but in reality isn't independent, says publicly that Putin is the only person who can fire him," Rostova told The WorldPost.

Whatever Putin's information control tactics are, they appear to be working, and his country's responses to at least one survey seem to be in line with his strategy.

Forty-nine percent of Russians believe information online should be subject to censorship, according to a report published in February 2015 titled "Benchmarking Public Demand: Russia's Appetite for Internet Control." Forty-two percent of Russians believe foreign countries are using the Internet against Russia and its interests, and 58 percent said they wouldn't mind if, during a national threat, Russia temporarily shut down the Internet completely. □

NAVIGATING *Social Media*

ISTOCK

DEFENSE LEADERS STRIVE TO TRAIN TROOPS ON RESPONSIBLE USE OF ONLINE APPS

FORUM STAFF

The mobile messaging app WeChat is hugely popular in China. At first, it seemed harmless when the wives of officers in a People's Liberation Army (PLA) brigade formed a chat group on the app to discuss how to best take care of their husbands.

The wives, however, sometimes chatted about sensitive topics such as the brigade's drill operations and schedules, the *People's Liberation Army Daily*, the Chinese Armed Forces' official newspaper, reported in April 2015.

Strangers were discovered probing for information about the brigade through the chat group, prompting the unit's commanders to set up lectures about military confidentiality for family members, the Hong Kong-based *South China Morning Post* newspaper quoted the *PLA Daily* as saying.

Social media use has experienced unprecedented growth in the Indo-Asia-Pacific, where more than a billion people use the Internet. At least three in five consumers in the region interact with social media via their mobile phones — more than in any other region in the world, according to online researcher Nielsen.

Increasingly, people are plugged into social media as part of the fabric of their lives. Hundreds of thousands of them are military troops — Soldiers, Sailors, Airmen, Marines.

Military officials throughout the Indo-Asia-Pacific and worldwide grapple with how to train Soldiers, personnel and families on the responsible use of social media to avoid the inadvertent disclosure of sensitive information. Some militaries embrace these tools to enhance internal communications and morale, while others take a more cautious approach to adapting to social media applications. Still others, including the PLA, forbid their use altogether.

"We depend on social media, but it can be extremely dangerous if you are not careful," warns the 2015 edition of the *U.S. Army Social Media Handbook*. Published annually since 2010, the handbook's precautions translate to many other nations' militaries.

"Since social media use is so commonplace in our day-to-day interactions, it is easy to become complacent," the handbook cautions. "Sharing seemingly trivial information online can be dangerous to loved ones and fellow Soldiers — and may even get them killed. … Enemies scour blogs, forums, chat rooms and personal websites to piece together information."

To avoid the potential pitfalls of social media, Indo-Asia-Pacific militaries are working to establish best practices:

Philippines: In July 2014, the nation's Armed Forces held their first social media summit to issue ground rules for troops, after the release of the *Philippine Army Social Media Handbook*, according to Rappler, a news website based in the Philippines.

Many of the handbook's precautions echo those of other militaries: *Do not post field assignments of personnel. Be careful in accepting friend requests on social media. Only post pre-approved content for public view. Do not reprimand subordinates on social media*.

"Social media is a reality," Philippine Gen. Emmanuel Bautista told reporters, according to Rappler. "We need a balance between transparency and the use of social media with the requisites of holding the confidentiality of information that will compromise the performance of our mission."

India: In December 2015, the Indian Army issued a 10-point list of "do's and don'ts" regarding social media for troops and their families, reported the India TV News website. It included admonishments such as: *Do not post photos with anything related to bases and weapons. Do not accept friend requests from strangers. Do not reveal your rank, battalion or place of posting*.

The Indian Army took this step after Pakistan's espionage agency employed a "honeytrap" strategy of having attractive women on social media lure Indian defense personnel into sharing sensitive information, reported India TV News.

Indonesia: In February 2015, the Indonesian Air Force issued an order reminding personnel of the dangers of using social media platforms. This order forbids them from posting comments on social media about military activities as well as social, political, economic and cultural issues, according to *The Jakarta Post* newspaper.

However, Air Force spokesman Hadi Tjahjanto told the *Post* that the order was not an outright ban on military personnel using social media: "This is actually not a ban, but they should know better what is proper to say and what is not," he said.

CHINA THE EXCEPTION

Defense and security officials worldwide are increasingly embracing social media as a tool — and even encouraging military units and individual Soldiers to use it in a constructive, proactive way. Organizers are holding global conferences about how militaries can harness social media to convey positive messages and to counteract false information.

In China, however, the PLA has gone against this

Social Media TIPS FOR TROOPS

- Don't reveal schedule information and event locations.
- Turn off the GPS functions on smartphones to avoid geotagging.
- Place privacy setting options to "friends only."
- Review photos and videos before posting them online to make sure sensitive information isn't revealed.
- Make sure family and friends understand what type of information should be posted on social networks.
- Do not talk negatively about supervisors.
- Particularly for leaders, conduct online should be professional. If you wouldn't say it in front of a formation, do not say it online.
- Leaders should communicate social media guidelines to their Soldiers.
- Monitor your social media presence to make sure other users are not posting sensitive information on your online presence.
- It is inappropriate to use rank, job or responsibilities to promote yourself online for personal or financial gain.

Source: *U.S. Army Social Media Handbook*

AFP/GETTY IMAGES

AFP/GETTY IMAGES

LEFT: The instant messaging platform WeChat is popular in China.

People use computers at an Internet cafe in Manila, Philippines.

trend. The world's largest military force bans its more than 2 million soldiers from using social media.

The PLA first announced this ban in 2010. "But in a sign that the ban was apparently being ignored in a country where social media are wildly popular, the military brass has taken the step of re-emphasizing the restriction, warning of a 'grim struggle' on the Internet," Agence France-Presse (AFP) reported in 2011.

State media said the ban was intended to "safeguard military secrets and the purity and solidarity" of the PLA, according to AFP. The *PLA Daily* warned soldiers that posting details such as their address, duties or contact information could risk revealing the locations of military sites. Posting photos of themselves could divulge sensitive information about military capabilities or equipment, the newspaper added.

In May 2015, China warned its retired military officers to be cautious when using social networks. Some of them had created chat groups on WeChat, where some still-active officers had joined discussions, the *South China Morning Post* quoted the *PLA Daily* as saying. According to the *Post*, the PLA instructed that "Military officers and soldiers should be cautious … to prevent some people with ulterior motives trapping military staff and acquiring secret information."

Also in May 2015, China banned its soldiers from wearing "Internet-connected wearable tech," the BBC reported, adding that security concerns were raised "after one recruit had received a smartwatch as a birthday gift."

THE DANGERS OF GEOTAGGING

A number of social media networks are offering an increasingly popular feature: the option of attaching geographical data to material that users post online.

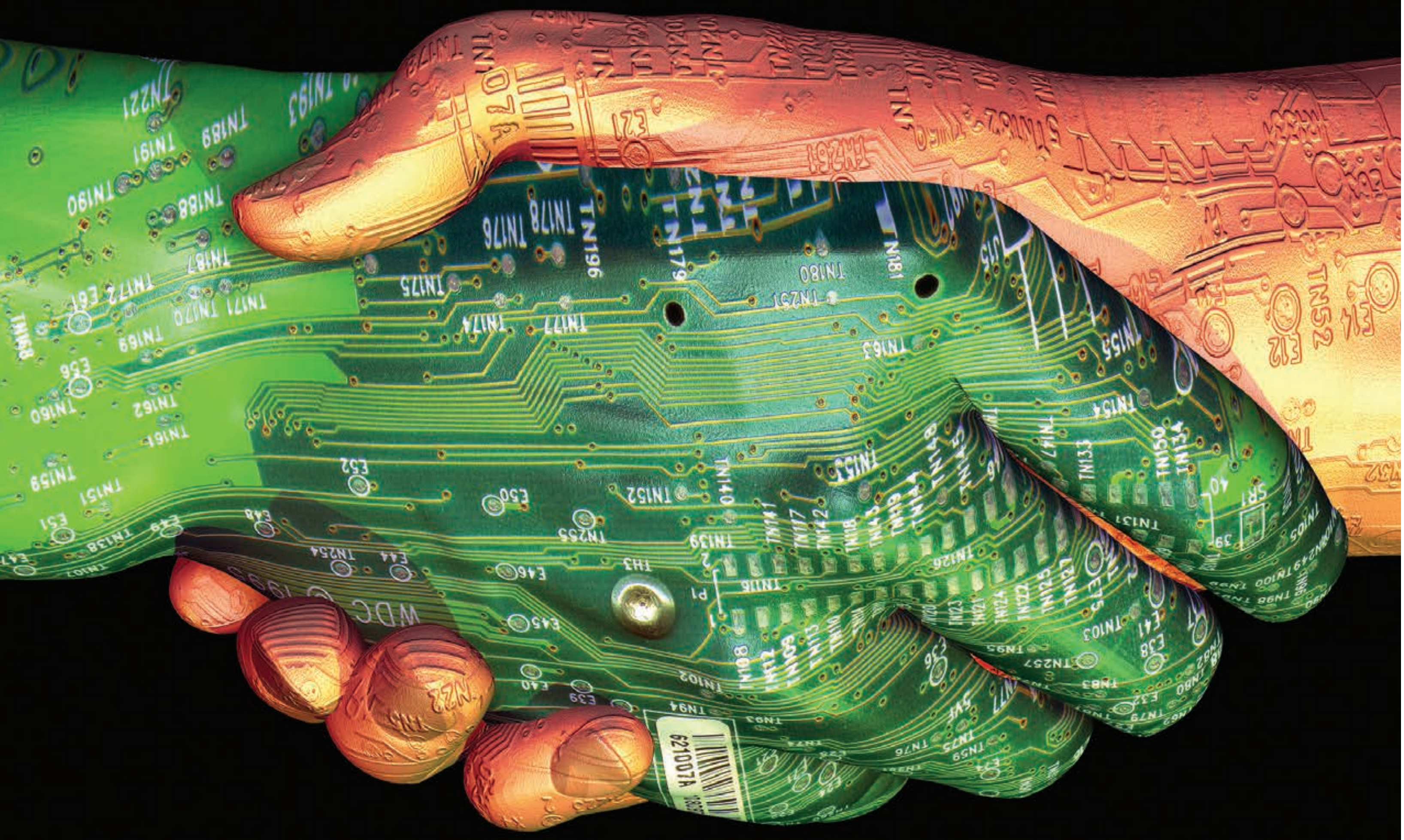
For Soldiers, this can be a problem. The *U.S. Army Social Media Handbook* has the following to say about it:

"Geotagging is the process of adding geographical identification to photographs, videos, websites and SMS messages. It is the equivalent of adding a 10-digit grid coordinate to everything posted on the Internet. Some smartphones and digital cameras automatically embed geotags into pictures, and many people unknowingly upload photos to the Internet that contain location information."

The rising popularity of this feature is creating serious operational-security concerns for military units, the handbook added.

"One Soldier exposing his/her location can affect the entire mission," it said, warning that Soldiers should avoid using location-based social networking sites. "These services will bring the enemy right to the Army's doorstep."

This represents another example of how today's rapidly evolving technologies prompt changes in society and create new and unforeseen challenges for defense and security officials. Social media is inescapable. That's why military leaders across the globe are taking proactive steps to ensure that Soldiers, personnel and families use it responsibly. □



ISTOCK

CYBER SECURITY RELATIONS

China and the United States continue to negotiate the fine print of their agreement and terms of cooperation

BY DR. CHING CHANG AND JACOB DOYLE

The fall of 2015 may well be remembered for the warming trend in China-U.S. relations involving the cyber realm.

It began with a visit in late September by Chinese President Xi Jinping to the United States — first to Seattle where he met with tech luminaries from China and the U.S., including Microsoft co-founder Bill Gates, then on to a summit meeting in Washington, D.C., where Xi met with U.S. President Barack Obama to discuss a range of issues, cyber security notably among them. The "cyber agreement" signed by the presidents was followed by a flurry of activity among their aides, culminating in a follow-up meeting on December 1 devoted to cyber security, attended by heads of law enforcement and national security. Reports from government officials and private sector analysts reinforce the notion of warmth and progress in an area troubled by the chill of contention for many years.

This 12-story building in a Shanghai suburb allegedly housed a Chinese military-led hacking group, according to a 2013 report by Mandiant, an Internet security firm. AFP/GETTY IMAGES

"It is believed that consensus reached by China and the U.S. on the issue of cyber security will help enhance mutual trust and promote cooperation between the two countries in this regard," China's Foreign Ministry spokesman Hong Lei told reporters after the summit on September 28, "and have positive effects on the sound and steady growth of China-U.S. relations."

The agreement promises cooperation from both sides on investigation of cyber crimes, collection of electronic evidence, and mitigation of malicious cyber activity emanating from their territory. Both countries also pledged that neither government will conduct or knowingly support cyber-enabled theft of intellectual property.

Policy analysts in the U.S. recognized the agreement as movement toward better cyber relations between the two countries.

"The United States and China have been disputing the issues of cyber intrusions for quite some time," Joseph S. Nye Jr., Harvard University distinguished service professor at Harvard Kennedy School, said in an interview with *FORUM*. "The Americans had accused the Chinese of using cyber attacks as a way to steal intellectual property for commercial purposes. The Chinese have replied that they didn't do that, that the United States was constantly interfering in their systems. So there had been a dispute for quite some time. It was dealt with by Obama and Xi at the Sunnyland Summit in 2013. But this agreement reached in September 2015 was the first bit of substantive progress that we've seen. I think the agreement is an important first step."

Nye's observations were largely shared by Andrew Scobell, a senior political scientist at Rand Corp., who added that the Chinese succeeded in showing that Xi understands the importance of reaching an understanding on cyber issues with the U.S. from a commercial perspective.

"The Chinese also realized that they needed to make some gesture to the Obama administration, and they did," said Scobell.

The need for gestures and tangible

expressions of cooperation in the cyber realm resonates from years of discord shared by the two countries in this area, as demonstrated by past statements from government officials in China and the U.S.

A 2014 study headed by Dr. Teng Jianqun, a retired officer of China's People's Liberation Army Navy, now director and research fellow of the Centre for Arms Control at the China Institute of International Studies, a think tank in the Ministry of Foreign Affairs in Beijing, indicates China's less-than-favorable view of U.S. cyber policies at the time.

"It is obvious that by making full use of its advantages in information technology, the United States has not only abused its legal and technological means in anti-terrorism operations," reads Teng's study, "but put the leaders of other countries, including its allies, and important international conferences under surveillance, all with the excuse of protecting national security."

The study reads critically of what it calls "cyber arms," purportedly used by the U.S., such as the malicious "Stuxnet worm" computer virus and various signal-jamming technologies.

The year following Teng's study, in January 2015, U.S. Director of National Intelligence James R. Clapper made remarks that echoed a 2014 U.S. indictment against five members of China's People's Liberation Army, accusing them of hacking into the networks of Westinghouse Electric, the U.S. Steel Corp. and other U.S. companies.

"China has been robbing our industrial base blind," Clapper told an audience at New York's Fordham University during a conference on cyber security.

Tensions escalated in June 2015, when the United States Office of Personnel Management announced that it had sustained a data breach targeting the records of as many as 4 million people. U.S. media reported that U.S. government officials were privately blaming China for the intrusion, to which China's Foreign Ministry issued a quick response.

"Cyber attacks are usually conducted anonymously and across borders, making it hard to trace back," Hong told reporters on June 5, 2015. "It is not responsible nor scientific to always use terms such as 'likely' or 'suspected' instead of conducting thorough investigations. It is the consistent position of China to firmly combat all forms of cyber attacks. China itself is a victim of cyber attacks. We are ready to carry out international cooperation on this issue and build a cyberspace that is peaceful, secure, open and cooperative. We hope that the U.S. side would discard suspicions, refrain from making groundless accusations, and show more trust, and conduct more cooperation in this area."

Whether the accusations were groundless, Hong's call for cooperation and peace is similarly made in chapter four of Teng's study: "China and the United States should cooperate in exploring

Customers use computers at a Beijing Internet bar in December 2015.
AFP/GETTY IMAGES

possible plans for cyberspace arms control," which advocates an "international cybersecurity treaty, which would set limits on the development of other nations' cyber-warfare capabilities."

Peace in cyberspace was not the only prospect luring China into a cyber dialogue with the U.S., Scobell contends. Intellectual property rights (IPR), he explained, have recently been discovered by the Chinese as things worth protecting.

"A lot of these commercial cyber hacks appear to be motivated by acquiring copyrighted or proprietary information that's owned by a particular company," said Scobell. "China didn't much care about IPR until Chinese firms began to develop their own valuable intellectual property. Now China is attuned to the problem and more willing to work with other states to protect IPR."

Nye recognized discussion of the topic of IPR and its corollary — concern about using cyber espionage for commercial purposes — as comprising one of the 2015 summit's two most important results relating to cyber issues.

"The second thing is that the two countries have set up a high-level group to deal with this," said Nye, "and that has actually occurred with Attorney General Loretta Lynch and Homeland Security Secretary Jeh Johnson meeting a Chinese counterpart in Washington on 1 December, 2015."

In addition to Lynch and Johnson, the meeting was attended by Chinese State Councilor Guo Shengkun, as well as representatives from the U.S. Department of State, National Security Council and the intelligence community, while the Chinese delegation included representatives from the Committee of Political and Legal Affairs of the Communist Party of China Central Committee, the Ministry of Public Security, the Ministry of Foreign Affairs, the Ministry of Industry and Information Technology, the Ministry of State Security, the Ministry of Justice and the State Internet Information Office.

According to Lynch's office, the meeting undertook to "review the timeliness and quality of responses to requests for information and assistance with respect to cyber crime or other malicious cyber activities and to enhance cooperation between the United States and China on cyber crime and related issues."

Chinese Foreign Ministry spokeswoman Hua Chunying called the meeting a success the day after it was held, saying the dialogue was "positive and constructive," adding that "China-U.S. law enforcement cooperation on cyber security has now entered a new phase of progress as the two sides have solved some specific problems through practical cooperation and candid communication, which helped boost mutual understanding and trust."

The second "U.S.-China High-Level Dialogue on Combatting Cybercrime and Related Issues" was set for June 2016 in Beijing, reported Lynch's office.

Formulating and agreeing to a "cyber code of conduct," or set of norms of behavior in the cyber realm that all signatory countries would follow, has been a topic mentioned in Teng's study and alluded to by the White House in a statement following the September summit. It said the U.S. and China "welcome the July 2015 report of the U.N. Group of Governmental Experts (GGE) in the Field of Information and Telecommunications in the Context of International Security, which addresses norms of behavior and other crucial issues for international security in cyberspace."

In early 2015, China and Russia, along with Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan, jointly submitted an update of their own International Code of Conduct on Information Security to the U.N. secretary-general. Originally submitted in 2011, it received criticism from the U.S. and its allies as "an attempt by the four countries to justify greater state control of the Internet's governance structures and online content," according to Alex Grigsby, assistant director for the Digital and Cyberspace Policy program at the Council on Foreign Relations. The recent updates, Grigsby added, reference the GGE's activities and "seem to soften China and Russia's stance on states taking a leadership role on Internet governance issues."

While the G20 group of nations endorsed the GGE report during their July 2015 summit in Antalya, Turkey, the concept of a multilateral cyber code of conduct is viewed by Scobell as a somewhat separate issue from the discussions and activities currently involving the U.S. and China.

"The United Nations is not an arbiter in the cyber realm," said Scobell. "I don't think either side in Washington or Beijing would shift the dialogue to a multilateral forum like the United Nations any time soon. I suspect both sides would tell you that the two countries need to hash this out. A multilateral dialogue cannot replace this, as there's some serious contentious issues here that involve the United States and China, and so there is really no substitute for one-on-one discussions."

Where there is friction, there is warmth. Time will tell if the warming trend continues. Experts agree that much work remains to define the terms of the agreement in practice to enable the thaw to progress. □

DISASTER RESPONSE IN NEPAL

U.S. PACOM'S CONTRIBUTIONS TO THE 2015 EARTHQUAKE RELIEF EFFORT

JUSTIN PUMMELL

The air is crisp as residents awake to conduct their morning routine. The evening echo of a dog's bark has been replaced by blaring horns and screeching minibus tires. Crows curiously jump from tree to tree, as monkeys trapeze along bouncing power lines. School is out, and many children are pouring into courtyards and parks to play. Cafes are full, as milk tea is tasted over the hum of quiet conversation. As the sun slowly lumbers from the treetops to prominence, the day appears idyllic — a typical Saturday morning in Kathmandu — when suddenly, a low growl bellows beneath, shaking the ground, causing an unexpected commotion.

Meanwhile, at the Tribhuvan International Airport (TIA), people have crowded the domestic and international terminals to head to destinations near and far. The paparazzi have just wrapped up their morning flights to Mount Everest. A majority of TIA senior staff are at home enjoying their Saturday rest, escaping from the usual trials and tribulations of managing Nepal's only international airport. The abrupt shaking of the ground causes screams to barrel through the terminals and departure gates. Panic strangles Kathmandu Valley.

Many natives had never experienced an earthquake, though it's something they had anticipated for years. On April 25, 2015, it became reality, when a magnitude-7.8 earthquake ripped through Nepal, killing nearly 9,000 people and injuring more than 22,000. It was the largest earthquake Nepal had experienced since 1934, with the Gorkha region at the initial epicenter.

Collapsed houses remain in Sankhu, on the outskirts of Kathmandu, and Sindhupalchowk, Nepal, in May 2015. Children, center, stand on the foundation of a collapsed house in a nearby village after the earthquake. REUTERS

RAPID RESPONSE

Within hours of the disaster, the government of Nepal convened its Central Natural Disaster Relief Committee, and the prime minister made an appeal for international assistance. Many countries, including the United States, sprang into action.

The U.S. government immediately issued a disaster declaration for Nepal. Within hours of the seismic event, the U.S. Agency for International Development's Office of U.S. Foreign Disaster Assistance (USAID/OFDA) had activated a response management team in Washington, D.C., and deployed a Disaster Assistance Response Team (DART) — including urban search and rescue specialists — to support emergency response efforts in Nepal.

After conducting initial assessments, USAID/OFDA determined that unique military assistance, such as rotary wing airlift, would be necessary to support the response, and delivered an official request for U.S. Department of Defense assistance. This request was approved by the U.S. secretary of state and the secretary of defense, and sent to U.S. Pacific Command (USPACOM) to fulfill.

USPACOM then ordered the III Marine Expeditionary Force to formulate a Joint Humanitarian Assistance Survey Team (JHAST) to travel to Nepal. Using the Joint Task Force-505 (JTF-505) concept of operation plan (CONPLAN), the JHAST supported civilian authorities, such as USAID/OFDA, and grew from a 23-person JHAST to a more than 290-member joint forward unit.

"JTF-505 brought a variety of unique capabilities to provide humanitarian assistance/disaster response to the government of Nepal," said Brig. Gen. Jeffrey Milhorn, commanding general of the U.S. Army Corps of Engineers Pacific Ocean Division and designated deputy commander of JTF-505. "Aviation assets were used to conduct area assessments, move humanitarian-aid supplies, transport personnel and transport mission-essential assets. Additionally, the 36th Contingency Response Group (CRG) helped augment host nation civil aviation partners to offload high volumes of aid being delivered by multiple organizations to Tribhuvan International Airport."

JTF-505 efforts were being performed in parallel to a large international and civilian response that was already well on its way.

The initial JHAST included Marines, Airmen, Soldiers and a U.S. Army Corps of Engineers (USACE) civilian. Traveling from Okinawa, Japan, the team landed in Nepal on April 29, 2015, shortly after the USAID DART team arrived.

"We offloaded adjacent to the main taxiway since all of the existing nine bays were full with other aircraft," said Master Sgt. Drew Kimmey, Civil Affairs NCO, U.S. Army Pacific (USARPAC). "The situation did not surprise me. We [JHAST] already knew TIA was going to be a very busy place, given its critical value to the country. I was just relieved that the runway did not sustain any significant damage."

Kimmey had reason to believe the airfield might be compromised. In 2011, on behalf of USPACOM, USACE and the Civil Aviation Authority of Nepal conducted a seismic evaluation of critical airfield infrastructure, including a geophysical investigation of soils and the development of a potential surface liquefaction map. These planning tools were designed for a magnitude-9.0 earthquake and indicated that the full length of the TIA runway might not be available. This also led to confirmation that a two-plan approach for TIA operability in the JTF-505 CONPLAN was necessary, according to Lt. Col. Vince Koopmann, a primary author of the CONPLAN.

PLANNING TOOLS

The CONPLAN included one primary plan and one branch plan based on the level of damage and accessibility into Nepal. It also included collaboration with government of Nepal ministries, the Nepalese Army, USAID/OFDA, United Nations Office for the Coordination of Humanitarian Affairs, World Food Programme (WFP) and others.

The primary plan was based on the assumptions that Nepal regional airfields and Tribhuvan International Airport would sustain limited damage with reduced aprons. In the primary plan, command and control and supplies and equipment were to be immediately deployed into Nepal via air, as well as rail and road networks if operational.

The branch plan was based on catastrophic damage rendering TIA and key physical infrastructure inoperative, forcing JTF-505 command and control and supplies and equipment to locate outside Nepal. In the branch plan, the command and control and supplies and equipment were envisioned to be situated in potential intermediate staging bases in India and Camp Red Horse, Royal Thai Navy Base-Utapao, Thailand.

The following morning, the JHAST coordinated with USAID/OFDA, connected into the Nepalese Army-led Multi-National Military Coordination Centre (MNMCC), and made contact with representatives at TIA. Once at the airport, the team sat down with TIA staff and asked how response efforts were progressing. The TIA Disaster Response Plan, developed in 2013 as part of USPACOM's security cooperation program, was already in use.

"Thanks to the USPACOM, USACE, the Federal Aviation Administration and the University of British Columbia, we had a plan in place that we could use," said Deo Chandra Lal Karna of the Civil Aviation Authority of Nepal. "We also tested the plan in 2014 by conducting an international exercise through the support of USPACOM, USARPAC and USACE. In particular, the emergency operation land use map served as principle guidance to ensure airfield space was maximized, organization was maintained, and everyone had a common picture to understand TIA's desired operational intention."

TIA authorities later enhanced this map during the response to more accurately reflect the most appropriate use of the aerodrome.

SPACE MANAGEMENT

For JTF-505 to fulfill its mission tasking from USAID, an operational space at TIA, or another outlying airfield, was critical.

"The Indian Air Force was already operating out of Pokhara," said Lt. Col. Rod Legowski, operations officer, 3rd Marine Expeditionary Brigade. "JTF-505 needed to decide whether it would also operate out of an outlying Nepali airfield or try to make room at TIA. We knew this through our planning for potential response."

Given the extensive cooperation and enduring relationship with TIA staff, the JHAST developed a plan and proposed it to TIA authorities. The plan included using two fixed-wing bays at TIA, as well as a portion of a taxiway to park helicopters.

After coordination and negotiation, the proposal was accepted, and JTF-505 had an operating space to support the people of Nepal and USAID.

"Due to increased needs and limited space capacity at TIA, it quickly became apparent to the humanitarian community that space management at the airport would be critical to the response," said Scott Aronson, USAID/OFDA's humanitarian assistance advisor. "In particular, these considerations had a direct impact on USAID/OFDA's response, and the support being provided by JTF-505. One of the most critical aspects of this operation was building trust with the Nepalese airport authorities that we would properly use space provided to us, work within the guidelines they gave, and demonstrate efficient use of the spots provided. This would not have been possible without already having strong relationships with TIA officials before the earthquake, which proved invaluable in trying to address the space issue."

THE NEPAL EARTHQUAKE RESPONSE DEMONSTRATED SEVERAL KEY LESSONS LEARNED THAT SHOULD BE SUSTAINED IN THE FUTURE

EXISTING RELATIONSHIPS ARE CRITICAL.

If the person across the table does not trust you, then the mission is at risk of failure. Spend time fostering positive and lasting relationships. Security cooperation activities are a great way to establish these relationships. The continuity of civilian employees is also helpful in making relationships last. The U.S. Army Corps of Engineers' role on the joint task force is a good example.

CIVIL-MILITARY COOPERATION IS ESSENTIAL.

The regular practice of plans and procedures helps civilians and military personnel better understand each other's capabilities so they can use them when necessary. This occurred among U.S. Agency for International Development's Office of U.S. Foreign Disaster Assistance, Joint Task Force-505 (JTF-505), Tribhuvan International Airport (TIA), World Food Programme, Deutche Post Logistics and many other international and nongovernmental partners. Previous exercises, such as U.S. Army Pacific's Disaster Response Exercise and Exchange, developed civil-military cooperation and should be continued.

SECURITY COOPERATION FOSTERS EFFECTIVE RESPONSE.

The situation in Nepal may have turned out a lot differently if regular humanitarian assistance and capacity development engagements had not occurred. For example, if TIA did not have a Disaster Response Plan, airfield operation and management could have quickly slowed to a halt. If humanitarian assistance/disaster relief exercises had not been performed regularly, the Multi-National Military Coordination Centre concept may have been unknown or not well practiced. Exercises provided an avenue to acquaint personnel with standard procedures and to refine draft concepts that may have failed.

A JOINT TASK FORCE PLAN IS NECESSARY.

The JTF-505 concept of operation was instrumental in guiding an effective U.S. Department of Defense response. Without this plan, an ad-hoc approach may have been used, which would have slowed U.S. military response efforts. A concept of operation plan should be established for other large-scale humanitarian assistance/disaster relief scenarios in the Indo-Asia-Pacific region.

Nepalese Army personnel unload relief aid in Kathmandu in April 2015.

AFP/GETTY IMAGES

A Nepalese Soldier carries an injured earthquake victim from a U.S. Marine Corps UH-1Y Venom helicopter to a medical triage area at Tribhuvan International Airport in Kathmandu, Nepal, in May 2015. REUTERS

The situation described above might have turned out differently if USPACOM's humanitarian assistance and capacity development programs had been less active with TIA partners. Since 2012, USPACOM humanitarian assistance funds have allowed for 34 engagements — spending more than U.S. $7.83 million — to build earthquake disaster preparedness and resiliency in Nepal. Activities have ranged from the development of the Disaster Response Plan to digging deep tube wells to the construction of a new crash fire rescue station.

"With a focus on TIA, USPACOM has made a concerted effort to build Nepal's capacity to prepare for and cope with a large-scale earthquake disaster … and we will continue this effort in the coming years," said Tiger Hession, manager of USPACOM's Overseas Humanitarian, Disaster and Civic Assistance.

INTERNATIONAL COOPERATION

During the response, JTF-505 combined efforts with Deutche Post Logistics Group, Nepal Airlines, Nepalese Army, WFP and others to manage material handling and cargo at TIA. "Once we were allowed access to the tarmac via support from the Nepal airport authorities and Nepal military, we could move around to most places to support humanitarian operations," said Nate Nathanson, Civil-Military Operations specialist with the WFP. "We had four open-bed mini-trucks to support movement of supplies from the TIA staging area to the humanitarian staging area. We did not have any organic material handling equipment [MHE], as this platform was in short supply within Kathmandu. Nets, cargo equipment, MHE was rented by the International Office of Migration, and MHE was also donated by DFID [United Kingdom's Department for International Development]."

The joint team commanded, assessed, and prepared a base for expeditionary and commercial aerodrome operations. The airport experienced limited operational downtime as a result. The team supported logistics, including unloading/loading aircraft, movement of aircraft palettes and warehouse relief supplies, and ground inventory, as well as making sure incoming supplies were received by the appropriate relief organizations. Cooperation among organizations permitted movement of cargo from the tarmac down to the humanitarian staging area and beyond, out to the beneficiaries. Also key to the operation was close coordination for material to be picked up at the tarmac by other agencies to support the efforts.

"JTF-505 immediately integrated with Nepal Army, Nepal Airlines, World Food Programme, and commercial entities in order to coordinate and streamline TIA logistical processes amongst all parties, as well as to optimize the use of 36th CRG's four deployed [4,500 kilogram] forklifts and a [11,300 kilogram] loader," said Lt. Col. Glenn Rineheart, commander of the U.S. Air Force's 36th Mobility Response Squadron. "Thirty-sixth CRG personnel would ultimately collaborate with militaries from seven

Earthquake survivors walk along a street next to collapsed houses in Sankhu, on the outskirts of Kathmandu, Nepal. REUTERS

countries and various commercial carriers to download [23,500 metric tons] of aid from 108 aircraft, as well as assist the WFP to distribute the equivalent of 360 truckloads of aid to 13 Nepal districts and 2.8 million earthquake victims."

By May 11, 2015, JTF-505 had completed a majority of its mission tasking matrix (MITAM) assignments. It was anticipated that the unique capability of the U.S. military was waning, and USAID would soon determine it was time for JTF-505 to return home. However, this all changed on May 12, 2015, when a magnitude-7.3 earthquake struck northeast of Kathmandu Valley.

At TIA, JTF-505 personnel supported terminal evacuation procedures, runway and infrastructure inspections, and the establishment of a temporary field hospital to receive injured personnel being brought from rural areas. JTF-505 personnel received the injured via helicopter, stabilized them in field tents set up on the tarmac, and then loaded them for transport to local hospitals. JTF-505 personnel also worked with TIA and Nepalese Army authorities after a UH-1Y helicopter went missing.

"The memories of those killed on 12 May will never be forgotten," Milhorn said. "Their selfless acts are an exemplary hallmark of humanitarian action."

UNIQUE CAPABILITES

The May 12, 2015, earthquake extended the need for unique military capability and resulted in many new MITAM assignments. JTF-505 primarily delivered aid to locations in the Sindhupalchowk, Ramechhap, Dolakha, Kavre and Okhaldhunga districts, but it also serviced many other areas.

Typically, JTF-505 personnel would receive a USAID tasking, and then work with the Nepalese Army to identify an appropriate landing zone to deliver the aid. This took extensive coordination through the MNMCC.

"The National Emergency Operation Centre would provide the request [for relief materials to be airlifted] 48 hours in advance to the MNMCC," said Col. Naresh Subba, MNMCC coordinator with the Nepalese Army. "MNMCC reps would then work out the mission tasking matrix with JTF-505, and a flight operation plan would be prepared. As per the flight operation plan, the Air Operation Centre at Mid Air Base would coordinate with local Nepalese Army units [where the flight was scheduled to land] to prepare landing sites and provide necessary security."

On May 23, 2015, JTF-505 officially departed Nepal, with the WFP filling the airlift logistics role, Nepal Airlines and Nepalese Army filling the material-handling equipment role, and USAID's international and nongovernmental partners filling the aid delivery role. In total, JTF-505 completed 25 MITAMs, delivered 113.8 short tons of aid to remote villages, transported 550 passengers (including 63 casualty evacuations), and provisioned stopgap airfield logistics supporting 108 aircraft and more than 23,500 metric tons of humanitarian aid. □

CRISIS COMMUNICATIONS

Exercise Pacific Endeavor tests nations' capabilities during major disasters

FORUM STAFF

Earthquakes. Typhoons. Tsunamis. Many of the world's deadliest natural disasters occur in the Indo-Asia-Pacific. During the past decade, half a million residents of the region have died from catastrophic forces of nature — comprising nearly 60 percent of the world's disaster deaths — the United Nations reports.

When disaster strikes, one of the first casualties tends to be the local communications infrastructure. Cellphone towers lose signals. Internet service providers go dark. Information can't get in or out.

Setting up communications quickly is vital to saving lives.

"Communications people are generally some of the first people on the ground," said Cpl. Rochelle Rowe, a communications specialist with the Royal New Zealand Air Force.

Military personnel from 21 nations gathered in the Philippines in September 2015 for Exercise Pacific Endeavor, an annual disaster-response drill organized by U.S. Pacific Command (PACOM). They'll repeat the exercise in August and September 2016 in Australia.

Planners designed the event to smooth communications between military and civilian responders during major disasters.

The Philippines exercise introduced the mock scenario of a magnitude-7.2 earthquake toppling buildings in the nation's capital city, Manila. The goal was to test participants' abilities to communicate with each other during a catastrophe.

The drill went on for hours. Hunkered down with radios, computers, satellite phones and assorted gear, the communications operators scrambled to connect with one another. During the exercise, power would cut off unexpectedly. Voices appeared and faded amid bursts of static. In real time, operators strived to relay bits of vital information about the hypothetical earthquake and its aftereffects, so they could help coordinate relief efforts.

"A disaster is a bad time to find out something doesn't work," said U.S. Navy Cmdr. Paul Salevski, Multinational Communications Interoperability Program (MCIP) workshop director for PACOM. "Life is in the balance."

MCIP, which organizes Pacific Endeavor, establishes a process to identify and document communications interoperability among member nations. MCIP's primary goal is to ensure the interoperability of military equipment such as radios, satellites, telephones and cyber communications.

Exercise planners called Pacific Endeavor 2015 a success, with participants working through various challenges. During the mock earthquake, they patched together a communications network that could provide vital information to an international disaster-response force.

"We're able to work with each other, especially on the military side, so that when the time comes, it's not as hard to conduct global humanitarian assistance and disaster relief operations," said Maj. Leo Caduyac of the Philippine Army's Signal Command.

Organizers attribute Exercise Pacific Endeavor's success to its frequency and longevity: It's been held every year since 2004, building upon lessons learned from previous exercises and from real-life disasters.

The exercise moves around the region, with recent hosts including Nepal in 2014, Thailand in 2013 and Singapore in 2012. Australia will host the exercise in 2016.

Since the exercise was founded, it has expanded to include most of the region's governments and military forces, the United Nations, nongovernmental

Philippine Army Maj. Leo Caduyac, left, a Signal Command Soldier, checks radio communications during Exercise Pacific Endeavor in Manila in September 2015. DVIDS | **A Nepalese Soldier walks through debris from collapsed buildings on April 30, 2015, in Kathmandu. Many houses, buildings and temples in the capital were destroyed by an earthquake, leading rescue workers to attempt to clear debris and find survivors.** GETTY IMAGES

Nepalese Soldiers run with parcels of food aid during relief operations after an earthquake struck Nepal on April 25, 2015, killing more than 8,000 people and leaving nearly 3 million homeless. AFP/GETTY IMAGES

organizations such as the International Federation of Red Cross and Red Crescent Societies (IFRC), and representatives of industry and academia.

Several planning workshops throughout each year culminate in a large-scale capstone event in August or September. When it came time for the Philippines to host Pacific Endeavor 2015, Philippine officials made it clear they wanted the exercise in their capital to simulate a major earthquake.

"Everyone was thinking typhoon, but they surprised us," said Salevski.

Philippine Army Lt. Col. Mark Edwin Moro, chairman of the workshops' Scenario Technical Working Group, explained the choice.

"During an earthquake, you don't have time to prepare, unlike a typhoon where you can track the progress," Moro said. "The earthquake scenario is more brutal and sudden."

Pacific Endeavor 2015, a two-week-long exercise that ran from August 31 to September 11, drew more than 330 participants to Manila, according to U.S. Navy Rear Adm. Kathleen Creighton, PACOM J6, director of Command, Control, Communications and Cyber Directorate.

Toward the end of the event, Rear Adm. Creighton took part in a three-day, Pacific Senior Communicators Meeting consisting of high-ranking military communications officials from all 21 participating nations. They pored over hard lessons that had been learned in recent disasters in the Indo-Asia-Pacific region.

Organizers presented senior communicators with challenging topics within the command, control, communications and computers realm, and they applied them to the unclassified information-sharing process used in a multinational disaster relief response, explained Creighton. "There were many pointed questions and worthy discussions held based upon the material presented," she said. "The lessons learned from the Philippines' Typhoon Yolanda/Haiyan, the 2015 Nepal earthquake and other disasters were well-delivered and accepted by the group."

The nations of the Indo-Asia-Pacific are well aware of the challenges. Disaster relief

agencies point to four major catastrophes from the past several years:

- An April 2015 earthquake near Kathmandu, Nepal, killed more than 8,000 people, destroyed more than 473,000 homes, and displaced more than 2.8 million people.
- Typhoon Haiyan — known as Typhoon Yolanda in the Philippines — killed at least 6,300 people and displaced 4 million when it made landfall in November 2013, making it the deadliest Philippine typhoon in history.
- During the summer of 2015, massive flooding in Burma around the Irrawaddy Delta affected about a million people and killed roughly 100.
- In March 2011, a magnitude-9.0 earthquake and tsunami in Japan killed nearly 16,000 people, stranded another 16,000, forced the evacuation of more than 350,000 people, and caused the release of radioactive material from damaged nuclear power plants.

U.S. Marine Corps Maj. Erika Teichert of the Naval Postgraduate School demonstrates setting up a mobile satellite system for communicators during Exercise Pacific Endeavor in Manila in September 2015. DVIDS

SHARING INFORMATION

Preparing to communicate with each other during such a catastrophe, Pacific Endeavor participants gained access to equipment tests, interoperability assessments, unclassified information sharing and technical demonstrations. The face time with one another helps develop better relations between militaries, Creighton said.

"The returns on investment are profound," she said. "It is an engagement event for so many military communications personnel, from the low ranks to the most senior."

During each year's Pacific Endeavor, participants can take part in Information Sharing Modules that focus on modes of communication, such as Cyber Endeavor, Radio Endeavor or Satcom Endeavor, which emphasizes satellite communications.

A crucial aspect of Pacific Endeavor is the opportunity for communications operators to share information about evolving technologies that could be useful in a crisis situation.

During 2015's Satcom Endeavor Information Sharing Module, for example, satellite communications experts showed participants how to use the broadband global access network (BGAN), a mobile Internet link designed for austere locations. The lightweight devices can be ready in a matter of minutes.

"The BGAN gives five or six people that first-in capability to tell their higher headquarters what the ground truth is, so that the higher headquarters can plan and ensure that the right help is going to the right people, at the right time and the right place," said U.S. Marine Corps Maj. Erika Teichert, an officer from the Naval Postgraduate School.

Traditional means of communication, such as high frequency (HF) radio, are also helpful. Military officials can use it for long-distance communication, giving them another option besides phones or the Internet.

"The reasons why we would choose radio frequencies or HF over Internet Protocol: It's a lot quicker to deploy, it's not so hard to get the equipment there, it's reasonably small, lightweight, and it's easy to train someone," said Staff Sgt. Andrew Wickham of the New Zealand Defense Force, a facilitator in 2015's Radio Endeavor Information Sharing Module. "Just like a cellphone, you can pick up the handset and start talking. You can send reports. You can ask for medivac and a range of facilities that you may require."

Pacific Endeavor 2016, to be held from August 22 to September 2 in Brisbane, Australia, will focus further on unclassified information sharing, said Salevski, the MCIP workshop director.

"We are building the baseline of knowledge in cyber, radio fundamentals, spectrum management, information and knowledge management, and satellite communications," Salevski said. "We build the personal relationships, mutual understanding and trust between the junior and senior levels of the enlisted, warrant and officer ranks. Those relationships also extend to the major civilian actors involved in international disaster response. All of these things work to eliminate those barriers to communication." □

STRENGTHENING THE NETWORK

THE SOVEREIGN CHALLENGE PROGRAM PROMOTES SECURITY BY BUILDING INTERNATIONAL RELATIONSHIPS

UNIPATH STAFF

Preserving the sovereignty of independent nations and protecting people from the threats violent extremists pose to security and stability are no small aims. These noble goals require not only a whole-of-government response but also an international commitment to synchronize efforts and build relationships that will enhance each country's efforts toward peace and prosperity.

As global news outlets shine spotlights on the atrocities of terrorists and their tentacles of influence and violence across the world, what does not always make headline news are determined and continual efforts to protect the sovereignty of nations and return stability to conflict-ridden areas of the world. Military officials, government leaders and other experts continually work to counter and defeat terrorists. While airstrikes and other military operations are one element of the fight, global partnerships and international dialogue aid in the ultimate defeat of violent extremism.

"Our network is strong and growing," said Gen. Joseph Votel, when he was commander of U.S. Special Operations Command (USSOCOM). He has been nominated to be commander of U.S. Central Command (USCENTCOM). "And through our network, we will defeat those transnational flows that threaten not only our own sovereign security, but global security as a whole."

One such initiative is the Sovereign Challenge program, established in 2004 by USSOCOM. The program serves as a platform for networking, as well as a way for representatives from partner nations to examine extremist threats and develop relationships and a shared understanding of the international challenges to preserving sovereignty and security across the globe.

U.S. SPECIAL OPERATIONS COMMAND

Gen. Joseph Votel was confirmed in March 2016 as commander of U.S. Central Command. He formerly served as commander of U.S. Special Operations Command.

Participants in Challenging Extremism: Engaging the Successor Generation, in Washington, D.C., in September 2015 SOVEREIGN CHALLENGE

"This is a truly unique program — there is nothing else like it," Votel said.

Each year, Sovereign Challenge brings together government and military officials, such as defense attaches posted to the United States and special operations forces professionals. In recent years, academic, industry and other security experts have also joined Sovereign Challenge conferences, seminars and other events where issues such as security, extremism, territorial integrity, terrorist finance networks, internal stability/conflict and transnational crime are discussed.

"The Sovereign Challenge program is one of the tools that help the command look at problems differently. It makes USSOCOM more culturally astute and brings people, capabilities and ideas together to help address some of our most pressing international problems," Sovereign Challenge Program Manager Larry Cook said.

In September 2015, officials met for a workshop in Washington, D.C., on the topic of Challenging Extremism: Engaging the Successor Generation. One of the themes discussed was social media's role in today's fight against the terrorist group Islamic State of Iraq and the Levant (ISIL).

The level of strategic dialogue at Sovereign Challenge events has attracted high-level participation from across the world. The April 2015 gathering brought together more than 200 participants from 81 countries, including Indo-Asia-Pacific nations such as Australia, Bangladesh, Laos, Mongolia, Nepal, the Philippines, and Thailand.

During the conference, Her Royal Highness Maj. Gen. Princess Aisha bint Al Hussein, the then-defense attache of Jordan to the United States, spoke about her country's struggle to defeat terrorism. Sharing borders with Syria and Iraq, Jordan has been troubled by the neighboring conflicts.

"Jordan is no stranger to the chaos that surrounds it," Maj. Gen. Aisha said. "Ten years ago, we mourned the senseless deaths of scores of Jordanians at the hands of terrorists who walked into hotels and weddings and blew themselves up. A mere couple of months ago, we mourned our pilot Muath Kasasbeh — may God rest his soul — whose barbaric killing at the hands of ISIL thugs propelled us to move to the next stage in the war against extremism. Our response as Jordan has been swift and strong. We have been hitting targets ranging from weapons and ammunition depots to training camps. And the momentum continues."

She explained that the fight against ISIL is a global concern as a long-term ideological war that has spread across the Middle East and into Africa, Asia and other regions of the world. She also urged nations to address the plight of marginalized Muslims who have little hope for a prosperous and peaceful future so that they are not easily swayed by extremist ideologies.

"It is clear that we need to eradicate desperation and tackle issues of development and poverty, which rears its ugly head in all parts of the world and in every religion," she said. "The Middle East particularly faces overwhelming challenges, with youth comprising up to 70 percent of the region's population. Failed or failing states are the ideal staging ground for these groups to move in, grow and proliferate. We must address such places today rather than tomorrow."

Much of the conference's discussion centered on these types of shared challenges that cannot be effectively tackled by any one country.

"Today we are witnessing a new type of transnational threat that threatens our respective sovereignty — flows of people, information and funding that move unimpeded across national borders in support of nonstate threat," Votel said in a speech before participants. "Ideas, communication, and recruiting propaganda stream across the cyberspace and increasingly motivate radicalized individuals; some migrate to become combatants, and others to enable them."

Although military powers — especially special

Participants in Transnational Flows in Turbulent Times in New York City in April 2015 SOVEREIGN CHALLENGE

operations forces — are integral to neutralizing these threats, Votel explained that it is far from a long-term solution. “Though we play an important role, we are but one instrument of national power. Complex challenges like the ones we face today require the careful and coordinated application of the full range of strategic options — diplomatic, informational, economic, as well as military. And the key to successfully coordinating such an effort lies in the relationships between the various instruments and partners executing each function,” Votel said.

Isabel De Sola, associate director of geopolitics and international security at the World Economic Forum, echoed these sentiments. During the conference, she explained how businesses have both a stake and role in defeating violent extremism. To put the issue concisely: Conflict is bad for business. By offering decent jobs and offering and supporting educational and mentorship opportunities, businesses can have a valuable impact on strengthening societies.

“Companies can help with, promote and extend counterterrorism narratives to those employed by violent extremist organizations,” De Sola said. For example, businesses in the media and entertainment industries reach vulnerable populations and terrorists themselves, making the messages and content important vehicles to disseminate information.

During a Sovereign Challenge seminar in Washington in September 2015, journalist and CNN security analyst Peter Bergen added his thoughts about the increasingly important role of the media in covering conflict.

“The Vietnam War was the first televised war; the Gulf War was the first cable news war that was available 24/7; and what is going on in Syria is [among] the first social media war[s],” Bergen said. He explained that ISIL uses social media to spread its propaganda and reach out to potential young recruits.

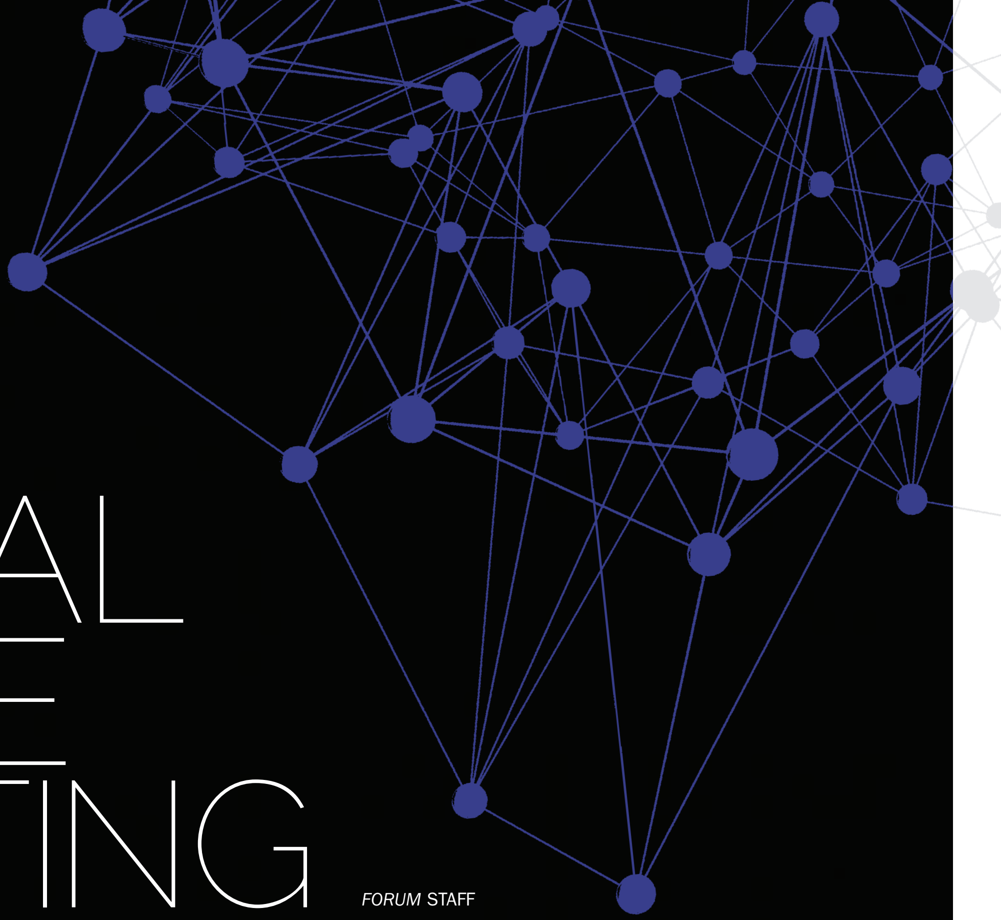
PREVIOUS SOVEREIGN CONFERENCES

- Transnational Flows in Turbulent Times, April 2015
- Sovereign Resilience: An Age of Emerging Threats, April 2014
- Regional Challenges to Global Security: Cultures, Conflicts, Contributions, June 2013
- Beyond Borders: Trafficking Trust and Transnational Security, November 2012
- Social Media: Prominence, Power and Potential, June 2012
- Civil War: Resilience, Reconciliation & Reconstruction, December 2011

To learn more about the Sovereign Challenge program, go to www.sovereignchallenge.org

Examining the threats posed by terrorist groups such as ISIL, al-Qaida and Boko Haram from a variety of angles is essential to developing a strategy that can defeat these organizations on all fronts — ideological, financial and operational. The network of people and organizations supporting Sovereign Challenge is helping accomplish this goal.

“It is through this network that we are able to bring our individual strengths and capabilities to bear against these mutual transnational challenges,” Votel said. “By increasing transparency, communication and collaboration with our partners, we maximize the effectiveness of our collective action.” □



Frontiers in DIGITAL CRIME FIGHTING

FORUM STAFF

Noboru Nakatani, executive director of the Interpol Global Complex for Innovation in Singapore, shares his views on emerging cyber threats

FORUM Staff

FORUM ILLUSTRATION

Noboru Nakatani is on the leading edge of fighting cyber crime in the Indo-Asia-Pacific and worldwide.

He's the executive director of the Interpol Global Complex for Innovation (IGCI), which opened in 2015 in Singapore. The state-of-the-art facility includes a cyber crime center with a digital forensics laboratory that equips the world's police with the tools and knowledge to better tackle the digital crimes of the 21st century.

The IGCI provides high-tech assistance to law enforcement agencies from Interpol's 190 member countries. It is also a research and development center that provides innovative training for digital investigators across the globe. In addition to teaming with law enforcement agencies, the IGCI has partnered with private-sector entities such as Kaspersky Lab, Trend Micro, and Japan's Cyber Defense Institute.

Before he was named the head of IGCI, Nakatani was a special advisor to the commissioner general of Japan's National Police Agency and director of its Transnational Organized Crime Office. He also held the post of director of Information Systems and Technology at Interpol's General Secretariat headquarters, overseeing the development of innovative IT services for the global law enforcement community.

Nakatani spoke to *FORUM* about the nature of emerging cyber threats.

Is the Indo-Asia-Pacific region particularly vulnerable to cyber crime? If so, are there any particular reasons why?

Cyber crime in the Asia-Pacific region accounts for a significant proportion of global cyber crime, yet the diversity between countries can be significant. The growing amount of people connected to the Internet means that cyber crime in the Asia-Pacific region is likely to continue to increase.

Capabilities to address cyber crime need to be assessed in light of a crime situation. Some countries have started to suffer from specific types of cyber crimes, while others have not yet. As cyber crime is a global problem and

Noboru Nakatani is the executive director of the Interpol Global Complex for Innovation in Singapore. INTERPOL | **An interior view of the Interpol Global Complex for Innovation's cyber fusion center is on display during the building's opening ceremony in Singapore in April 2015.** AFP/GETTY IMAGES all regions and nations are vulnerable to it, countries should be equipped to address cyber threats and develop cyber capabilities.

Interdependence is a defining characteristic of the digital world, meaning we are only as strong as our weakest link.

Why is international collaboration important in addressing the issue of cyber crime?

International collaboration is perhaps the single most important requirement for better cyber security, as criminality is evolving from the physical to the cybersphere. When it comes to cyber crime, the list of challenges facing communities and governments is daunting. Traditional methods are no longer adequate to combat the transnational nature of cyber crime, which now requires stronger international collaboration. There are very few crimes which do not rely in some way on the use of the Internet — for example to move money, for communication between criminals or for access to victims.

Police worldwide must collaborate with each other to effectively counter the threats of cyber crime, but they must also work with other actors from private industry to share knowledge and expertise. There are many benefits that law enforcement agencies can tap on from global partnerships and from a multistakeholder approach, together with the private sector and academia.

Has an increasing reliance on the Internet also created unexpected vulnerabilities?

The Internet has created a borderless society, providing unprecedented opportunities to generate wealth and stimulate economies. An increasing reliance on the Internet has also created unexpected vulnerabilities, with organized crime groups operating across the world able to coordinate complex attacks in a matter of minutes and with the click of a button.

The Internet has become a huge part of daily life for citizens around the world, be it for emails, social networking, financial transactions, filing tax returns and so on. Individuals and companies share more and more data with devices connected to the Internet. It is those data that can be analyzed, used and sold at very fast speeds. This mobility of data carries a risk because criminals look at it as a means of making profit.

More importantly, when governments become targets of cyber crime, consequences extend beyond just monetary losses: a major Internet disruption can also put our power grids, banking systems, energy pipelines and other critical systems at risk.

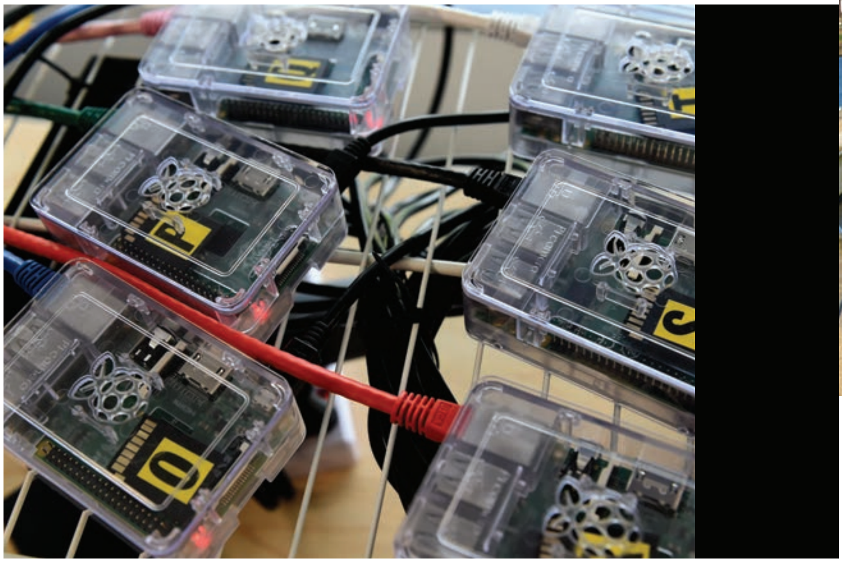
The Internet also provides terrorists with unprecedented situational awareness and tactical advantage over both the police and the government.

The cyber realm has a great destructive potential that makes us more vulnerable than ever before.

Is there a wide diversity between countries in the Indo-Asia-Pacific region regarding their capability to fight cyber crime?

We can observe a wide diversity in countries' capability to deal with cyber threats in every region. The existence of intraregional differences is not a characteristic unique to the Asia-Pacific region. This is why the baseline capability to address cyber crime needs to be enhanced globally.

This highlights the importance of international collaboration in addressing the issue of cyber crime, especially given the current pace of technological change.



Devices to simulate cyber crime are exhibited at the Interpol Global Complex for Innovation during its opening ceremony in Singapore in April 2015. AFP/GETTY IMAGES

What is the role of the Interpol Global Complex for Innovation in addressing cyber crime?

It was under Interpol's vision of connecting police for a safer world that the Interpol Global Complex for Innovation in Singapore was created to address the unprecedented challenges facing law enforcement in a digital age.

Interpol strives to assist its member countries in the fight against cyber crime in the framework of the IGCI, based on a multistakeholder approach. In this context, Interpol has the unique capability — at IGCI — to provide a global, neutral and secure platform for international law enforcement, private sector and academia to share information and work together against cyber crime in a collaborative environment.

IGCI's added value to our member countries is threefold. We provide law enforcement agencies worldwide with a global platform for operational support, global analysis for research-led innovation, and a center of excellence for capacity building and training.

Interpol stands ready to support its membership, paving the way for police to address 21st century crime threats. □

BELGIUM, NETHERLANDS

PEACEFUL Border Swap

THE ASSOCIATED PRESS

Throughout history, borders have caused unfathomable bloodshed, ageless feuds and decades-old legal disputes, which makes plans for a friendly exchange of land between the Netherlands and Belgium all the more remarkable.

The reason for such magnanimity? "Because it makes sense to do so," says Marcel Neven, the mayor of Vise, Belgium.

While Belgium will be losing a splendid piece of nature that juts into the Meuse River dividing the two nations, it will also unburden itself of a jurisdictional nightmare that developed over time as the river meandered to turn the portion of land belonging to Belgium — about 15 soccer fields worth — into a peninsula linked only to the Netherlands.

Preparatory work has been done, and the two nations' parliaments should be able to complete a deal sometime in 2016, Neven said, almost two centuries after the 1843 border posts were set. And all with a smile on everyone's face, even though Belgium will get only a tiny part around a lock that has been built to promote traffic between the two nations.

Belgian military historian Luc De Vos said that friendship between neighbors makes all the difference. "It is possible between Belgium and the Netherlands because these countries have a lot of ties for centuries and after the Second World War, territory was no longer that important," De Vos said. The Associated Press

BRAZIL

TRANSGENIC MOSQUITO to Join War on Zika Virus

A genetically modified mosquito has helped reduce the proliferation of mosquitoes spreading Zika and other dangerous viruses in Brazil, its developers said in January 2016.

The self-limiting strain of the Aedes aegypti mosquito was developed by Oxitec, the United Kingdom-subsidiary of U.S. synthetic biology company Intrexon. The male mosquitoes are modified so their offspring die before reaching adulthood and reproducing.

Oxitec, which produces the mosquitoes in Campinas, Brazil, announced it will build a second facility in nearby Piracicaba, Sao Paulo state.

THE ASSOCIATED PRESS

Oxitec said its proprietary OX513A mosquito succeeded in reducing wild larvae of the Aedes mosquito by 82 percent in a neighborhood of Piracicaba, where 25 million of the transgenic insects were released between April and November 2015. The Aedes vector also carries the dengue virus. Authorities reported a big drop in dengue cases in the area.

"This is a powerful and versatile tool that can dramatically reduce the levels of infestation, which is the core of Brazil's prevention strategy right now," said Glen Slade, Oxitec's business development director in Brazil.

Zika virus, first detected in Africa in the 1940s, was unknown in the Americas until 2015 when it appeared in northeastern Brazil. The virus has quickly spread through Latin America.

Brazilian health authorities have linked the Zika outbreak to a surge in the number of babies born with unusually small heads, a damaging neurological condition called microcephaly. There is no vaccine or treatment for Zika, which causes mild fever and rash. Reuters

Improving Transparency

THE CONTINUING NEED FOR ATTENTION TO GOOD GOVERNANCE AND ANTI-CORRUPTION

Takehiko Nakao

Asian Development Bank President Takehiko Nakao in Tokyo, Japan, in December 2015 REUTERS

Welcome to this year's celebration of International Anti-Corruption Day. International Anti-Corruption Day has been commemorated annually at the Asian Development Bank (ADB) every year since the United Nations Convention Against Corruption was passed in 2003.

Weak governance and corruption hurt the poor the most. Despite strong economic growth in recent years, the Asia and Pacific region remains home to half of the world's extreme poor when we use the new poverty threshold of U.S. $1.90 a day, defined as the minimum amount of income needed for life's necessities. These poor and vulnerable rely most heavily on public services and are often forced to pay bribes to receive those services. Indeed, studies have empirically shown that the portion of income lost to corruption is higher when the household is poor.

Good governance and rule of law contribute to a positive business environment, which in turn supports economic growth and poverty reduction.

ADB is working with our developing member countries (DMCs) to strengthen anti-corruption initiatives, improve regulatory frameworks for a better investment climate, and enhance the involvement of civil society in policy development and implementation.

I am pleased to note that the success rate of our public sector management projects improved from 44 percent in the 1990s to 67 percent in 2014, according to our independent evaluation department. Similarly, the number of projects involving governance and capacity development increased from 53 percent of the ADB-wide total in 2011-2013 to 60 percent in 2012-2014.

Partnerships at the international level are important to build meaningful and lasting change. Last year, ADB joined the Open Government Partnership to promote more transparent, accountable and responsive governments.

ADB also continues to jointly lead the largest network of anti-corruption authorities in Asia and the Pacific through the ADB/Organisation for Economic Co-operation and Development Anti-Corruption Initiative.

Internally, we recently introduced the staff instruction on integrity due diligence for sovereign operations and co-financing. This provides a process for assessing private sector participants in sovereign operations, such as financial intermediaries and co-financiers, to mitigate any governance and corruption risks in our projects.

Sound fiduciary management is indispensable to our procurement and disbursement procedures. While we are implementing the Procurement Reform 10-Point Action Plan to streamline processes and remove any unnecessary burden for implementing agencies and contractors, we have kept our strong anti-corruption and integrity requirements intact.

I would like to explain why fighting corruption and promoting good governance is more important than ever here at ADB.

First, we have raised our financing capacity to as much as U.S. $20 billion per year, or 50 percent more than the previous level. This was made possible by the merger of the Asian Development Fund lending operations with the ordinary capital resources balance sheet. We have also committed to doubling our annual climate financing to U.S. $6 billion by 2020. We must ensure that these additional monies are used effectively and sustainably, and are not diverted by fraud and corruption.

Second, in September 2015, world leaders came together to adopt 17 Sustainable Development Goals (SDGs). Goal 16 promotes just, peaceful and inclusive societies. Two of the targets under Goal 16 are to "substantially reduce corruption and bribery," and to "develop effective, accountable and transparent institutions at all levels."

Third, we are starting the preparation of ADB's new long-term strategy. In this new "Strategy 2030," to better use our expanded financial capacity and to align our operations with the SDGs, we will further mainstream governance, transparency and anti-corruption into our operations.

Fourth, we are now working on our new operational plan for capacity development for 2016 to 2020. This will provide more support to our DMCs to effectively deliver quality public services and enhance governance.

Fifth, as part of our reform to strengthen our expertise and knowledge, we set up eight thematic groups, including the governance thematic group, as well as seven sector groups. This governance thematic group will contribute to creating and sharing cutting-edge knowledge across departments and with our DMCs and ensure that governance remains an integral part of our operations.

All these initiatives are aimed at ensuring that our efforts regarding anti-corruption and governance count, and that they contribute to fulfilling ADB's goal to reduce poverty and improve the quality of life in our DMCs.

Today, I pledge to continue to do my part to fight corruption and promote good governance in ADB's operations. I ask all of you to do the same.

Takehiko Nakao, president of the Asian Development Bank, delivered this introductory speech at the International Anti-Corruption Day 2015 on December 9, 2015, at ADB headquarters, Manila, Philippines. It has been edited to fit this format.

Driverless Taxi Offers Glimpse of Future

A South Korean university is testing a sedan that can pick up and transport passengers without a human driver, giving a glimpse into the future of autonomous public transport.

Seo Seung-Woo, director of the Intelligent Vehicle IT Research Center at Seoul National University, said the university has been testing the driverless taxi to transport disabled students around campus.

The vehicle, called Snuber, had been navigating the 4,109-square-meter campus for six months without any accidents. It works in conjunction with a hailing app created by the university.

Companies around the world are betting that automated driving technology will transform public transportation.

However, it is not yet ready for use outside the relatively controlled campus environment.

“It will take a huge amount of time and effort,” said Seo. “We need more tests in real traffic conditions.”

He predicted that by early 2020, a driverless car will be running between toll gates on highways. A door-to-door pickup service using a self-driving car is likely by early 2030, he said. The Associated Press

THE ASSOCIATED PRESS

REUTERS

SMOG PRESENTS FORECASTING OPPORTUNITIES

Air pollution in China could be big business.

Two of the world’s largest technology firms, IBM and Microsoft, are vying to tap the nascent, fast-growing market for forecasting air quality in the world’s top carbon emitters.

Bouts of acrid smog enveloping Beijing prompted authorities in the Chinese capital to declare two unprecedented “red alerts” in January 2016, a warning to the city’s 22 million inhabitants that heavy pollution was expected for more than three days.

Such alerts rely on advances in pollution forecasting, increasingly important for Communist Party leaders as they seek improvements in monitoring and managing the country’s notorious smog in response to growing public awareness.

Official interest has also been boosted by China’s preparations to host the Winter Olympics in 2022, because Beijing’s smog is worse in the colder months.

“There is increasing attention to the air quality forecast service,” said Yu Zheng, a researcher at Microsoft. “More and more people care about this information technology.” A rudimentary forecast was pioneered by Dustin Grzesik, a geochemist and former Beijing resident who created Banshirne.com, a free website and smartphone app, in 2013 to predict clean air days using publicly available weather data on wind patterns.

“If you can predict the weather, it only takes a few more variables to predict air quality,” said Robert Rohde of Berkeley Earth, a U.S.-based nonprofit that maps China’s real-time air pollution. “Most of the time, pollutant emissions don’t vary very rapidly.”

Now, advances in “cognitive computing” — machines programmed to improve modeling on their own — allow more sophisticated forecasting software to provide predictions for the air quality index up to 10 days in advance using data on weather, traffic and land use, as well as real-time pollution levels from government monitoring stations and even social media posts.

Forecasts can help governments plan when to close schools and airports, restrict vehicles or postpone sporting events, and also decide which polluting factories to shut down temporarily. Reuters

Human imprint has thrust Earth into new geological epoch

REUTERS

The indelible imprint left by human beings on Earth has become so clear that it justifies naming a new geological epoch after mankind, experts revealed in January 2016.

The dawn of the "Anthropocene" would signal the end of the Holocene Epoch, considered to have begun 11,700 years ago at the end of the Ice Age. The new term, suggested in 2000, is based on the Greek word *anthropos*, meaning "man." "Human activity is leaving a pervasive and persistent signature on Earth," said a report in the journal *Science*.

"We are becoming a geological agent in ourselves," said Colin Waters of the British Geological Survey, who led an international team.

The start date could be around the mid-20th century, they wrote.

They said the Atomic Age, starting with a bomb test in New Mexico in the United States on July 16, 1945, and the postwar leap in mining, industry, farming and use of man-made materials such as concrete or plastics all left geological traces.

Concrete, invented by the Romans, was now so ubiquitous that it would amount to 1 kilogram for every square meter of the planet's surface if spread out evenly, they said.

Any formal recommendation to adopt the Anthropocene as a new geological epoch would require years of extra research, partly to pin down a start date, Waters said.

Some experts reckon the Anthropocene began with Europe's Industrial Revolution in the 18th century. Others would give it a more widespread origin, dating it from the spread of agriculture several thousand years ago.

"Any definition will inform the stories that we tell about human development," said Prof. Simon Lewis of University College London, who was not involved in the study. He favors 1610 as a start date, marking the spread of colonialism, disease and trade to the Americas from Europe.

Erle Ellis of the University of Maryland, a co-author of the study released January 14, 2016, said pinning down the Anthropocene would transform understanding of humanity's role on the planet.

He said it was a "challenge no smaller than a second Copernican revolution." In the 16th century, Nicolaus Copernicus helped show the Earth rotates around the sun.

ISTOCK

SNAKE WINDS

AROUND LUGGAGE CART AT BANGKOK AIRPORT

Bangkok's main international airport has issued an apology after a snake was found on a luggage cart in the arrival hall and startled passengers.

Suvarnabhumi International Airport, built on land previously known as "Cobra Swamp," said it would like to "apologize for the incident that frightened passengers" in a January 2016 statement.

Passengers spotted the snake coiled around the base of the trolley after a female traveler had loaded bags onto it and was preparing to leave the arrival hall, Thai media reported.

ALEXANDRE ROUX

"After being alerted, security officers captured the snake right away and no passengers were injured," Airports of Thailand said in a January 2016 statement that described the reptile as "a small baby snake" but did not identify the species.

Snake expert Thanaphong Tawan at a Bangkok snake farm run by the Thai Red Cross Society said the snake appeared to be a nonvenomous variety called Dryocalamus davisonii — commonly known as Blanford's bridle snake — based on a picture taken at the airport and published by Thai media.

The statement sought to "reassure that clear and strict measures have been imposed to prevent all poisonous animals from slipping into the airport's buildings" and said it was believed "the baby snake managed to slip into the airport because it was very small." The Associated Press

THE ASSOCIATED PRESS

TIGERS, PIRANHAS

MAY JOIN CROCODILE GUARDS AT INDONESIA JAIL

After sparking ridicule with a proposal to build a prison island for drug convicts surrounded by crocodiles, Indonesia's anti-drugs czar has now gone further — revealing in November 2015 he also wants tigers and piranhas as guards.

In an idea that seemed straight out of a James Bond film, Budi Waseso unveiled the prison island plan, explaining that crocodiles can't be bribed by drug traffickers seeking to escape from jail.

The head of the national anti-drugs agency embarked on a tour of the country to find "the most ferocious type of crocodile" to guard the jail, which is to be for drug convicts who have been sentenced to death.

He faced widespread mockery over the plan. But far from backing down, Waseso said he was considering the addition of man-eating piranhas and tigers as guards.

"It is also possible we may use piranhas, and because the number of personnel at the prison might not be enough, we can also use tigers," he said.

Indonesia already has some of the toughest anti-narcotics laws in the world, including death by firing squad for traffickers. It sparked an international uproar in April 2015 when it put to death seven foreign drug convicts.

President Joko Widodo has insisted that drug dealers must face death because the country is fighting a "national emergency" due to rising narcotics use.

"This is serious, this is not a joke," said anti-drugs agency spokesman Slamet Pribadi. "Drug trafficking is an extraordinary crime and therefore the fight must also be extraordinary. We cannot fight the usual way." The Associated Press

COW DUNG PATTIES

SELLING LIKE HOTCAKES ONLINE IN INDIA

THE ASSOCIATED PRESS

Like consumers around the globe, Indians are flocking to the online marketplace in droves these days. There's one unusual item flying off the virtual shelves: Online retailers are selling cow dung patties.

The patties – cow poop mixed with hay and dried in the sun, formed mainly by women in rural areas and used to fuel fires – have long been available in India's villages. But online retailers, including Amazon and eBay, are now reaching out to the country's ever-increasing urban population, feeding into the desire of older city folks to harken back to their childhoods in the village.

"Cow dung cakes have been listed by multiple sellers on our platform since October, and we have received several customer orders" since then, said Madhavi Kochar, an Amazon India spokeswoman.

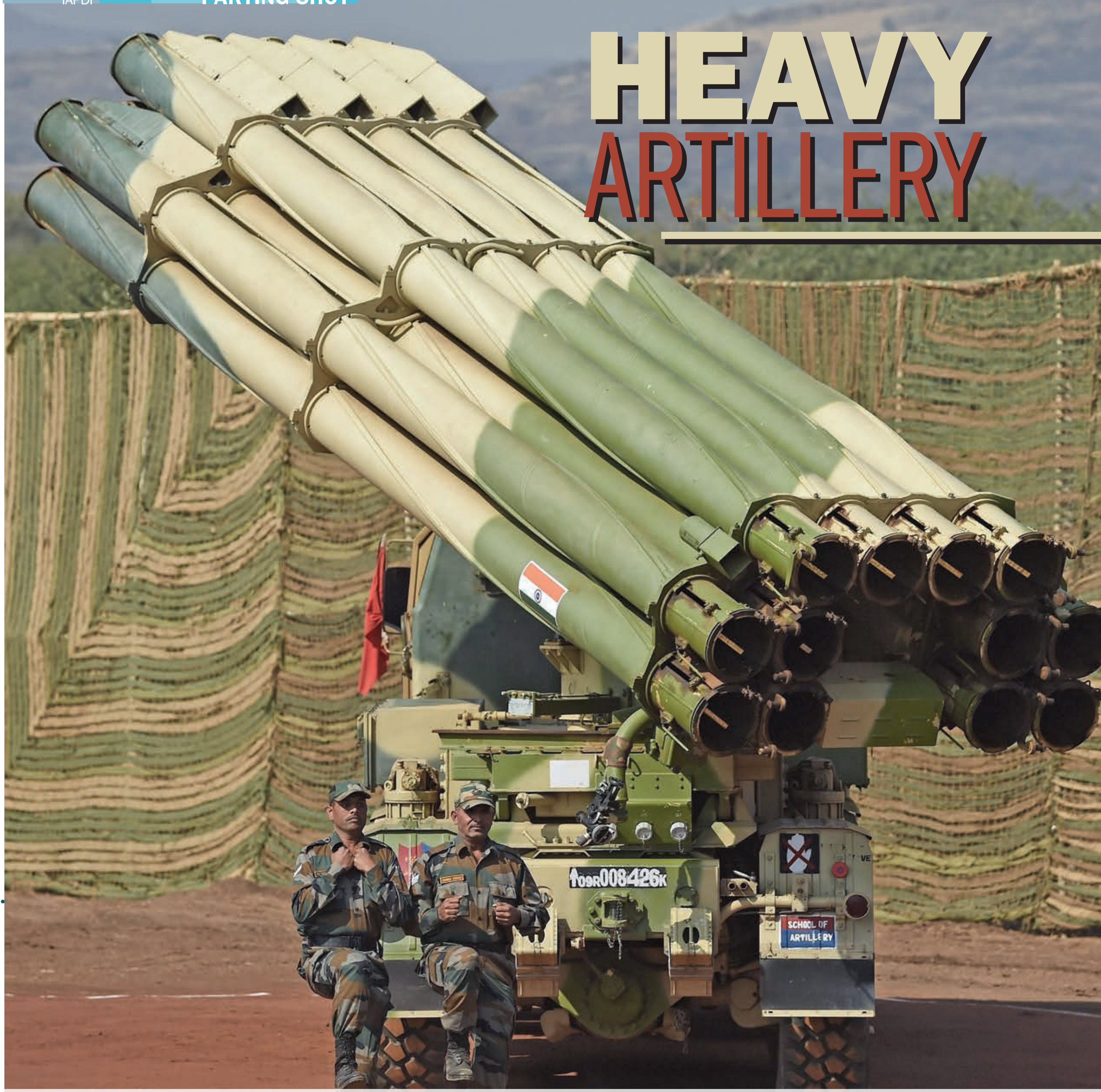
In India, where Hindus have long worshipped cows as sacred, cow dung cakes have been used for centuries for fires, whether for heating, cooking or Hindu rituals. Across rural India, piles of drying cow dung are ubiquitous.

Online retailers said people also bought the dung cakes to light fires marking the new year and for the winter festival known as Lohri, celebrated in northern India.

The cakes are sold in packages that contain two to eight pieces weighing 200 grams each. Prices range from 100 to 400 rupees (U.S. $1.50 to $6) per package.

The Associated Press

HEAVY ARTILLERY



Indian Army Soldiers take positions beside a Smerch multiple rocket launcher on January 11, 2016, during Exercise Sarvatra Prahar. It was conducted at the School of Artillery of the Indian Army in Devlali in the Nasik district of western Maharashtra state, nearly 200 kilometers northeast of Mumbai. The exercise included firepower demonstrations with artillery weapons of various calibers, ranging from mortars to Bofors 40 mm anti-aircraft guns. The Smerch features 12 tubes that fire 300 mm rockets. Developed in the 1980s, it remains one of the world's most lethal artillery rocket systems.

Photo By: **INDRANIL MUKHERJEE** | AFP/Getty Images

WOULD YOU LIKE YOUR FAVORITE PHOTO OF A RECENT EXERCISE OR PARTNERSHIP EVENT FEATURED IN PARTING SHOT? PLEASE SEND SUBMISSIONS TO **EDITOR@APDF-MAGAZINE.COM** FOR CONSIDERATION.

RELEVANT. REVEALING.
ONLINE.

www.iapdforum.com

NEW
CONTENT
POSTED
DAILY!

INDO-ASIA-PACIFIC DEFENSE
FORUM
HOME
FEATURES
DEPARTMENTS
CONTRIBUTORS
ABOUT US
ARCHIVES
SUBSCRIBE
SPECIAL REPORT
December 14, 2015
U.S. ponders China's commitment to anti-hacking deal
Targeting Terrorist ties to WMD
India: New Attack Submarine Debuts
Follow APDF
Subscribe to FORUM for FREE
North Korea talks
Select Menu
U.S. donated ship to bolster Philippine presence in South China Sea

FREE MAGAZINE SUBSCRIPTION

Indo-Asia-Pacific Defense FORUM is a military magazine provided FREE to those associated with security matters in the Indo-Asia-Pacific region.

FOR A FREE MAGAZINE SUBSCRIPTION:

www.iapdforum.com/subscribe

write: *IAPD FORUM* Program Manager
HQ USPACOM, Box 64013
Camp H.M. Smith, HI
96861-4013 USA

PLEASE INCLUDE:

- Name
- Occupation
- Title or rank
- Mailing address
- Email address

Join us on
Facebook.