INDO-PACIFIC DEFENSE FORUM

VOLUME 43, ISSUE 1, 2018

Envisioning the Future Battlespace

Technologies for Promoting Peace and Security

VOLUME 43, ISSUE 1

features

62

departments

ABOUT THE COVER: This illustration conjures the Soldier of tomorrow engaging in a push-button operation to suppress an enemy threat and reveal the complexity of the future battlespace.

FORUM ILLUSTRATION

U.S. PACIFIC COMMAND

Dear Readers,

Welcome to the first quarter edition of *Indo-Pacific Defense FORUM* in 2018. As you likely noticed, *FORUM*'s title has changed to more accurately reflect the region's evolution into a strategic system of interconnected economies, security agreements, and political organizations of a broader region.

The Indian and Pacific oceans now contain some of the fastest-growing economies in the world, linked by one of the world's busiest trade corridors. As the recent U.S. National Security Strategy points out, India is a leading global power and strong strategic and defense partner. Similarly, the Association of the Southeast Asian Nations (ASEAN) and Western Pacific Naval Symposium (WPNS) have expanded their influence beyond Asia as well. *FORUM* will continue to encourage Asia's growing influence in the world by providing a platform for military personnel of the Indo-Pacific region to address shared values, security concerns, and opportunities.

This current edition celebrates the importance of interoperability and innovation in future security. Rapidly evolving technologies, capabilities, and cyber realities are revolutionizing approaches to defense and security. Allies and partners must not only continuously adapt, but also cooperate now more than ever on new ways to counter the next generations of increasingly potent threats.

With the proliferation of technological breakthroughs and shifts comes increasing pressure for Indo-Pacific militaries to be interoperable among their own services and components and with allies and partner forces. To ensure security and prosperity, ally and partner nations must work together to develop defense technologies and processes to address continually evolving threats.

Recent social media manipulations, as well as malware and ransomware attacks, provide just a glimpse of the types of potentially nefarious applications of information tools and cyber capabilities to come. An article in this issue discusses cyber strategies, policies, and practices to address such threats. Yet, many more types of perils could result from the sweeping technological changes ahead. Allies and partner nations must use a collaborative, multilateral approach to fight adversaries across all domains given the range of unprecedented challenges in the future battlespace.

I hope you find this edition insightful and thought-provoking, and I welcome your comments. Please contact the *FORUM* staff at **ipdf@ipdefenseforum.com** with your perspectives.

All the best,

Harry Harris

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

IPD **FORUM**

Interoperability & Innovation
Volume 43, Issue 1, 2018

USPACOM LEADERSHIP

HARRY B. HARRIS, JR.
Admiral, USN
Commander

BRYAN P. FENTON
Lieutenant General, USA
Deputy Commander

KEVIN B. SCHNEIDER
Major General, USAF
Chief of Staff

PATRICK A. PIERCEY
Rear Admiral, USN
Director of Operations

PROGRAM OFFICER

NATHAN T. DIVELBESS
Lieutenant Colonel, USA
IPD FORUM Manager

CONTACT US

IPD **FORUM**

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

www.ipdefenseforum.com
email:
ipdf@ipdefenseforum.com

Indo-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-Pacific area. 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.) DAVID SHANAHAN serves on the faculty of the Daniel K. Inouye Asia Pacific Center for Security Studies. His interests include security sector development, emerging technology and security and complexity management. He served for 30 years in the U.S. Army in command and staff assignments, culminating as the chief of staff of U.S. Army Pacific (USARPAC). During his tenure, he oversaw the post-9/11 evolution of USARPAC's role in providing the base to U.S. Pacific Command Joint Task Force Homeland Defense. USARPAC's assigned forces also supported the global war on terrorism. Featured on Page 16

ERICA SULLIVAN is the program manager for Agile Space at Los Alamos National Laboratory's National Security and Defense Program Office. In that role, she works with multiple Department of Defense users to leverage the laboratory's CubeSat technology. She has also served other projects across multiple technical disciplines in global security. In 2015, the CubeSat project received the secretary of energy's Achievement Award. The project also won the Los Alamos' Distinguished Performance Award. Sullivan graduated summa cum laude with bachelor's degrees in economics and biology from Loyola Marymount University in 2000 and received her master's degree in business administration from San Diego State University in 2002. Featured on Page 22

SAROSH BANA is the executive editor of *Business India* in Mumbai, India. He writes extensively on defense and security, cyber security, space, energy, environment, foreign affairs, food and agriculture, shipping and ports, and urban and rural development. A Jefferson fellow of the East-West Center (EWC), Hawaii, he is treasurer/secretary on the Board of the EWC Association. Featured on Page 32

CMDR. TOM OGDEN is the director, Strategic Initiatives Group, and special assistant to commander, U.S. Pacific Fleet. He graduated from the U.S. Naval Academy and holds a master of arts in strategic studies from Georgetown University. Afloat, he served aboard USS Duluth, USS Paul Hamilton, USS Kidd, USS Mobile Bay, and most recently as executive officer and then commanding officer of USS Chung-Hoon, deploying to the Western Pacific Ocean. Ashore, he served at Joint Interagency Task Force South in Key West, Florida, leading the U.S. counter narcoterrorist operations in the Caribbean and Eastern Pacific oceans and Central and South America. Serving temporary duty at Commander Third Fleet, he assisted planning and developing its maritime operations center. Featured on Page 50

Join the Discussion

We want to hear from YOU!

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

Indo-Pacific Defense FORUM offers extensive content online, with new articles posted daily, at
www.ipdefenseforum.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

INDO-PACIFIC

REUTERS

TECH SOLUTIONS TO FIGHT MODERN SLAVERY

Indo-Pacific business leaders are working on recommendations to protect migrant workers from modern-day slavery and to ensure companies' supply sources are free from such unethical employment, according to Andrew Goledzinowski, Australia's ambassador for people smuggling and human trafficking.

One idea might be to create a regional website that rates employment recruiters — something already being done in Vietnam, Goledzinowski said. Another idea could be to designate a common telephone number as a regional hotline, like what the sportswear company Adidas provides to its factory workers in China and elsewhere. (Pictured: Burmese migrant workers sort shrimp at a seafood market in Mahachai, Thailand, in July 2017.)

Goledzinowski suggested the ideas at a forum of officials and business leaders from 45 Indo-Pacific countries and territories. Known as the Bali Process, the forum started in 2002 and also aims to ensure companies' materials are not tainted by unethical employment. Participants agreed at the meeting in Perth, Australia, to submit recommendations to governments in 2018. "We are hoping they will come up with the recommendations for how to better manage the recruitment of migrant workers and the protection of migrant workers," he said.

The measures also aim "to manage supply chain transparency so that businesses are not just responsible for what happens in their business, but also who they buy from."

Migrant workers often end up dealing with recruiters they do not know, being charged high fees and having their passports taken when they reach their destination, Goledzinowski said. "And very quickly you are trafficked, in fact, you are in debt bondage," he said, expressing hope that business leaders agree that "migrant workers should not have to pay for their own recruitment."

The recommendations will cover employment ethics, transparency standards and safeguards for victims and whistleblowers. "There's a lot that can be done which actually is quite easy, but it only works if everyone does it," Goledzinowski said. The Associated Press

SOUTH KOREA

CRYPTOCURRENCY TRADERS BANNED FROM USING ANONYMOUS BANK ACCOUNTS

South Korea banned the use of anonymous bank accounts in cryptocurrency trading beginning in late January 2018, regulators said in a widely telegraphed move designed to stop virtual coins from being used for money laundering and other crimes.

The measure comes on top of stepped-up efforts by Seoul to temper South Koreans' obsession with cryptocurrencies. Everyone from housewives to college students and office workers have rushed to trade the market despite warnings from global policymakers about investing in an asset that lacks broad regulatory oversight.

Policymakers around the world are calling for tougher, coordinated regulation of cryptocurrency trading. South Korea's chief financial regulator said in January 2018 the government may consider shutting down domestic virtual currency exchanges.

South Korea's presidential office has clarified that an outright ban on trading on the virtual currency exchanges is only one of the steps being considered and not a measure that has been finalized.

"The government is still discussing whether an outright ban is needed or not, internally," said a government official who declined to be named.

Government statements in January 2018 have underscored differences between the Justice Ministry, which has pushed for a more hard-line approach, and regulators who have shown a reluctance to enforce an outright ban.

As of January 30, 2018, cryptocurrency traders in South Korea were not allowed to make deposits into their virtual currency exchange wallets unless the names on their bank accounts match the account names in cryptocurrency exchanges, Kim Yong-beom, vice chairman of the Financial Services Commission, told a news conference in Seoul.

"Everyone knew this was coming, as the government already said they will enforce the real-name system before," said a local bitcoin investor who only agreed to be identified by his family name Ahn. "Rather, I can see this as a chance to go in, not out. I don't see any reason to take my money out." Reuters

bitcash
비트코인 (BTC) ₩ 18,800,000
대시 (DASH) ₩ 968,600
이더리움 클래식 (ETC) ₩ 32,370
이더리움 (ETH) ₩ 711,000
라이트코인 (LTC) ₩ 338,850
리플 (XRP)
비트코인캐시 (BCH) 1,734,000
모네로 (XMR) ₩ 336,500
제트캐시 (ZEC) ₩ 409,100
퀀텀 (QTU
294,700
비트코인 (BTC) ₩ 18,030,924
Exchange Rate: USD 1,090.8 EUR 1,282.73 CNY 164.73

SINGAPORE

THE ASSOCIATED PRESS

First Woman PRESIDENT

Singaporeans declared Halimah Yacob, a former speaker of Parliament, as their first female president in September 2017, after the Returning Officer, who oversees presidential elections, announced she was the sole candidate to qualify for the contest.

Aiming to strengthen a sense of inclusivity in the multicultural city-state, Singapore had decreed the presidency, a largely ceremonial post, would be reserved for candidates from the minority Malay community this time.

"Although this is a reserved election, I'm not a reserved president," Halimah said in a speech at the elections department office. "I'm a president for everyone."

Halimah's experience as house speaker automatically qualified her under the nomination rules.

The last Malay to hold the presidency was Yusof Ishak, whose image adorns the country's banknotes.

Yusof was president between 1965 and 1970, the first years of Singapore's independence following a short-lived union with neighboring Malaysia, but executive power lay with Lee Kuan Yew, the country's first prime minister.

The separation of Singapore from Malaysia gave ethnic Malays a clear majority in Malaysia, while ethnic Chinese formed the majority in independent Singapore. Reuters

JAPAN

Fresh start *for an* old market

Tokyo's famed Tsukiji fish market — the world's biggest — will be moved to a new location, the city's top official confirmed in June 2017, after months of delays over concerns about toxic contamination at the new site.

City Gov. Yuriko Koike added a new element to the long-standing relocation plan, saying the current site would eventually be redeveloped to capitalize on Tsukiji's globally recognized brand.

The present location, a popular tourist attraction that hosts an early morning tuna auction, is earmarked for the Tokyo 2020 Olympics.

"After that, we will turn it into a new market with a food theme park," Koike told reporters, adding that redevelopment would happen within five years.

"I think it's wisest to use both Toyosu and Tsukiji," she said, referring to the new location.

The government initially planned to sell all or part of the current site near the upscale Ginza shopping district. Koike, a former TV anchorwoman elected in 2016 as Tokyo's first female governor, did not say when the main market would move to Toyosu, a former gas plant.

"We'll need to discuss detailed schedules with the people involved," she said.

The top-selling *Yomiuri* newspaper reported that the governor was mulling the possibility of opening the new site in May 2018.

Plans to uproot the more than 80-year-old market have been in the works for years, with advocates citing the need for upgraded technology as they pointed to Tsukiji's antiquated refrigeration systems.

Agence France-Presse

THE ASSOCIATED PRESS

Philippines, Malaysia, Indonesia

EYE JOINT COUNTERTERRORISM TASK FORCE

REUTERS

Philippine President Rodrigo Duterte will discuss with Indonesia and Malaysia the possibility of creating a task force to combat Islamic State-inspired militancy, he said in early September 2017.

Duterte expressed willingness to open the borders to Indonesian and Malaysian security forces hunting Islamist fighters. He plans to meet with Indonesian President Joko Widodo and Malaysian Prime Minster Najib Razak on the matter.

"We have agreed that we will talk, the three of us. We are just waiting for the right time," he told reporters.

Asked what could be discussed, he said: "In all probability, it will be a joint ... task force. And I will open my borders to the Malaysian authorities and Indonesian authorities. They'll be given access."

Southeast Asian nations have agreed to use spy planes and drones to stem the movement of militants across their borders, as concerns rise over the growing clout of the Islamic State in the region.

In June 2017, foreign ministers and defense officials of the three neighboring countries agreed to pool intelligence, track communications and crack down on the flow of arms, fighters and money.

Malaysian Foreign Minister Anifah Aman said in June 2017 that extremism needed an immediate response and constant engagement among the three countries that must be as a "cohesive unit."

"This means our enforcement agencies must constantly engage with one another, not only in intelligence sharing but new active and innovative measures," he said during the Trilateral Security Meeting in suburban Pasay city, southeast of Manila, Philippines.

Indonesia, Malaysia and the Philippines have also launched joint patrols to control militant movements across their archipelagic region. In November 2016, the Philippines agreed to allow Malaysia and Indonesia to carry out "hot pursuits" in its territorial waters to tackle kidnappings and piracy by Islamist Abu Sayyaf Group rebels.

Duterte indicated in September 2017 that the meeting with Widodo and Najib could take place after the siege of Marawi city in southern Philippines involving militants loyal to Islamic State was resolved.

In October 2017 the Armed Forces of the Philippines liberated Marawi, declaring an end to five months of fierce urban warfare and to the Philippines' biggest security crisis in years. At that time, the death toll exceeded 1,100, including 920 militants and their leader, Isnilon Hapilon, a DNA analysis confirmed.

Defense Secretary Delfin Lorenzana said in late October the military terminated combat operations after troops prevailed in the last stand against gunmen who held their positions inside several buildings in the heart of Marawi.

"There are no more militants in Marawi," he told reporters on the sidelines of a meeting of regional defense ministers.

Military spokesman Maj. Gen. Restituto Padilla confirmed there was still gunfire in the city, but there were "no more terrorists" in Marawi. He did not elaborate.

The defense secretary later said that the military had crushed "the most serious attempt to export violent extremism and radicalism in the Philippines and in the region."

"We have contributed to preventing its spread in Asia and gave our share to maintaining global peace, stability and security," he added.

Indonesian Sailors participate in the launch of coordinated patrols in June 2017 among Malaysia, Indonesia and the Philippines in the Tarakan sea off Indonesia to control militant movements across their archipelagic region. REUTERS

FAR LEFT: Indonesian National Police Chief Tito Karnavian, from left, Philippine National Police Chief Ronald Dela Rosa and Royal Malaysian Police Inspector General Khalid Abu Bakar link arms before the Trilateral Security Meeting in Pasay city, southeast of Manila, Philippines, in June 2017.

THE ASSOCIATED PRESS

Philippine Defense Secretary Delfin Lorenzana, center, inspects a high-powered firearm seized from one of the various hideouts of Islamist militants during his visit at a military camp in Marawi city.

REUTERS

A Thai Soldier is lowered from a helicopter to distribute supplies to a rescue boat in the Chaiya district of Thailand's southern province of Surat Thani in January 2017. AFP/GETTY IMAGES

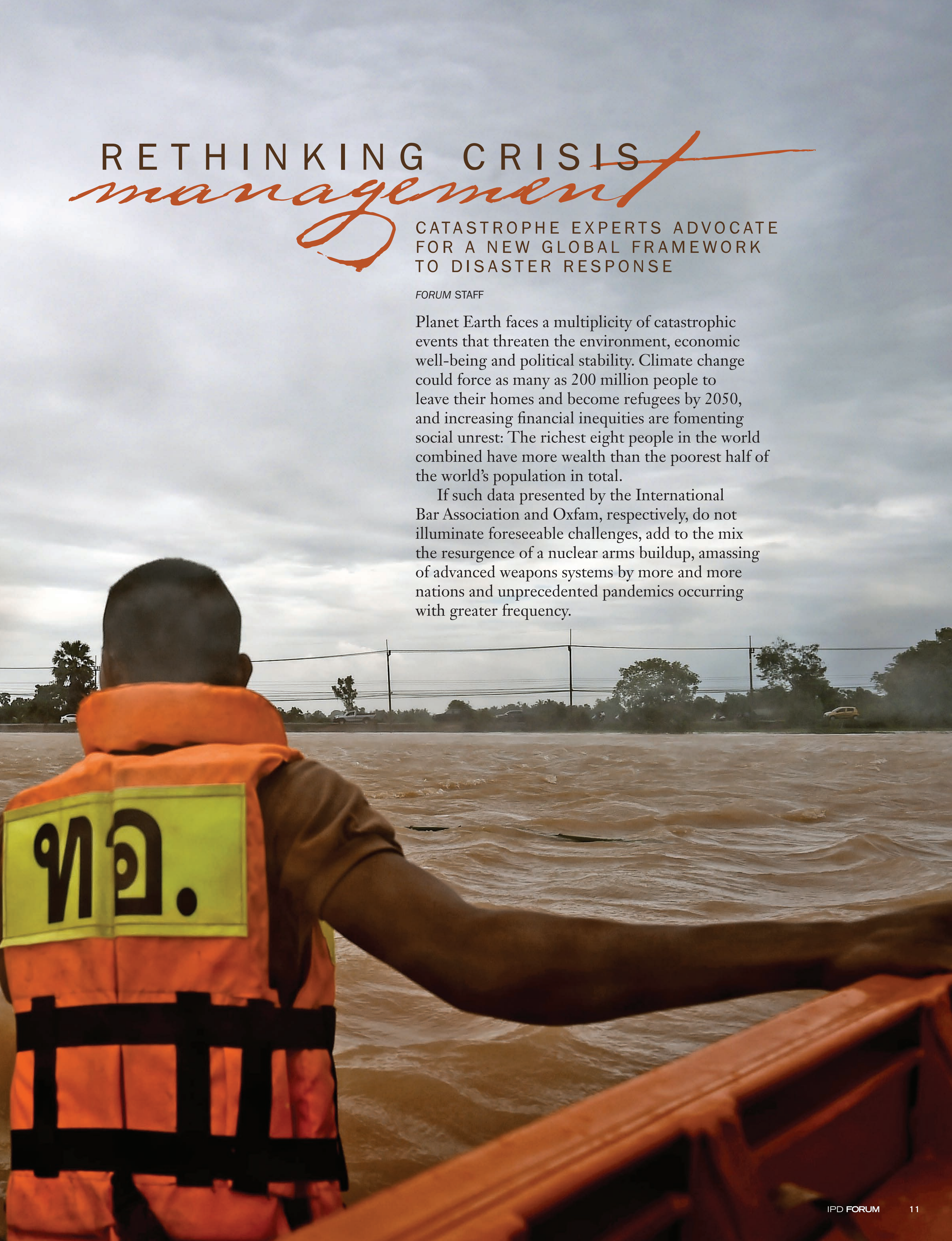
RETHINKING CRISIS *management*

CATASTROPHE EXPERTS ADVOCATE FOR A NEW GLOBAL FRAMEWORK TO DISASTER RESPONSE

FORUM STAFF

Planet Earth faces a multiplicity of catastrophic events that threaten the environment, economic well-being and political stability. Climate change could force as many as 200 million people to leave their homes and become refugees by 2050, and increasing financial inequities are fomenting social unrest: The richest eight people in the world combined have more wealth than the poorest half of the world's population in total.

If such data presented by the International Bar Association and Oxfam, respectively, do not illuminate foreseeable challenges, add to the mix the resurgence of a nuclear arms buildup, amassing of advanced weapons systems by more and more nations and unprecedented pandemics occurring with greater frequency.



These global risks continue to evolve, but crisis-management experts say many of the institutions and strategies used to address these challenges have remained stagnant. Do organizations like the United Nations and World Bank — along with governments and militaries — have updated expertise and resources to meet modern-day challenges? Are there different organizations or institutions better suited for the problem-solving skills needed today?

Members of the crisis management community say such questions deserve greater attention.

"The problem today is that the challenges we have are global … and that we've actually run out of systems to control them," Mats Andersson, vice chairman of the Global Challenges Foundation, based in Sweden, said in February 2017. He was at the Brookings Institution in Washington, D.C., where he joined a panel discussion on managing global risks. "We need to find new ways. We're trying today to fix the problems of today with the toolbox from yesterday. We need to find a new toolbox that can actually work to mitigate the risks that we have."

Founded in 2012, the Global Challenges Foundation aims to "incite deeper understanding of the most pressing global risks to humanity," according to its mission. It also seeks to accelerate new ways to tackle them. To that end, the foundation launched a competition to find new models of global cooperation capable of handling global risks. The competition has generated more than 4,000 entrants from participants in 150 countries. The winner will receive U.S. $5 million in prizes for the best ideas to "re-envision" global governance for the 21st century.

"Increasingly, we can be said to be living in a global community. This means that the inhabitants of every individual country, through their behaviors and decisions, can have a major impact on the essential interests of the inhabitants of all other countries," Laszlo Szombatfalvy, founder of the Global Challenges Foundation, wrote in a letter to competition participants. "Our current international system — including but not limited to the United Nations — was set up in another era, following the Second World War. It is no longer fit for purpose to deal with 21st century risks that can affect people anywhere in the world."

Szombatfalvy said crisis managers urgently need fresh thinking to address the scale and gravity of today's global challenges, "which have outgrown the present system's ability to handle them."

Soldiers from the Chinese People's Liberation Army (PLA) and the U.S. Army Pacific carry an injured person from a boat in the U.S.-China Disaster Management Exchange drill at a base in Kunming, southwestern China's Yunnan province.

THE ASSOCIATED PRESS

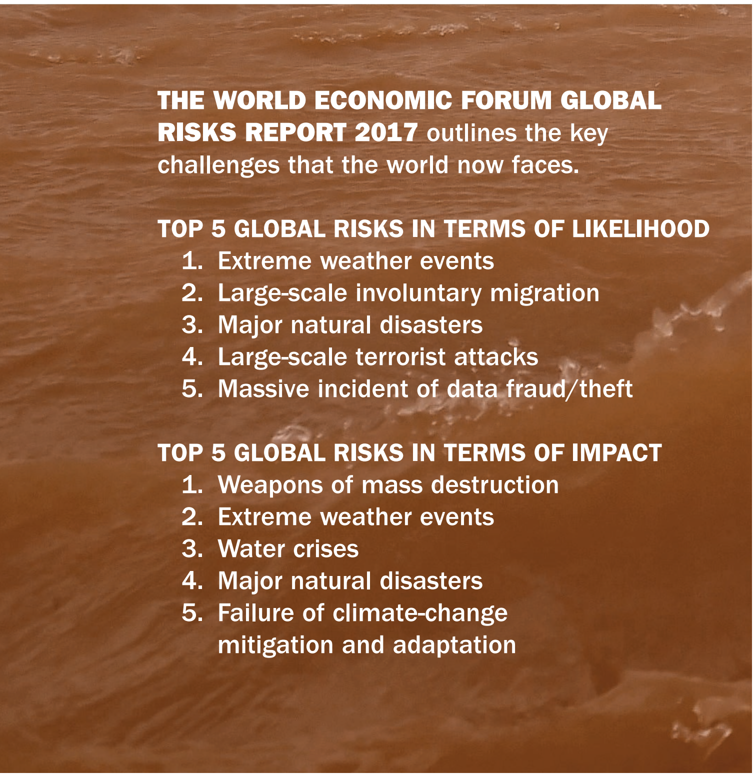
FRESH PERSPECTIVES, SUSTAINED COOPERATION

Kemal Dervis, vice president and director of the Global Economy and Development program at Brookings, agreed with the notion that governments, legacy institutions and militaries must take a fresh look at whether their strategies to address challenges have evolved with the challenges themselves.

"The toolbox largely that we have today is largely coming from the catastrophe of World War II," Dervis said.

He promoted the idea that governments should create decision-making authority during disaster response or crisis as close to the local level as possible. That doesn't require a drastic shift in the multiple layers of governance, he said. Rather, create an additional level that gives citizens and locals greater oversight to deal directly, and more quickly, with a disaster affecting their neighborhood.

Dervis also favored a military and security community that operates separately from economic, social and environmental affairs for crisis management. A separate military and security community could boost the military's autonomy to implement crisis prevention strategies.



THE WORLD ECONOMIC FORUM GLOBAL RISKS REPORT 2017 outlines the key challenges that the world now faces.

TOP 5 GLOBAL RISKS IN TERMS OF LIKELIHOOD

1. Extreme weather events
2. Large-scale involuntary migration
3. Major natural disasters
4. Large-scale terrorist attacks
5. Massive incident of data fraud/theft

TOP 5 GLOBAL RISKS IN TERMS OF IMPACT

1. Weapons of mass destruction
2. Extreme weather events
3. Water crises
4. Major natural disasters
5. Failure of climate-change mitigation and adaptation

Separation for decision-making purposes, however, does not negate integration among every disaster response component. Cooperation must always remain and has, in fact, increasingly expanded among civil-military alliances.

"Vulnerable countries have begun to integrate disaster risk management policies and practices into their overall civilian governance framework to enhance unity of effort at the local, national, and international level," according to the 2015 "Advances in Civil Military Coordination in Catastrophes" report by the U.S. Department of Defense Center for Excellence in Disaster Management and Humanitarian Assistance (CFE-DM).

The center's report drew lessons learned from Super Typhoon Haiyan, also known as Yolanda, which struck the Caroline Islands, the Philippines, South China and Vietnam in November 2013. In the Philippines the storm brought strong winds and heavy rains that resulted in flooding, landslides and widespread damage. From that disaster, the CFE-DM identified three best practices:

- Create a commonly understood "end-to-end warning system" that prepares a nation for crises.
- Establish a bilateral commitment that responders execute multilaterally on the ground through a multinational coordination center and promotes optimal civilian use of foreign defense assets.
- Maintain close coordination with the government, military and private sector so civilian responders successfully multiply a nation's surge capacity to meet the life-saving needs of the affected population.

THE IMPORTANCE OF HUMAN CAPITAL

Keeping the emphasis on the people involved in the process, and not the organization, represents an important piece of the paradigm shift for Maria Ivanova, associate professor of global governance at the John W. McCormack Graduate School of Policy and Global Studies at the University of Massachusetts Boston, where she co-directs the Center for Governance and Sustainability.

She views the crisis management system as "fragmented." Governments and organizations should evaluate whether they have procedures that deploy multiple actors, or multiplicity in action, she said.

"That requires us to really look into these institutions, to look into the various levels of governance, see how they function, and remember what is the goal," Ivanova said during the Brookings Institution panel on crisis management. "Where do we want to get? And ultimately, I think we will have functioning institutions and functioning governments when we have the right people in the right places."

It's not enough to simply hire an expert. That individual must have a clear directive of their role within an institution or government.

"What does it mean to actually make that institution functional? What kind of individuals do you need there and [on] these various levels of governance? And I would say they have to be committed, they have to be able, and they have to be inspired," Ivanova said.

She acknowledged that inspiring people to talk about global catastrophic risks can prove difficult.

"Yet, we've seen that happen with the climate

Indonesian rescuers recover the body of a woman after a wall of mud slammed into houses following heavy rainfall in Ponorogo district, East Java, in April 2017. AFP/GETTY IMAGES

debate, that it changed from a narrative of sacrifice to a narrative of opportunity," Ivanova said. "And that's when [the] Paris Agreement came about, when people could see that 'I could be part of a different economy. I can contribute to a different outcome in the world.' And that's when people become engaged and when individuals become active and productive elements in institutions."

IMPLEMENTING A VISION FOR CHANGE

"In the absence of crisis, change tends to be incremental at best," Stewart M. Patrick, senior fellow and director of the program on International Institutions and Global Governance at the Council on Foreign Relations, said during the Brookings discussion. "Think of it as sort of natural selection as opposed to punctuated equilibrium in the evolutionary field. You know, the irony is that institutions are really bad at either predicting, anticipating and preparing themselves for catastrophic risks, but what happens, ironically, is that catastrophes are actually one of the only things that actually creates some institutions."

The Association of Southeast Asian Nations (ASEAN) has worked hard to avoid falling into that category through the creation of the ASEAN Vision 2025 on Disaster Management. It identifies key areas for making the ASEAN Agreement on Disaster Management and Emergency Response (AADMER) a people-centered, people-oriented, financially sustainable and networked approach by 2025.

"While ASEAN has progressed in terms of cooperation and collaboration, it is evident that the mechanisms to respond to these new

challenges need to be further developed," according to Vision 2025.

The World Humanitarian Summit Synthesis Report has outlined five key areas of action to future humanitarian action that ASEAN has adopted as part of its Vision 2025: dignity, safety, resilience, partnership and finance.

Here's how the report elaborated on each point:

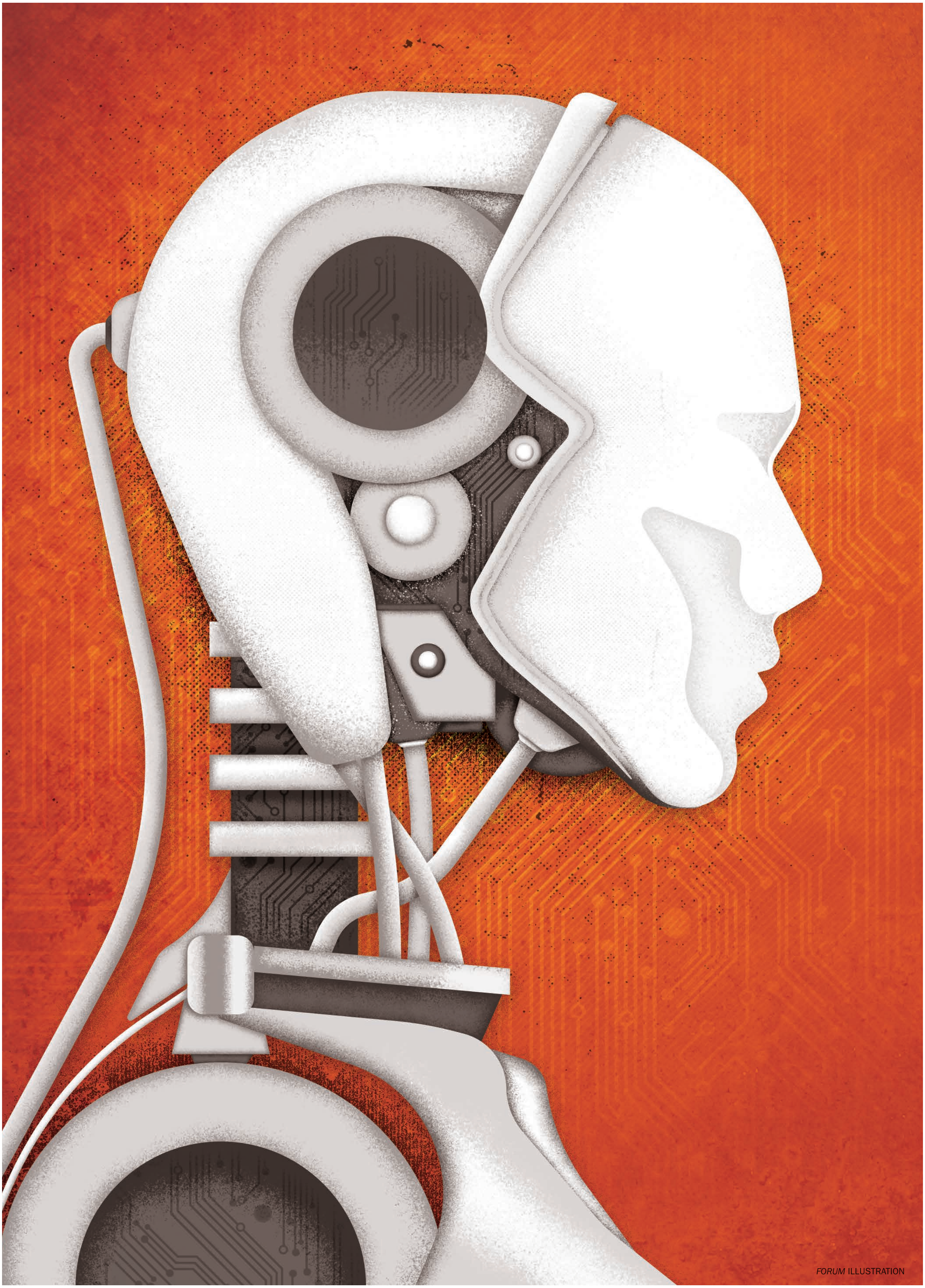
- **Dignity**
  "ASEAN will need to further develop and apply its people-centered approach as a main priority. With this approach at the center of the humanitarian initiative will ensure gender equality and empowerment for women, girls, the youth and children so that they can act as agents of their own response."
- **Safety**
  "ASEAN and the future implementation of AADMER need to ensure that there are mechanisms to enable protection and assistance for all, especially those most vulnerable. Protection should be a priority for all ASEAN responders at all times during humanitarian events as they themselves act as advocates for international law and peace."
- **Reslience**
  "Strengthening resilience requires ASEAN to shift their focus from managing crises to managing risks so that their constituents will be better prepared for what lies ahead of them. As such, achieving resilience within ASEAN requires the building of capacities of member states and within them in communities to reduce exposures and vulnerabilities."
- **Partnership**
  "Through partnerships, the future AADMER work program should actively engage the other sectors of work such as but not limited to: the private and public sectors to leverage their capabilities. In addressing needs of the future humanitarian landscape, a collaborative effort by all parties is needed to provide for the most comprehensive and holistic response to those affected."
- **Finance**
  "ASEAN, through AADMER, should look at alternative sourcing of funding and not rely solely on donations from member states. Tapping new sources at local, regional, national and at international levels will be key to providing adequate support for disaster-affected population as well."

NEVER UNDERESTIMATE THE RISKS

Szombatfalvy, creator of the Global Challenges Foundation, reminds crisis management teams that major challenges are interconnected and impact each other positively or negatively.

"They [major crisis challenges] represent the greatest threat to humanity today and should be at the top of the international political agenda," Szombatfalvy said. "In my view, political and business leaders, influenced as they are by short-term and self-interested concerns, are gravely underestimating them. These risks demand urgent global collective actions in order to safeguard future generations."

The greatest threats faced today transcend national boundaries, Szombatfalvy said. "They therefore need to be addressed jointly by all countries based on an increased realization of our mutual dependence." □



FORUM ILLUSTRATION

SECURITY INNOVATION

Enhanced governance of emerging technologies needed to promote peace and stability

COL. (RET.) DAVID SHANAHAN
DANIEL K. INOUYE ASIA-PACIFIC CENTER FOR SECURITY STUDIES

Many technology experts predict the next decade will offer cascades of technologically enabled advances. Lowered barriers for new and innovative ways of using old technologies are already offering unprecedented asymmetrical offset opportunities to regional partners, rivals and nonstate actors to enable achievement of security and development goals and allow some actors to pervert them for nefarious purposes.

Many national and multinational governance mechanisms and processes, conceived in an era when the technology governance could be considered discretely within defined technology areas, cannot cope with the pace and the cross-feeding nature of today's technology environment. Mechanisms and processes must evolve to increasingly coordinate and collaborate between disparate fields to enable opportunities and to define and respond to threats the emerging technology environment will inevitably pose.

Countless advances could play out in fields such as information, artificial intelligence (AI), energy, materials manufacturing, biotechnologies and advanced human health, as future forecasters detail in reports such as the "Paradox of Progress" issued by the Office of the Director of National Intelligence in the United States. Technologies will be increasingly fused and distinctions blurred between the physical, digital and biological spheres, as Klaus Schwab of the World Economic Forum describes in his book *The Fourth Industrial Revolution*.

The allure of the world that these advances promise is richly described by such entrepreneur technologists as Singularity University co-founder Peter Diamandis, who has sponsored SpaceX, Tesla's Elon Musk, and the XPrize and co-authored the book *Abundance: The Future Is Better Than You Think*. The world they portray is a hope-filled utopia in which the technology-empowered capacity to fulfill human needs will reliably outpace problems and challenges.

The challenge of these rosy perspectives is that, for the organizations and people responsible for ensuring national and regional security, they offer little comfort or insight for engaging with the potential issues and problems created or exacerbated by the advances.

CHALLENGES OF DISRUPTION

Technology, from the wedge to the smartphone, has propelled and disrupted the sweep of human history. Novel today is the rapid pace from inception to pervasive impact that characterizes many elements of the current technological revolution.

The exponential growth of computational power per unit cost, as expressed by the 52-year-old Moore's law, has been a key accelerant of the pace of innovation. Whereas past exponential growth appears more horizontal when at the knee in the curve, the future looks increasingly vertical. The opportunity for effective policy and governance interventions is before technologies achieve takeoff on the curve.

Anticipating when, where and how technologies will alter the dynamics of economies, social structures and security is a tough task corresponding to the complex nature of the underlying systems they affect. This inherent complexity stymies attempts to harness technologies to defined ends, suggesting that the best the world can hope to accomplish is to forge accepted rule sets that mark boundaries and how players are required to interact.

Governance processes that enable the establishment of those parameters are under stress and in many cases, are inadequate to face demands that emerging technological advances will impose.

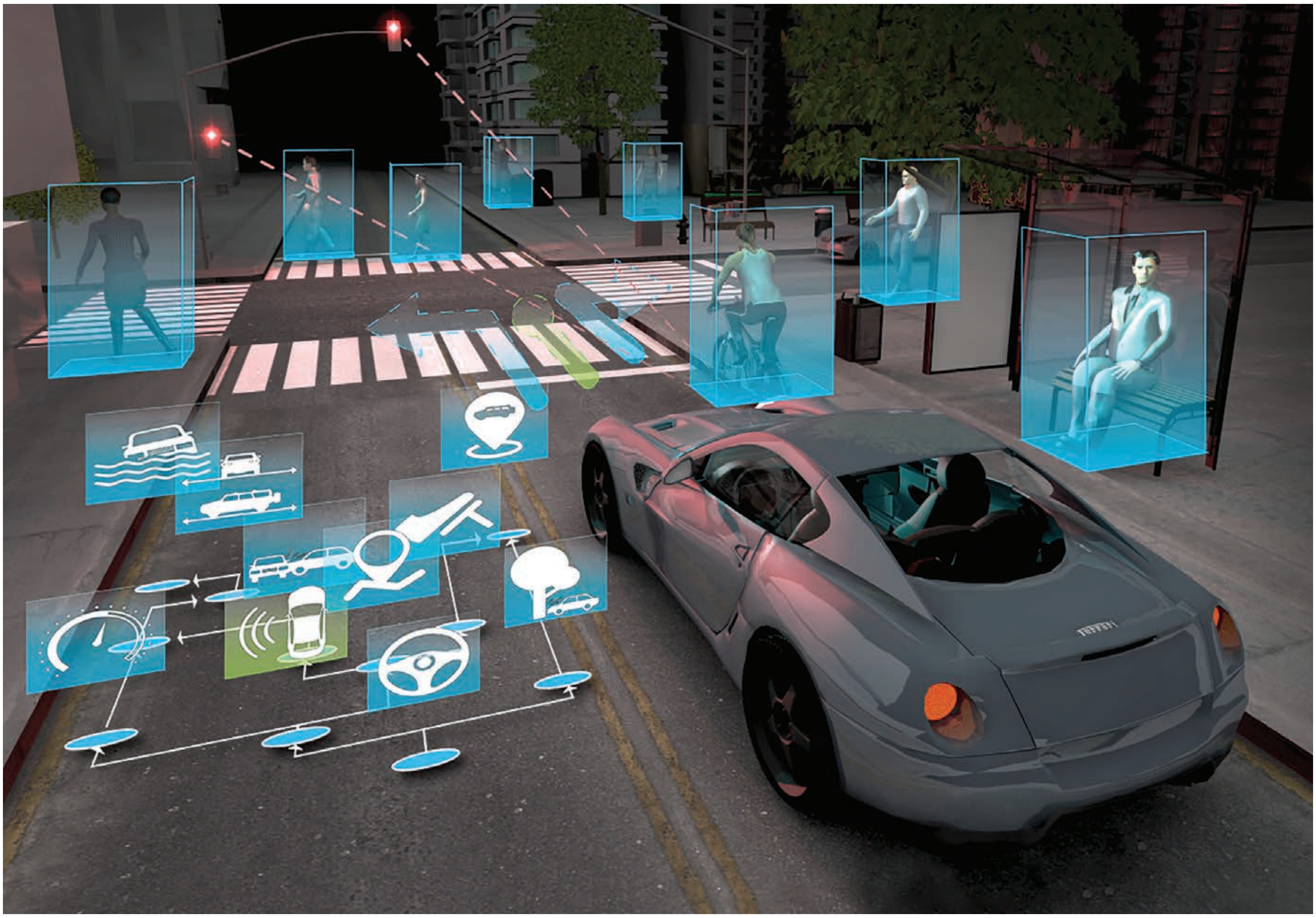
Technological development and deployment increase as equipment, techniques and procedures proliferate widely and combine to achieve new discoveries. Many highly anticipated predictions — such as prevalent nuclear fusion energy, beam weapons or personal flying machines — have not arrived, long after first promised. Some scoff at the idea of the effect of technology's exponential pace because of these disappointments.

Other fields, though, have shown arguably more impactful advances that have outpaced even what the most optimistic experts initially predicted. Illustrative of the latter are such trends as exponential advances in biotechnologies, information communications technologies (ICT) and AI. Taken together, such technologies hold promise to disruptively alter the near-term future and provide existential challenge to mankind's role and purpose in the longer term.

A dramatically advancing gene-manipulation technology (CRISPR) offers an example of the potential disruptive power of emergent converging technologies. Over the past five years with the help of advances in computational power and genomics, this technology has opened the door to staggering breakthroughs in the capacity for humans to design and manage the basic building blocks of life. Genomics pertains to the study of the complete set of genetic material within an organism and how it is structured, functions and evolves. The potential to use technologically available modifications to the human "germline" for disease prevention yields to a slippery slope with ill-defined and even less enforceable redlines.

For example, biohacking, or exploiting genetic material experimentally while disregarding ethical standards and even existing laws, has occurred worldwide, especially in the West. Lately, however, enthusiasm for biohacking is growing significantly in the Indo-Pacific, catalyzed by such organizations as the Singapore-based Biochin.Asia and Hong Kong-based Biohacking Asia. It's concerning that ever-lowering entry barriers for dual-use technologies in the field of bioengineering allow unregulated or monitored amateur "biohackers" to not only manipulate but also create beneficial and potentially deadly life-forms. Little imagination is necessary to

> "*Today, thanks to the internet and social media, the manipulation of our perception of the world is taking place on previously unimaginable scales of time, space and intentionality.*"
>
> — RAND WALTZMAN,
> RAND CORPORATION



DARPA

The U.S. Defense Advanced Projects Research Agency (DARPA) is developing machines that apply information from new situations to become better and more reliable.

predict the woeful impact of their use by bad actors.

POLICY CONVERGENCE

Another example of disruptive technologies converging to produce enormous impacts are in ICT and AI, which together are critical enablers that will influence nearly every industry. Increasingly capable AI algorithms coupled with big data have the promise to move the world from analytics that describe or predict future systems' behavior to ones that are able to prescribe it. This capacity will be readily usable in benign and nefarious ways.

For example, Richard Thaler and Cass Sunstein in their 2008 book *Nudge: Improving Decisions about Health, Wealth and Happiness*, describe how governments might steer citizens toward such actions as healthier or more environmentally friendly behavior by means of a "nudge" — or promoting a preferred behavior by creating a choice architecture based on insights about biases and habits instead of implementing a regulation or punishment for an undesired behavior. Some, however, might construe such nudges as a contemporary form of paternalism. A caring government could make sure that citizens do things that it considers right for society and national interests. Already, new commerce and social systems using big data and AI reinforce pre-existing wants rather than intriguing users to discover new ideas. They funnel users into increasingly customized silos in which they are already comfortable, echo chambers in many cases. This is troubling. What happens, however, when the confluence of AI and ICT enables bad and/or hidden actors to nudge citizens to take in only certain information feeds, to impugn correct information or to give credibility to false information? This is scary, and it is playing out in national, regional and world affairs daily.

"Today, thanks to the internet and social media, the manipulation of our perception of the world is taking place on previously unimaginable scales of time, space and intentionality," stated Rand Corp.'s Rand Waltzman in U.S. Senate testimony on April 27, 2017, titled "The Weaponization of Information." "We have entered the age of mass customization of messaging, narrative and persuasion. We need a strategy to counter a constantly changing set of adversaries large and small."

The claims and counterclaims of manipulation in recent elections reveal the scope of the challenges. For example, existing AI software can create incredibly real-looking images and video for disinformation campaigns, according to a recent study by University of Washington researchers. Unchecked, such developments in AI offer adversaries the ability to readily manipulate information for bad purpose.

"Deep learning" algorithmic models increasingly form the decision-making processes of autonomous systems being placed into automotive, financial, medical and military systems. These models, though, are even now programming themselves in ways the engineers who built them cannot explain. This dilemma will only increase as AI becomes more powerful and ubiquitous. As Tommi Jaakkola, a professor at the Massachusetts Institute of Technology who works on applications of machine learning, observed, "Whether it's an investment decision, medical decision or military decision, you don't want to just rely on a 'black box' method" in explaining how it was made.

The scenarios anticipated in these examples, as well as a host of other fields experiencing simultaneous technology advances, are daunting. The disruptive changes are so profound that, from the perspective of human history, many argue there has never been a time of greater promise or potential peril. These scenarios challenge the international community to foster exploiting these technologies' opportunities, as well as mitigate their many embedded risks. Decision-makers, however, are too often caught in traditional, linear (and nondisruptive) thinking or are too consumed by immediate concerns to think strategically about the forces of disruption and innovation shaping the future.

This has sparked urgent calls to increase capacity to govern the technological onslaught through policy, processes and mechanisms to ensure that nations feed, harness and guide the technological horses that will pull the international community on the wild ride into tomorrow. Perhaps foremost among these clarion voices is Azhar Zia-ur-Rehman, whose recent book *Technology Governance – Concepts and Practices* serves as the recognized reference for the concept of technology governance.

Many helpful steps are emerging. The Association of Southeast Asian Nations (ASEAN) among other regional organizations has focused on technology governance in the cyber area, and in 2016 it initiated a ministerial conference on cyber security.

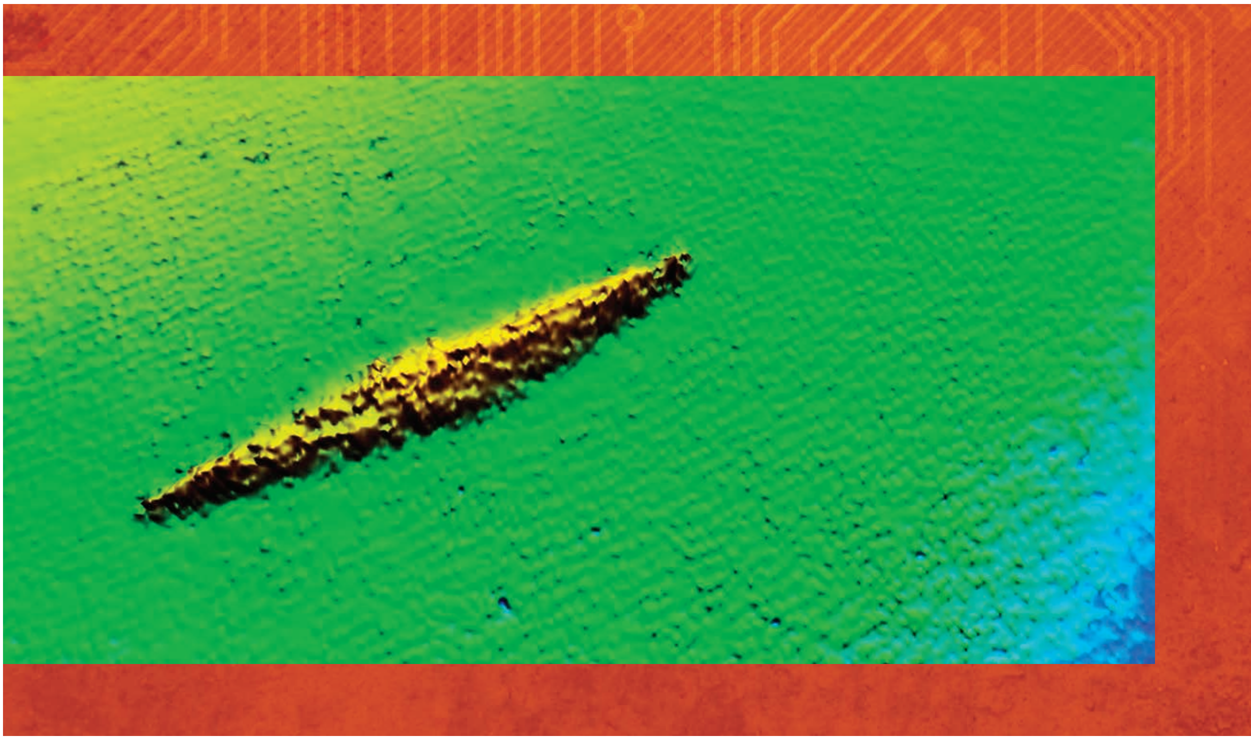
Recent malware and ransomware attacks have highlighted the urgent need to develop such regional gatherings to mitigate threats and to foster confidence-building measures regionally and internationally between similarly challenged states. These forums, though vitally important, tend to look at technology-enabled challenges discretely and without account for the systemic challenges posed by their combined effect. A more holistic approach is needed.

THE ASSOCIATED PRESS

RISK MITIGATION

So, what should be done to enable security policymakers to identify and mitigate the risks that the coming decade's confluence of highly impactful and interconnected technological advancements promise? The start of a to-do list should include the following:

- **Embed foresight and critical thinking:** Make foresight and scenario thinking part of organizational culture of security agencies. Conduct regular horizon scanning that includes how converging technology affects part of the strategy and planning process. For example: Use tech scanning "red teams" to spark opportunistic inquiry, question assumptions and identify risk.
- **Stimulate public dialogue and education:** Raise the extent and quality of public discourse, so society is aware of where science and technology could take us and can be capable of informed debate around what is desirable and acceptable, the safeguards that need to be in place, and the mechanisms required to prepare ourselves for change. Policy practitioners, technologists, educators and ethicists need to create new or invigorate existing collaboration forums to



REUTERS

A suspected North Korean drone that took pictures of a missile defense system is found in Inje, South Korea, in June 2017.

Royal Australian Navy analysts used an advanced side-scan sonar system aboard an autonomous underwater vehicle to discover in late 2017 an 800-ton submarine lost for a century off the coast of Papua New Guinea.

forge societal awareness, assurance and insistence that all necessary will be done to ensure emergent technologies are controlled by people, for the benefit of people, as opposed to being controlled by unauditable algorithms or malevolent actors. In addition, courses in technology, ethics and civics could be added to primary education curricula.

- **Promote national, regional and international technology governance:** Examine ways to help shape the long-term security consequences of trends in international and regional technology governance and standards bodies — for example, the International Organization for Standardization, the International Telecommunications Union, the International Committee for Information Technology Standards, and the Pacific Areas Standards Congress. Develop international collaborative bodies, within or supplementary to existing collaborative forums, chartered to the task of framing risk and developing holistic strategies for ensuring the impacts of emergent disruptive technologies such as AI, geoengineering, lethal autonomous weapons, synthetic biology and nanotechnology don't grow into unmanageable national, regional or global security threats. Security professionals need to use all means at their disposal to participate in identifying emergent risks to national policymakers, as well as participate actively in the increasingly diverse bodies and mechanisms necessary to mitigate them.
- **Future workforce development:** Examine the impacts of accelerating technology, generational change and cultural evolution on the future workforce. Leverage innovative learning and private sector concepts to build new models for predicting and mitigating the effects of manual labor and cognitive surpluses and shortages due to displacement by automation. Failure to effectively manage these disruptive transitions will exacerbate inequality and foster populist backlash increasing the likelihood of societal and interstate violence.

The next decades promise with near certainty a wild ride as security practitioners and policymakers try to keep pace with governance requirements adequate to guide development and mitigate the risks embedded in the pervasive effects of exploding technological growth. Governance mechanisms must be created to evolve and to adequately guide, without thwarting, emergent technologies' potential to fulfill human need. To paraphrase George Clemenceau speaking of war and generals, emergent technology use and impacts are too important to leave to the technologists, especially technologists in silos. Security policymakers and practitioners, therefore, must proactively contribute in forging and exploiting the governance tools necessary to be reliable sentinels in protecting the region and world from future peril. □

BIG IMPLICATIONS, LITTLE TECHNOLOGY

How small satellites are revolutionizing space

ERICA SULLIVAN/LOS ALAMOS NATIONAL LABORATORY

On a clear morning in Sriharikota, India, in mid-February 2017, a rocket launched carrying a record-breaking 104 satellites, including 101 CubeSats.

CubeSats are nothing new. A type of small satellite comprising units measuring 10 centimeters by 10 centimeters by 10 centimeters, they were first developed at Cal Poly and Stanford universities in the late 1990s as a training tool for aerospace engineering students. ("SmallSats" by definition weigh less than 500 kilograms; so all CubeSats are SmallSats, but not all SmallSats are CubeSats.) It wasn't long before governments began to look for ways to use CubeSats and other small satellites to bolster national security.

It's no coincidence that the rise in interest in these smaller than a mini-refrigerator satellites coincided with the awareness that existing satellites were vulnerable. In 2007, China proved this when it used a missile to obliterate one of its own satellites. Then there's the threat of cyber attack. The May 2017 ransomware virus that infected hundreds of thousands of computer systems around the globe and shut down hospitals and train stations was a stark reminder of the power of hackers. If that cyber attack was so debilitating on Earth-based systems, a carefully orchestrated cyber attack on a space-based asset would be catastrophic.

Virtually every military mission relies, to some extent, on satellites. Communications satellites enable joint force command and control by ensuring the availability of accurate, complete and timely information for the operational chain of command for land, sea and air forces. Meteorological satellites provide up-to-date weather information to field units in every branch of the military. Navigation satellites provide accurate positioning — within a few meters — for troops, planes and ships. Space-based surveillance systems provide treaty-monitoring capability during peacetime and serve as essential warning systems during conflict.

An H-IIA rocket, carrying a Michibiki 2 satellite, lifts off from the Tanegashima Space Center in Japan in June 2017. REUTERS

Los Alamos National Laboratory built and launched several CubeSats into low-Earth orbit. LOS ALAMOS NATIONAL LABORATORY

For the civilian arm of the government, satellite imagery is indispensable for disaster planning and response, mapping, urban planning and traffic monitoring. Then there are commercial uses: satellite phones, the internet, television, navigation and commercial tracking, resource exploitation — even predicting the weather for air travel or planting crops.

A successful attack on just one of those satellites could have far-reaching negative consequences on security and the economy.

TECHNOLOGICAL ADVANTAGES

What if, instead of one giant satellite providing critical national security functions, there were a hundred small satellites doing the same thing? The target would not only be smaller, but it would be dispersed — making a cyber criminal's job significantly more difficult.

Small satellites offer a lot of advantages. First and foremost, they're inexpensive. The average large satellite can cost anywhere from U.S. $500 million to U.S. $1 billion or more to build and launch. That's a hefty price for any budget. Small satellites, by comparison, are a bargain.

For example, Los Alamos National Laboratory has built and launched several CubeSats and estimates production costs of about U.S. $150,000 per unit. Also, the less expensive hardware means more technology can be acquired — enabling greater geographic coverage for observation and detection missions such as Earth/wave movement, seismic and volcanic activity detection, and atmospheric measurements.

Furthermore, by using less expensive platforms such as CubeSats and SmallSats, space scientists can test advanced concepts such as reconfigurable computing in space. In the past, once a satellite was in orbit, there was little operators could do to alter it. For the lifetime of the spacecraft, its functions would continue to be what they were programmed to be at the outset. Not so with CubeSats, which space scientists have made reprogrammable to allow for mission changes and improvements.

It also allows for a more agile approach to space hardware. Constrained mission needs enable rapid, focused development. While a large satellite can take a decade to design and build, space scientists can do the same with a CubeSat in a year or less. They also enable more testing in the operational environment rather than in simulated environments on the ground, and they allow cutting-edge technologies to be incorporated as they hit the market. Instruments and components can be tested in space before they're integrated into larger platforms for the final mission. These demonstration and validation missions greatly inform the design of instruments for any size satellite.

REVOLUTIONIZING ENGINEERING

For these reasons, small satellites are revolutionizing the way scientists approach engineering space systems. A staggering 2,400 SmallSats and CubeSats will be launched during the next six years, experts estimate. Whereas in the past, the commercial, government and academic sectors have used SmallSats equally, commercial use is expected to leapfrog the rest soon. In fact, over the next three years, commercial use of small satellites is anticipated to account for more than 70 percent of launches.

Small satellites aren't perfect. The majority, especially CubeSats, are launched to LEO and will re-enter the atmosphere due to drag much more quickly than spacecraft at higher altitudes — so their useful lifetimes are shorter. This is offset by the fact that getting to LEO is cheaper and easier and subjects the satellite to fewer radiation effects. Also, LEO allows the satellite to be closer to targets, improving the resolution of imagery, enabling lower-power communications and decreasing communications latency.

Increasingly, the government, industry and academia are looking for ways to use small satellites in orbits beyond LEO. For example, at Los Alamos, scientists and engineers are thinking of ways to use small satellites and CubeSats for deep space and interplanetary exploration missions. For these technically challenging missions, smaller, less expensive satellites create the opportunity to spread technical risk over redundant systems and to collect data from more locations.

LAUNCH CHALLENGES

There's also the issue of limited launch availability. Small satellites are often constrained to the rocket equivalent of Uber: They must "rideshare" with bigger payloads. This limits orbit options and schedules to those set by the primary payload, which pays the preponderance of the launch costs. Launch delays and the lack of dedicated small satellite launch vehicles have constrained the market potential, creating a backlog of SmallSats waiting for a ride to space.

System reliability is another issue. A comprehensive database of missions shows that more than 40 percent of CubeSats launched since 2000 failed to accomplish their objectives — perhaps an acceptable rate for student engineering programs or experimental commercial systems, but a nonstarter for meeting national security objectives. The challenge is engineering a system with the reliability required from space assets, while keeping the costs for components and testing in line with the costs of small satellite and CubeSat hardware.

Limitations on data processes and regulatory restrictions are other challenges. Launches require extensive paperwork to demonstrate that the secondary payloads "do no harm" to the primary payload. Then there's the concern over space junk and the consequent de-orbit requirements.

Perhaps the biggest challenge small satellites present is the very thing that makes them so appealing: their relatively low price tag. Because CubeSats and SmallSats are inexpensive (and the price will keep dropping as the technology advances), soon anyone will be able to access space, including adversaries for whom space has historically been out of reach.

For decades after the Soviet Union launched Sputnik, space was dominated by three nations: the United States, USSR/Russia, and — later — China. Increasingly, space is becoming more crowded. Today, satellites from China, the European Space Agency, France, India, Israel, Iran, North Korea, Russia, the United Kingdom, and Ukraine have been launched into space. With the low-cost threshold of small satellites, that number is expected to skyrocket. With that comes the question: Who will be in space in 10 years, and what will they be doing? Unfortunately, the answer is likely not all good. It's not hard to imagine a terrorist organization working with a friendly nation to develop CubeSats with reconnaissance capability hitching a ride into LEO. With more access comes more opportunities — for allies and partners as well as adversaries.

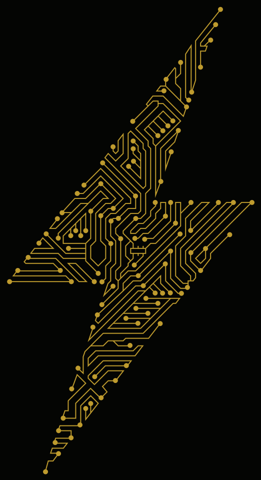
MANAGING RISK, FOSTERING COOPERATION

A leading challenge is to develop faster and smarter than the rest. The U.S. and its allies and partners must acknowledge that many nations now have access to space, and it must become a strategic military priority to introduce resiliency and redundancy into space systems. In short, nations must spread the risk. The good news is that advances in distributed computing and machine learning mean scientists can create a distributed network that can heal itself. So, if one satellite out of a constellation of a hundred is damaged, the others can compensate for that disability.

Also, the technology must be optimized. If there are more small satellites gathering more data than ever before, the next question becomes: How will that data be processed? Then, of course, there are myriad other questions as well: How do nations secure their networks? How do nations make their satellites impervious to space weather (that is, any and all conditions and events on the sun, in the solar wind, in near-Earth space and in the upper atmosphere)? Los Alamos, for one, is leveraging decades of experience developing space instruments, understanding of the extreme space environment and supercomputing prowess to answer these questions.

It's not only about developing the right technology, however. The U.S. and its allies and partners must also plan carefully — and not just on a national scale — but on a global one. Just as the international community has figured out international shipping and air traffic routes, the international community needs to collaborate to figure out how to work cooperatively to regulate space.

The reality is, during the next few decades, space will become more and more crowded and how it's used will change the world. That change is coming quickly. Will the international community rise to meet these challenges before they overwhelm Earth's orbits ? If the answer is to be yes, nations must start working together to solve these issues now. □



CYBER

STRATEGIES, POLICIES AND PRACTICES

Today’s computer networks require governments to maintain a robust defense plan on pace with cyberspace evolution

FORUM STAFF

The rapid development and spread of the internet of things — so-called smart devices enabled to collect and exchange data — and technology create the unavoidable need for policymakers and digital security experts to adapt to an ever-changing environment. Doing so means remaining flexible in creating cyber strategies to deter potential foes, defend critical infrastructures and adjust tactics when unique threats arise.

"Securing our cyberspace … requires us to have a better situational awareness of our overall cyber environment," Dr. Yaacob Ibrahim, the Singaporean minister for communications and information and minister-in-charge of cybersecurity, said during the Association of Southeast Asian Nations (ASEAN) Ministerial Conference on Cyberspace in October 2016. "This is key to improving our collective cyber hygiene, as we can better direct our prevention and remediation efforts when we know where we are vulnerable and where there may be suspicious cyber activities."

The 10 member states of ASEAN — Brunei, Burma, Cambodia, Indonesia, Laos, Malaysia, the Philippines, Singapore, Thailand and Vietnam — remain keen on a comprehensive strategy, having launched in April 2017 the ASEAN Cyber Capacity Programme (ACCP). Its main objectives include raising awareness and fostering deeper regional discussions on cyber norms, enhancing regional coordination of capacity building and incident response by developing metrics to assess effectiveness in these areas, building regional capacity in strategy development and cyber legislation and contributing to global efforts to develop a set of cyber security internet of things standards.

"Countries today face a full spectrum of cyber threats — cyber crime, attacks, espionage and other malicious activities," Ibrahim said. "We in ASEAN have not been immune to this. … Southeast Asian governments are more likely to be the target of a cyber attack than other organizations in the region, and advanced persistent threats remain one of our biggest threats."

Attacks could range from financial to data theft, reputational damage or disruption to critical information infrastructure. Any of these could harm economies and societies.

These risks reinforced the need for ASEAN to establish the ACCP. Among the ACCP's goals: Create a secure and resilient cyberspace that enables economic progress and better living standards.

Regardless of the assessment, that's no small feat. Malware, for example, presents itself like any other business. Cyber threat groups compete and innovate. The most successful grow and spread.

A man uses a computer in an internet cafe in Beijing.

AFP/GETTY IMAGES

A man is reflected on the electronic board of a securities firm in Tokyo. Governments worry that a cyber attack could cripple financial systems.

THE ASSOCIATED PRESS

Filipino police officers check their phones outside an Association of Southeast Asian Nations summit in Manila, Philippines, in April 2017. REUTERS

INTERNATIONAL INITIATIVES

Globally, cyber crime costs about U.S. $3 trillion a year, according to Keshav Dhakad, regional director for Microsoft Asia's Digital Crimes Unit. A survey revealed that 71 percent of interviewed companies admitted to falling victim to cyber attacks in 2015, according to Dhakad. The potential risk for more victimization will only increase because of the sheer volume of users.

The Indo-Pacific, for example, will grow to roughly 4.7 billion internet users by 2025, with nearly half of those gaining access between 2012 and 2025, according to a Microsoft Cyber 2025 Model.

"Cyber security cannot be a piecemeal effort, and each organization must have a 360-degree security framework," Dhakad said. "This includes having a comprehensive protect, detect, respond posture and commensurate investments and resources, coupled with regular assessment and review of its cyber security practices to protect its identity, data, apps, devices and infrastructure."

Few treaties exist that directly deal with cyber operations. Those that do have a limited scope.

This lack of cyber-specific international law, however, does not mean that cyber operations exist in a world with disregard for rules and regulations. In fact, cyber experts gather often to tweak agreements, suggest new guidelines as the space evolves and maintain

Continued on page 30

AUSTRALIA BOOSTS CYBER CRIME COOPERATION WITH ASIAN ALLIES

THE ASSOCIATED PRESS

Australia is intensifying cooperation with its Asian neighbors on cyber crime amid growing criminal threats and the need to boost regional commercial security.

The agreement, signed in Bangkok in June 2017, means Australia is now working in tandem with Thailand, Singapore and China on issues of cyber crime and security. Australian Ambassador for Cyber Affairs Tobias Feakin said cooperation was vital in the face of growing challenges posed by cyber-criminal networks in the Indo-Pacific.

"Criminals and nefarious actors can adapt and absorb all [this information] so much quicker than governments," Feakin said. "So if we're not talking about it, sharing best practices and keeping on the move as well, then we will soon find ourselves behind by quite a margin."

Feakin held talks with senior leadership of the Thai Royal Police, national security and foreign affairs officials with Australia to provide support in cyber crime digital forensic development.

Australia already cooperates with Thailand through the Royal Thai Police and Office of Narcotics Control Board, based on threats by transnational criminals, including Australian biker gangs linked to drug trafficking of amphetamine-type stimulants into Australia. Thailand is also a base for securities fraud operators, known as boiler room share scams, where foreign expatriates, including British and American, target Australia and New Zealand investors with fake online investments.

Feakin said cooperation was directed to "upskilling the digital forensics capability of the Royal Thai Police" to ensure evidence was credible when presented at court. "To get the evidence, how you secure it, to a degree that it is admissible in a court and then, what is your investigative processes to actually try and find the individual or group who may be responsible," he said.

Officials said support to Thai police was a "cornerstone of digital forensics about capturing electronic evidence on various devices, how to process and extract data." They said increasingly transnational crime investigations centered on the use of digital media for communications, storing of information by organized crime gangs. The agreement with Thailand comes after the signing of a pact between Australia and Singapore on cyber security, including information sharing, training and joint exercises in safeguarding critical information infrastructure.

In April 2017, an agreement with China enhanced cyber security cooperation, after Australia pressed China on issues of cyber-enabled intellectual property theft.

Tobias Feakin, Australian ambassador for cyber affairs, bottom left, signs a memorandum of understanding with David Koh, chief executive of Singapore's Cyber Security Agency as Australian Prime Minister Malcolm Turnbull, top left, and Singapore's Prime Minister Lee Hsien Loong, top right, look on in June 2017. THE ASSOCIATED PRESS

"What you saw through the agreement that we signed with China was an acknowledgement that it needs to be a key part of discussions together," Feakin said. "China is a huge economic partner. There are some [common] areas, there are some differences. That we got to a point of signing an agreement which said we agree to not conduct cyber-enabled intellectual property theft — I think it's a good point."

Continued from page 28

forums where governments and experts can collaborate and expand commerce.

"A secure and resilient cyberspace is an enabler of economic progress and better living standards," according to ASEAN cyber program documents. "States can contribute to the security and resilience of cyberspace by adhering to well-defined and practical voluntary norms of behavior that are supported by robust confidence-building measures."

Public and private actors in the cyber realm gather often to foster support and confidence building. One such gathering took place at the Center for Strategic and International Studies (CSIS) in Washington, D.C., in March 2017. During the daylong Cyber Disrupt Summit — the first hosted by CSIS — experts and government officials assessed the evolving international security environment and offered potential responses to increased hostilities in cyberspace.

Thomas Bossert, assistant to U.S. President Donald Trump for homeland security and counterterrorism, detailed lessons on cyber the United States has learned in the past decade and offered insight on emerging U.S. policy. One of Bossert's most important messages was that countries — as well as corporate and individual actors — recognize norms when operating in the cyber realm.

"Norms are important. They are our statement, as a country, that we have a certain expectation for how people will behave themselves on an open, interoperable platform that allows for innovation, free trade, fair trade and other things that we think are important to our societal organization [and] socio-economic organization," Bossert said. "You start by candidly telling other countries how we expect them to behave and how we promise to behave in return. And if they accept those norms and then fail to abide by them, we have a responsibility to call them out on it, and we have a responsibility to do something about it."

The cyber threat to U.S. critical infrastructure has outpaced efforts to reduce pervasive vulnerabilities, according to a February 2017 report by the U.S. Department of Defense Science Board Task Force on Cyber Deterrence.

"For the next decade at least, the United

Anti-cyber war force police officers march during a National Day parade in Vietnam. As a member of the Association of Southeast Asian Nations, Vietnam is cooperating with other member states on cyber security. REUTERS

States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries," Craig Fields, Defense Science Board (DSB) chairman, wrote in the report, acknowledging the need for a "more proactive and systematic approach" to cyber deterrence.

Foremost, not all cyber attacks can be deterred, the DSB report noted.

"As one important example, even the certain promise of severe punishment may not deter terrorist groups bent on wreaking havoc on the United States and our allies," the DSB report said. "As a second and quite different example, if the United States were in a major war with another nation, we should not expect to be able to deter even debilitating cyber attacks on U.S. military capabilities that produced little or no collateral damage to civilian society."

The DSB report defined cyber deterrence as the use of both deterrence by denial and deterrence by cost imposition to convince adversaries not to conduct cyber attacks or costly cyber intrusions. The U.S., in some instances, extends its deterrence practices to protect allies and partners.

"Just as cyber is a relatively new domain, cyber deterrence is a relatively new endeavor. For the most part, to date the United States has been establishing its cyber deterrence posture step-by-step, in response to attacks," according to the DSB report. "Although the United States responded with diplomatic moves and economic sanctions to North Korea's Sony hack, China's IP theft and Russia's meddling in U.S. elections, it is far from clear that such responses have established effective deterrence of future cyber attacks and costly cyber intrusions."

DEFENSIVE PRACTICES

A strong information technology (IT) and "internet hygiene" process provide the foundation for a robust cyber security posture, according to Dhakad. He recommends that organizations develop an "assume breach" posture, which deploys an active defense strategy and investments into identifying vulnerabilities to avoid a reactionary situation.

Leaders in ASEAN agree that the ever-expanding realm of cyber requires conversations to avoid digital conflict.

"It is timely for ASEAN to start our dialogue on cyber norms. Global discussions on cyber norms have kicked off in the last decade, catalyzed by platforms such as the United Nations Group of Governmental Experts," Ibrahim said during the ASEAN cyber gathering in October 2016. "While staying plugged in to the global conversations, we should also make sure that norms and behaviors are kept relevant and applicable to our unique ASEAN context and cultures. This ASEAN perspective can be our joint contribution to global conversations."

Internal conversations by governments should also include a checklist for ensuring a vigorous cyber security posture that can withstand and respond effectively to cyber attacks and malware infections. Dhakad offered these recommendations:

- **Keep your house in order.** The question is not whether cyber criminals are going to attack, it's just a matter of when. That said, the usage of IT assets that are old, unprotected or are nongenuine in nature substantially increase the chances for a cyber attack. For example, pirated and counterfeit software are known to come with embedded malware infections. The case for having a strong IT (software and hardware) asset procurement, usage, maintenance and periodic upgradation is more critical than ever before.
- **Start from within.** Poor cyber hygiene of IT users, negligent employee behavior or weak credentials/password protection within an organization, adds a high degree of vulnerability for system compromise. With more and more personal devices being used at the workplace, the higher the chance they are infected, including unprotected interconnected devices (internet of things), which can be easy targets for cyber criminals to inflict damage.
- **Monitor all systems in real time.** Invest in modern threat protection technologies to monitor, detect and remove common and advanced cyber threats in real time, and develop in-house expertise to undertake threat analytics. Some studies have suggested that the average time to discover a cyber threat from the time of infiltration in the Indo-Pacific is 510-plus days, which far exceeds the global average rate of 140-200 days.
- **Maintain a trusted IT supply chain and regular review.** Only use genuine, current and updated software. Have a trusted supply chain across software, hardware and the internet of things. Bring your own device and regularly review and assess cyber security investments and performance of both software and hardware deployment, including customer and vendor access to the corporate/government network.

Momentum continues to build as conversations expand on cyber security. For example, a bill introduced in the U.S. Congress in May 2017 (and still pending approval when *FORUM* went to press) aims to help the Indo-Pacific increase cyber cooperation with allies. If passed, it would authorize U.S. $2.1 billion for security initiatives in the region.

"No one needs reminding of the escalating tensions in the Asia-Pacific," U.S. House Armed Services Committee Chairman Rep. Mac Thornberry, who introduced the bill, said in a prepared statement, according to *The Hill*. "It is essential that the United States reassure our allies and friends that we are committed to stability and security in that region now and in the future. One of the best ways to do that is to increase our military presence and enhance our readiness there. To do that, we need to invest in a broad range of defense capabilities, and this legislation does just that." □

COMBATING WILDLIFE CYBER CRIME

INDIA ADDRESSES ILLICIT INTERNET TRADE

FORUM ILLUSTRATION

SAROSH BANA

The website advertised *dhaariwala chaddar*, which is Hindi for "striped bedsheet." It is also code for tiger skin, the sale of which is illegal under the Convention on the International Trade of Endangered Species (CITES), a treaty signed by 183 countries that protects 5,000 species of animals and 29,000 species of plants. In foreign markets, a tiger rug can sell for more than U.S. $160,000, and investigators have seen a stuffed tiger priced at U.S. $728,000.

Although the internet has facilitated trade in rare and endangered species for decades and contributed to the decline of many species worldwide, such trafficking has become more prevalent in recent years in India, a country rich with diverse and extraordinary creatures.

Poaching and wildlife crimes increased 92 percent in India, from 15,800 to 30,382 between 2014 and 2016, according to a book by New Delhi's nonprofit Centre for Science and Environment titled *State of India's Environment 2017*. The number of species poached or illegally traded also increased from 400 in 2014 to 465 in 2016, data from the Wildlife Protection Society of India revealed.

India's national animal, the tiger, has declined from 100,000 a century ago to about 2,226 at present, according to India's Environmental Ministry. India harbors about 60 percent of the world's tigers, with the other remaining 1,400 distributed across 12 countries, the World Wildlife Fund (WWF) estimates.

Poachers killed at least 15 of the 74 tigers that died in India between January and July of 2017, government officials said. Six died of natural causes, and 53 deaths are pending investigation. Twenty-one of the 122 tigers that died in 2016 were poached. Poachers also did not spare the peacock, India's national bird. They killed 340 peacocks between 2015 and 2016, a tally that nearly doubled that of 2014.

Kaziranga National Park rangers find a tiger carcass in floodwater at the Bagori range in August 2017.

THE ASSOCIATED PRESS

Internet traffickers have also targeted India's one-horned rhinos. A rhino horn commands 1 million rupees (U.S. $15,625) in local markets and more than twice that when sold as an aphrodisiac in the Chinese or Vietnamese markets. More than 260 rhinos have fallen to poachers in the state of Assam since 2001, according to government figures. Seventeen more perished in the heavy rains in 2016, and the two waves of flood this season have claimed the lives of 28 more. Poachers are aware they can acquire the horn without having to kill the animal. A rhino's horn does not grow out of its skull. It is composed of keratin, a protein found in hair, fingernails and animal hooves, and can be excised without killing the animal.

ELUDING ENFORCEMENT

The internet has streamlined illegal cross-border wildlife trade, making detection of traffickers more difficult. These traders face minimal risk of being exposed or tracked because they do not need bricks-and-mortar showrooms or conventional means to peddle their wares, experts explain. They now make deals online from remote locations, removed from law enforcement scrutiny. Prospective clients place orders, usually in code, paying online for what often appears to be legitimate products, skirting discovery.

Moreover, many of these criminal organizations are politically connected and well-funded. India's Supreme Court, the country's highest court, observed in a 2010 ruling against a trafficker that many animals are being driven to the brink of extinction by "ruthless sophisticated operators, some of whom have top-level patronage."

"The actual poachers are paid only a pittance, while huge profits are made by the leaders of the organized gangs who have international connections in foreign countries. Poaching of wildlife is an organized international illegal activity which generates massive amount of money for the criminals," the judgment said.

ONLINE TRACKING

India has increased its efforts to thwart such cyber traffickers. In 2016, Indian Environmental Minister Anil Madhav Dave released a list of websites, including Amazon India, Snapdeal, OLX India, eBay India, Alibaba India and Quikr, that were selling rare animals and their parts. India's Department of Information Technology was monitoring the online activity as part of its efforts to combat cyber crime at the central and state government levels.

The Wildlife Crime Control Bureau (WCCB), based in New Delhi, compiled a list of more than 100 websites. A 2007 statute established WCCB under the Ministry of Environment and Forests to combat organized wildlife crime in India. One section of the Wildlife (Protection) Act calls for the collection, collation and dissemination of intelligence on organized wildlife crime activities to enforcement agencies for immediate action to apprehend such criminals.

Indian authorities recently tracked down clandestine online trade in the dried penises of monitor lizards that were being sold as *hatha Jodi*, which means "folded hands" in Hindi, a rare plant root used as a talisman in tantric, or occult, rituals. The e-commerce sites of Amazon, Snapdeal, eBay and Alibaba on which this item was sold had not ascertained the origin of the products.

"We hope to rid the internet of such items so that people are not getting fooled by criminals and buying wildlife trade products unbeknownst to them," said Jose Louies, who heads the enforcement assistance and law division of the Wildlife Trust of India (WTI) and who helped uncover this trade.

Trade in monitor lizards is illegal under the Wildlife Act and also is cruel. Trappers immobilize an animal by tying its legs together after pulling out its claws. They then burn the reptile's groin while it is still alive to make the penis protrude enough to excise it with a knife. The animal dies an excruciating death, Louies said.

WTI and WCCB have launched an online

Criminals market monitor lizards and their parts, which are advertised on the internet as aphrodisiacs.

THE ASSOCIATED PRESS

campaign to stop the use of animal products in such occult practices in India along with other initiatives to combat cyber trafficking of wildlife in general, Louies said.

“The bureau is regularly monitoring the websites for any such advertisements or offers for immediate action in the matter,” said WCCB Additional Director Tilotama Varma. “Considering the seriousness of the issue, the bureau has also taken several initiatives, such as contracting a cyber crime specialist to carry out regular cyber patrolling to detect any posts or offers over such trade portals on the World Wide Web, apart from retrieving details of suspects and passing them on to relevant enforcement agencies for legal action.”

“WE HOPE TO RID THE INTERNET OF SUCH ITEMS SO THAT PEOPLE ARE NOT GETTING FOOLED BY CRIMINALS AND BUYING WILDLIFE TRADE PRODUCTS UNBEKNOWNST TO THEM.”

— JOSE LOUIES, WILDLIFE TRUST OF INDIA

Moreover, “if the investigations or criminal analyses by the WCCB or any other agency determine the involvement of any foreign nationals, the details of such culprits are sought from the respective countries through the National Central Bureau [Interpol],” she said.

WCCB convened a meeting of representatives from online trade portals in May 2016 to alert them to internet trafficking and to discuss how they could assist the bureau, Varma said. Many of the websites, she noted, are hosted from overseas, and the businesses are difficult to locate.

TARGETING MARKETERS

Worldwide demand for animal and plant products continues to drive wildlife trafficking in India, with the U.S. and China topping the list of markets. Traffickers are emboldened, some experts say, because the U.S. is the largest consumer of legally traded plant and animal products regulated by CITES. The U.S. Congress passed the Eliminate, Neutralize, and Disrupt Wildlife Trafficking Act in September 2016, providing the country with “additional tools to combat wildlife trafficking and to foster international action to end this threat to our natural heritage.”

China, too, is a major consumer of legal and illegal wildlife products. Traditional Chinese medicine is based largely on natural flora and fauna. Consumption in China is also driven by age-old beliefs in the aphrodisiacal powers of various animal products such as tiger penises and rhino horns, many of which are unfounded.

While China is the main market for ivory, Vietnam is the top market for rhino horn, says Dr. Richard Thomas of Cambridge-based TRAFFIC, the joint wildlife trade monitoring network of the WWF and International Union for Conservation of Nature. China has pledged, however, to end ivory trade by the end of 2017, a move that has sent prices plummeting globally and that raises hopes for elephant conservation. The Chinese market has been a major driver of elephant poaching in Africa, where 30,000 elephants are slain each year.

International trade in ivory has been banned since 1990, but many countries, including the U.S. and China, have continued to allow its domestic sale. However, Washington passed regulations in June 2016 banning such trade, though exempting ivory antiques and some other categories.

Apart from ivory, other wildlife products continue to be routed to China through India, Nepal, Burma and Bangladesh, among others.

E-tailers such as Amazon, eBay, OLX and Snapdeal say they have terminated such sales. Amazon India says it took down 296 items in the “animal specimen” category in May 2017 and 104 items under the “snares or traps” category listed by third-party sellers. “Such products are no longer available on Amazon. In addition, we have strictly enforced any attempts to inadvertently sell them,” a spokesperson said. EBay states that it has zero tolerance for any wrongdoings and has outlined policies against such sales on its site. OLX reports it is taking steps to ensure that protected animals and birds are not listed for sale by any of its users.

India’s Madhya Pradesh Tiger Strike Force, which was set up in 2008 by the state forest department as a check on wildlife poaching, recently served notices on e-commerce companies Snapdeal, IndiaMart, Wish and Buy, and Craft Comparison for listing wildlife products on their portals. These firms had been linked to the online sale and seizure of animal products related to the work by India's Wildlife Trust and Louies. Indian authorities directed the companies to remove all such content from their sites and demonstrate why they should not be acted against. The confiscated items included *hatha jodi* as well as *siyar singhi* – clumps of hair that grow on a jackal's head – that is used in a similar fashion in tantric rituals and believed to possess magical properties that will bring wealth and help resolve problems.

Some online companies have been working to curb internet marketing of illegal items. In 2009, eBay forbade the sale of ivory across all its platforms. Chinese online marketplaces Alibaba and Tabao banned postings of wildlife sales in 2009 and 2008, respectively, according to an Organisation for Economic Co-operation and Development task force on countering illicit trade report. Another e-commerce firm, Etsy, banned such sales in 2013, and Chinese tech giant Tencent, which owns WeChat and the QQ instant messenger, in 2015 launched a campaign, "Tencent for the Planet – Say 'No' to Illegal Wildlife Trade."

WCCB Joint Director Kamal Datta said the bureau has supplied the trade portals with code words and filters and has asked them to report suspicious activity. The WCCB also conducts training for its staff to keep them abreast of such trends and to take action. It also facilitates capacity-building programs for forest and police officials, organizes interagency meetings and sponsors awareness sessions for people living near wildlife reserves.

"We are constructively coordinating with all concerned agencies like the forest protection force, the police, Customs, Central Bureau of Investigation, Intelligence Bureau, Reserve Police Force and SSB [*Sashastra Seema Bal*, Hindi for Armed Border Force] for effective enforcement," Varma said. "The bureau also coordinates with the Indian Navy and Coast Guard in the Andaman and Nicobar Islands, in the Bay of Bengal, and the Gulf of Mannar and the Lakshadweep Islands in the Lakshadweep Sea [an expanse of the sea bordering India, the Maldives, and Sri Lanka in the Indian Ocean] for effective action against illegal poaching of marine species."

SUCCESSFUL ARRESTS

The WCCB, working with its various components and counterparts, continues to rack up successes. Between 2013 and 2016, WCCB tracked 725 smuggling cases and arrested 275 perpetrators, Varma said.

WCCB has arrested at least 129 people involved in poaching of the pangolins and trading of their scales, sought for their medicinal and aphrodisiacal qualities, since March 2015 when the Madhya Pradesh forest department created a special task force to tackle the issue. Demand from China for the endangered mammals is driving the illicit trade and has led poachers to establish three main smuggling routes from central India to China, the *Hindustan Times* newspaper reported in February 2017. The first moves goods through Nepal and Tibet, the second through Burma to Laos and Thailand, and a third through Uttarakhand to Tibet. Illegal drugs often accompany shipments, one informant said.

Indian officials seized roughly 5,900 kilograms of scales between 2009 and 2014, which means about 2,000 pangolins were killed during that time, according to the *Hindustan Times*. In China, the scales sell for U.S. $2,500 a kilogram.

"Our research shows while the number of seizures is increasing, the volume of seized scales is declining. This is a clear indication that the population of pangolins is decreasing in India," pangolin expert Rajesh Kumar Mohapatra told the *Hindustan Times*. Mohapatra is a member of the International Union for Conservation of Nature's Pangolin Specialist Group.

Similarly, in the largest turtle interdiction in the country so far, a special task force run by the Uttar Pradesh police seized 6,430 endangered soft shell and flap shell turtles from a house in Amethi district in January 2017, the *Times of India* newspaper reported. As many as 37,267 turtles were rescued in India between 2015 and 2016, or about 100 turtles every day of that year, the Centre for Science and Environment reported.

Today, most species in India are threatened by poaching, shrinking habitats, haphazard development and by hunters looking for game. Despite the enforcement successes, much work remains. Wildlife trafficking, deforestation and loss of habitat are no longer localized problems but global ones. Sharing information internally and regionally is key for strengthening enforcement networks and increasing understanding and commitments to counter cyber criminals who engage in illegal trade in animals, plants and wildlife, trafficking enforcement experts advise. Many Indian officials point out that the foreign demand drives poaching and the often-needless slaughter of endangered animals. To curb cyber trafficking, factors driving demand must also be addressed, they say. □

Paramilitary police officers participate in an anti-terrorism drill at China's Haiyang nuclear power plant in May 2017.

ENERGY SECURITY

Cooperation and good governance key for ensuring safe nuclear power generation and regional stability

FORUM STAFF

PHOTOS BY REUTERS

Experts predict the Indo-Pacific region will drive future nuclear energy development, with China, Japan, India and South Korea propelling much of the growth. The region operates more than a quarter of the world's 449 nuclear power reactors, and more than half of the world's new nuclear capacity is being built there, the Nuclear Energy Institute reports.

More than 40 plants are already under construction, and another 90 are in the planning stages in the region, according to the latest tally by the World Nuclear Association (WNA). In addition, more than 20 other Indo-Pacific nations, including Bangladesh, Indonesia, the Philippines, Malaysia, Sri Lanka and Thailand, are planning or considering building nuclear power plants in the coming decades.

"The prospects for nuclear power in the Asia-Pacific region are not only promising ... it is relevant and will continue to remain so in the coming years," said Maria Zeneida Collinson of the Philippines' Foreign Affairs Department, who facilitated the September 2016 International Atomic Energy Agency (IAEA) and International Framework for Nuclear Energy Cooperation conference in Manila, according to *The Japan Times* newspaper. "This Asia-Pacific region has one of the fastest economic growth rates in the world. It follows that the demand for affordable and sustainable energy sources is expected to rise," she said in a summary statement.

Nuclear power has the potential to cut pollution levels, reduce dependence on oil and fossil fuels and help slow unwanted changes to the climate. "Nuclear energy could contribute to sustainable development by meeting rising energy demands and, at the same time, mitigating climate change," Collinson explained.

China, for example, relies on fossil fuels — mainly coal — to produce more than 70 percent of its electricity. To help meet its growing demand for energy, China plans to more than double its nuclear capacity to 58 gigawatts by 2021, WNA reported. One gigawatt is enough to power about 725,000 homes in a developed country. China, which operates 36 nuclear power plants and has 24 under construction and more planned, also intends to export its nuclear technology, according to WNA.

Meanwhile, India in May 2017 approved plans to build 10 more nuclear reactors that will increase the nation's capacity by an additional 7.8 gigawatts and propel its industry forward, Reuters reported. Its current 22 nuclear plants produce about 6.8 gigawatts, and six plants that will supply 6.7 gigawatts by 2021 were already under construction. The 10 additional reactors would employ India's pressurized heavy water reactor design and create more than 33,400 jobs, according to a government statement. "It will be a major step toward strengthening India's credentials as a major nuclear manufacturing powerhouse," the statement said.

Growth Risks

The outlook for nuclear power remains positive in the region despite the nuclear accidents of Three Mile Island, Chernobyl and Fukushima and ongoing proliferation concerns. South Korea, which operates 25 reactors, obtains about 30 percent of its electricity needs from nuclear power, and Japan gets about 22 percent from the operation of 43 reactors, and those numbers are forecast to increase, according to WNA. South Korea's government, however, halted construction in June 2017 on

two partially completed nuclear reactors to address public concerns over atomic safety, Reuters reported. In recent years, about 10 new plants on average have become operational annually worldwide.

Although the risk of another nuclear accident cannot be reduced to zero, nations must factor relative risks in their assessments, Dr. Bill Wieninger, a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies (APCSS), explained at the U.S. Pacific Command's Operational and Science and Technology Conference in Honolulu in March 2017. "For all the horrors of a major accident, the simple truth is that mortality risks from nuclear power are dwarfed by those posed by fossil fuels, whether one considers particulate pollution, carbon emissions, supply stability, extraction pollution or transportation accidents."

As the use of nuclear energy grows in the region, however, so does the risk of destruction and proliferation because of the sheer numbers, experts say. As it is, the risk is ever-present because nearly every country worldwide has access to the small quantity of uranium needed to produce a few weapons, according to the WNA March 2017 online report "Safeguards to Prevent Nuclear Proliferation."

In addition to the growing number of nuclear energy facilities in the Indo-Pacific, most countries — including Bangladesh, Indonesia, North Korea, the Philippines and Vietnam — already have research reactors, according to the WNA.

So far, international safeguards have worked to prevent nuclear proliferation globally. "To date, civil nuclear power has not been the cause of or route to nuclear power in any country that has nuclear weapons, and no uranium traded for electricity production has been diverted for military use," the March 2017 WNA report said.

Given the predicted future rapid rate of growth, increased cooperation and good governance practices are needed to ensure that nuclear energy generation is safely implemented and expanded in the region, experts say.

Fishermen stand in front of the Kudankulam nuclear power plant in the southern Indian state of Tamil Nadu.

NUCLEAR POWER *(April 2017)*

COUNTRY	POWER REACTORS Operable or in Operation	POWER REACTORS Under Construction	POWER REACTORS Planned	RESEARCH REACTORS	OTHER STAGES OF THE FUEL CYCLE
Australia				1	🟡
Bangladesh			2	1	
China	36	24	40	16	🟡 🔵 🔴 🟢
India	22	6	22	4	🟡 🟢 🟠 ⚫
Indonesia			1	3	🟢
Japan	43	3	9	14	🔵 🔴 🟢 🟠 ⚫
S. Korea	25	3	8	2	🔵 🟢
Malaysia				1	
N. Korea				1	🔵 🟢 🟠
Pakistan	4	2	2	1	🟡 🔴 🟢
Philippines				1	
Taiwan	6	2		1	
Thailand				1(+1)	
Vietnam			4	1	
TOTAL	136	40	88	49*	

*48 research reactors operable, 1 under construction in Thailand.

🟡 Uranium Mining
🟢 Fuel Fabrication
🟠 Reprocessing
🔵 Conversion
🔴 Enrichment
⚫ Waste Management facilities for used fuel away from reactors

Sources: World Nuclear Association, World Energy Outlook

Expanding Cooperation

More and better regional and international cooperation can help mitigate the risk of nuclear accidents and of proliferation and enhance overall security by reducing resource competition.

Historically, past accidents have led to the production of better tools for cooperation. After the Three Mile Island accident in Pennsylvania in 1979, the nuclear power industry created the Institute of Nuclear Power Operations, a nonprofit headquartered in Atlanta, to promote the highest levels of safety and reliability in the operation of commercial nuclear power plants. The industry founded the organization in response to the findings of the Kemeny Commission, which investigated the accident. The institute has worked with industry internationally to establish performance objectives, criteria and guidelines for the nuclear power industry to conduct regular detailed evaluations of nuclear power plants and to help improve performance, according to its website.

> *Historically, past accidents have led to the production of better tools for cooperation.*

"There was robust cooperation among various stakeholders in safe reactor design, construction and operation even prior to the incident at Fukushima, as demonstrated by the continuing cooperation between Westinghouse, Southern Power and China's State Nuclear Power Technology Corporation on the construction and the eventual operation of AP1000 reactors in the U.S. and China," APCSS' Wieninger explained.

After the 2011 Tohoku earthquake that measured 9.0 on the Richter scale, a 15-meter tsunami disabled the power supply and cooling of three Fukushima Daiichi reactors. All three largely melted in the first three days, causing a nuclear accident on March 11, 2011, as WNA reported. The disaster provided many lessons learned and generated new means for regional and international cooperation. For example, the IAEA director general and the U.S. Nuclear

WORLD NUCLEAR GENERATION and CAPACITY (April 2017)

COUNTRY	Number of NUCLEAR UNITS	NUCLEAR CAPACITY (MW per year)	NUCLEAR GENERATION (GWh per year)	NUCLEAR FUEL SHARE (Percent)
U.S.*	99	99,319	805,327.2	19.7
France	58	63,130	386,452.9	72.3
Japan	43	40,290	17,537.1	2.2
China	36	31,384	197,829.0	3.6
Russia	37	26,528	184,054.1	17.1
South Korea	25	23,077	154,306.7	30.3
Canada	19	13,554	95,650.2	15.6
Ukraine	15	13,107	76,077.8	52.3
Germany	8	10,799	80,069.6	13.1
Sweden	10	9,740	60,647.4	40.0
U.K.	15	8,918	65,149.0	20.4
Spain	7	7,121	56,102.4	21.4
India	22	6,240	35,006.8	3.4
Belgium	7	5,913	41,430.5	51.7
Taiwan	3	5,052	30,461.0	13.7
Czech Republic	1	3,930	22,729.9	29.4
Switzerland	5	3,333	20,303.1	34.4
Finland	4	2,764	22,280.1	33.7
Bulgaria	2	1,926	15,083.5	35.0
Hungary	4	1,889	15,183.0	51.3
Brazil	2	1,884	14,970.5	2.9
South Africa	2	1,860	15,209.5	6.6
Slovakia	4	1,814	13,733.4	54.1
Argentina	3	1,632	7,677.4	5.6
Mexico	2	1,552	10,272.3	6.2
Romania	2	1,300	10,388.2	17.1
Pakistan	4	1,005	5,438.9	4.4
Iran	1	915	5,924.0	2.1
Slovenia	1	688	5,431.3	35.2
Netherlands	1	482	3,749.8	3.4
Armenia	1	375	2,194.9	31.4
TOTAL	**451**	**391,521**	**2,476,671.2**	

* IAEA and U.S. Energy Information Administration nuclear capacity figures vary slightly.

Source: International Atomic Energy Agency

Regulatory Commission, among others, issued recommendations on how to improve reactor safety.

A leading example of strengthening cooperation between nations occurred in March 2016 when China and the U.S. opened a joint nuclear safety center in Beijing to offer training on the safe handling of nuclear materials and the prevention of terrorist attacks on nuclear facilities, provide a forum for bilateral and regional best practice exchanges, and serve as a venue for demonstrating advanced technologies related to nuclear security. Strong leadership can help ensure that improved safety practices and technologies are implemented.

The U.S. Department of Energy's National Nuclear Security Administration's Office of Defense Nuclear Nonproliferation and the China Atomic Energy Authority have worked together on more than 50 training and technical exchanges on nuclear security best practices that culminated in the creation of the Beijing center of excellence.

Fukushima also contributed to the growing realization of the interdependence of nations when it comes to resource management and many other security issues. "No one country can just start creating nuclear power because, especially after the accidents of Three Mile Island, Chernobyl and Fukushima, [they showed] that the whole world is connected," IAEA Deputy Director General Mikhail Chudakov said during the 2016 Manila conference, according to *The Japan Times*.

Good Governance

Good governance will also be key for reducing the dangers of nuclear facility incidents, waste disposal and the potential spread of nuclear weapons and radiological dispersal devices as the number of nuclear power plants in operation increases in the region.

"Government policy will need to play a key role in all things nuclear, particularly in the establishment of a strong and effective regulatory framework that reduces the dangers of nuclear weapons proliferation, nuclear facility incidents and waste management," Wieninger said.

Prior to the Fukushima accident, seismologist Professor Ishibashi Katsuhiko questioned the independence of Japan's Nuclear Safety Commission after a senior Nuclear and Industrial Safety Agency official appeared to rule out a new review of the commission's seismic design standards. After the disaster, Japan revised its atomic regulations in response to an official inquiry into the disaster documented collusion between regulators and industry.

In 2016, the IAEA said that Japan's regulatory body for nuclear and radiation safety, the Nuclear Regulatory Authority, has "demonstrated independence and transparency" since it was set up in 2012. The authority also "needs to further strengthen its technical competence in light of upcoming restarts of Japanese nuclear facilities," the IAEA said. "Good, strong, noncorrupt regulatory processes must be in place," Wieninger said.

Nuclear reactors have been designed that do not produce weapons-grade plutonium and thereby minimize the risk such materials could be secretly used for illicit weapons production.

Policies that promote improving information exchanges between experts will also enhance regional cooperation. For example, a society could be created in the Indo-Pacific that is modeled on the European Nuclear Society, which includes members from more than 27 nations and many corporations, Wieninger said.

Policies that promote development of better technologies will also enhance safety of nuclear power production and management of undesirable waste byproducts by increasing efficiency of processing nuclear fuel. Nuclear reactors have been designed that do not produce weapons-grade plutonium and thereby minimize the risk such materials could be secretly used for illicit weapons production.

Additionally, nations continue to pursue the development of other alternative sources of energy that will reduce dependence on burning hydrocarbons for fuel. Nuclear energy has increasingly become part of integrated and comprehensive energy grid plans that include wind, solar, geothermal, hydro and tidal power generation. Better technology by itself however, is not enough. "In a long-term perspective, nuclear power industry will be more definitely recognized as an essential base load energy source that operates continuously to meet the minimum power demand year round. Therefore, we have to make more efforts not only to develop new technologies to enhance safety and economic efficiency but also to gain public acceptance," Jumpei Matsumoto, senior manager, Mitsubishi Heavy Industries Inc., said at the March 2017 Nuclear Power Asia conference in Kuala Lumpur, Malaysia.

Many of the remaining hurdles to wider use of nuclear power are political, not technical. Government leaders and policymakers need to educate populations on the relative risk of various sources of energy, experts say.

Challenges Ahead

Many challenges remain before nuclear power can be widely adopted in the Indo-Pacific. Those challenges include cooperation among governments, educational institutions and business sectors; human resource development; and proper selection of proven reactors, Kumiaki Moriya, corporate chief engineer, Hitachi-GE Nuclear Energy, explained at the 2017 Nuclear Power Asia conference.

Japan has worked to meet such challenges by organizing events such as sending professors and experts from Japan to other countries for lectures, seminars and trainings, inviting students to learn about technologies at educational institutions in Japan, and using lessons learned from the construction and operation of advanced boiling water reactors, Moriya said.

As a result, Japan has greatly improved its nuclear know-how and shared its lessons with

A Tokyo Electric Power Co. employee walks past storage tanks for contaminated water at the Fukushima Daiichi nuclear power plant in Okuma, Japan, in February 2017.

other countries. The latest generation of reactors that are being installed worldwide employ passive cooling technologies that will cool reactors even in the event of a power failure like the one that occurred in Fukushima.

An increasing number of countries with developing economies in the region are considering turning to nuclear power in the 2025 to 2030 time frame. Bangladesh has signed a contract with Russia to build a plant to be operational there by 2022. Vietnam also signed a contract to start building two plants, construction of which has been delayed. Many other members of the Association of Southeast Asian Nations (ASEAN) are also seriously considering developing nuclear power. Thailand and Indonesia have well-developed plans to do so, and discussions are also underway in Laos, the Philippines, Malaysia and Singapore, WNA reported.

"ASEAN countries face risks similar to [those of] many other countries considering embarking on a nuclear power program. However, given the location of the region, post-Fukushima, the public perception of risk has undoubtedly risen," Anthony Wetherall, a senior research fellow at National University of Singapore, told the Nuclear Power Asia forum in March 2017.

"There is a need to strengthen the regional nuclear governance, in particular, as concerns, greater cooperation/consultation among ASEAN states such as on nuclear safety (e.g., siting of NPPs near borders) and security (e.g., at ports, borders) matters, facilitating increased public and stakeholder participation, dialogue and engagement such as about how risk will be managed as one way to help alleviate fears about new build."

Emerging nuclear energy countries and expanding ones can reduce the risk of future accidents by heeding the lessons learned in previous accidents and from experiences of companies and governments that have operated and overseen nuclear plants for decades. Enhanced regional and international cooperation, coupled with the implementation of good governance practices, will help ensure the growth of nuclear power in the Indo-Pacific brings opportunity for prosperity and better security and not peril to the region. □

Military Mountaineers

INDO-PACIFIC PARTNERS SHARE COLD FACTS ABOUT HIGH-ALTITUDE OPERATIONS

FORUM ILLUSTRATION

FORUM STAFF

When the doors finally opened after a 2½-hour airplane ride, 128 paratroopers braced for the ride of their lives.

They were jumping from an altitude of about 400 meters into an Arctic no man's land — a place called Deadhorse, Alaska — wearing more than 90 kilograms of kit that included snowshoes, weapons and supplies.

"As the paratroopers exit, it's 104 degrees [Fahrenheit] below zero for 2½ seconds until their chute opens," said Maj. Gen. Bryan Owens, former commanding general of U.S. Army Alaska (USARAK). "Once their chute opens, it's minus 63 to the ground, and in four hours of operations on the ground, it's minus 63. It was incredible."

The Soldiers from the 4th Infantry Brigade Combat Team (Airborne), 25th Infantry Division who braved the deadly cold in February 2017 were participating in Spartan Pegasus, an annual cold-weather training exercise in frozen tundra just a few kilometers from the Arctic Ocean.

Training lessons learned during the exercise, which in 2017 was designed to retrieve a downed satellite, and at courses in the Northern Warfare Training Center in Black Rapids, Alaska, can mean the difference between successful missions and tragedy.

In subzero temperatures, the smallest mistakes can be lethal — something like touching a weapon or brushing up against skiing equipment with bare skin.

"Something as simple as skin-to-metal contact is deadly," Owens told *FORUM* during the Association of the U.S. Army Institute of Land Warfare's Land Forces of the Pacific Symposium and Exhibition (LANPAC) in May 2017 in Honolulu, Hawaii. "That will give you instant frostbite. You've got to be careful not to have any of the metal parts touch your skin."

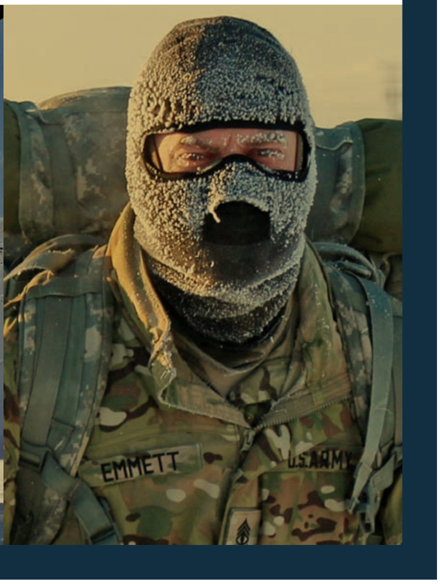
PACIFIC PARTNERS

From North America's tallest peak, Denali, to the majestic Himalayas of Asia to the Andes in South America, many of these military mountaineering and cold-weather lessons are universal. USARAK teams up with Indo-Pacific countries to expose Soldiers to new techniques and challenging environments. USARAK's main mountaineering training partners in the region include India, Japan, Mongolia, Nepal and Chile — all countries with mountainous terrains.

"We look for similarities with our partners in geography and similar challenges that they have," Owens said. "That allows us to share best practices. It allows us to build

U.S. Army 1st Sgt. Jonathan M. Emmett leads Soldiers from an aviation task force through cold-weather training at Fort Wainwright, Alaska. SPC. LILIANA S. MAGERS/U.S. ARMY ALASKA PUBLIC AFFAIRS

U.S. Army Soldiers from B Company, 1st Battalion, 52nd Aviation Regiment prepare to offload equipment and supplies from a CH-47F Chinook helicopter after landing on Kahiltna Glacier during high-altitude training in Alaska. JOHN PENNELL/U.S. ARMY



on each other's strengths. That's been very beneficial for us."

The exchange also has benefited Nepal, which is home to Mount Everest and some of the world's most unforgiving terrain, said Nepal's chief of Army, Gen. Rajendra Chhetri.

In a country where 80 percent of the landscape is mountainous, thriving in high-altitude environments — everything from conducting military operations to rescuing climbers from Everest — is part of everyday life for Nepalese Soldiers, Chhetri said. "There are many challenges we have to face while operating in altitude," Chhetri said. "There are health hazards if you don't properly dress up. With the low oxygen level, you can feel altitude sickness. If you don't have proper gear, frostbite will affect you."

The Nepalese Army shares these lessons with its many partners. It has been operating the Nepal Army's High Altitude and Mountain Warfare Training Academy for more than four decades, Chhetri said. Neighboring Indo-Pacific countries, including Bangladesh, China, Pakistan and Sri Lanka, send their Soldiers to train there, as do the United States, Canada, the United Kingdom and other European countries. "We opened up our altitude warfare school to international students, including U.S. students," Chhetri said. "The U.S. is a regular participant in that course."

While Nepal's Soldiers are extremely experienced at operating in high altitudes, a Mongolian military leader says his country shares insights in these military-to-military exchanges that are derived from centuries of conducting operations in austere environments.

Lt. Col. Shinebayar Dorjnyam, deputy commander of the Mongolian special forces, said through a translator during LANPAC that he attended entry-level high-altitude training in Alaska in 2015 and was impressed with the new technology supplied by the U.S. Army.

While the U.S. provided top technology, the deputy commander said, his Soldiers possess their own secrets of the trade. "We are unique because we still maintain our nomadic lifestyles," he said. "We preserve the skills that we have with that. We know how to make fire, adapt and adjust — free of technology."

THRIVING IN SUBZERO

While survival is difficult in subzero temperatures, Soldiers can't afford to set the bar that low. They train to conduct military operations in environments many people will never experience, Owens said. "A lot of people think you can take a very highly trained unit and put them into extremely cold weather, and they'll sort it out. They'll be able to function there," he said. "That is not the case."

Extensive training, the best equipment and savvy leadership are keys to success. "There's a difference between surviving in a cold region and thriving," he said.

At the Northern Warfare Training Center, Soldiers are taught basic military mountaineering as well as advanced cold-weather skills, which involve heat management — "the ability to dress properly, layer and shed properly so you don't end up perspiring in a cold-weather environment."

"You don't want to perspire in a cold-weather environment," Owens said. "That's very dangerous."

In subzero climates, profuse sweating can cause the body to lose heat quickly, inducing hypothermia.

The human body isn't the only thing that can become sluggish in the Arctic. Equipment does, too. Weapons and helicopters, for example, don't function the same in subzero temperatures as they

Arctic warriors from U.S. Army Alaska's Northern Warfare Training Center train near Galbraith Lake, Alaska.

SGT. 1ST CLASS ADAM MCQUISTON/U.S. ARMY

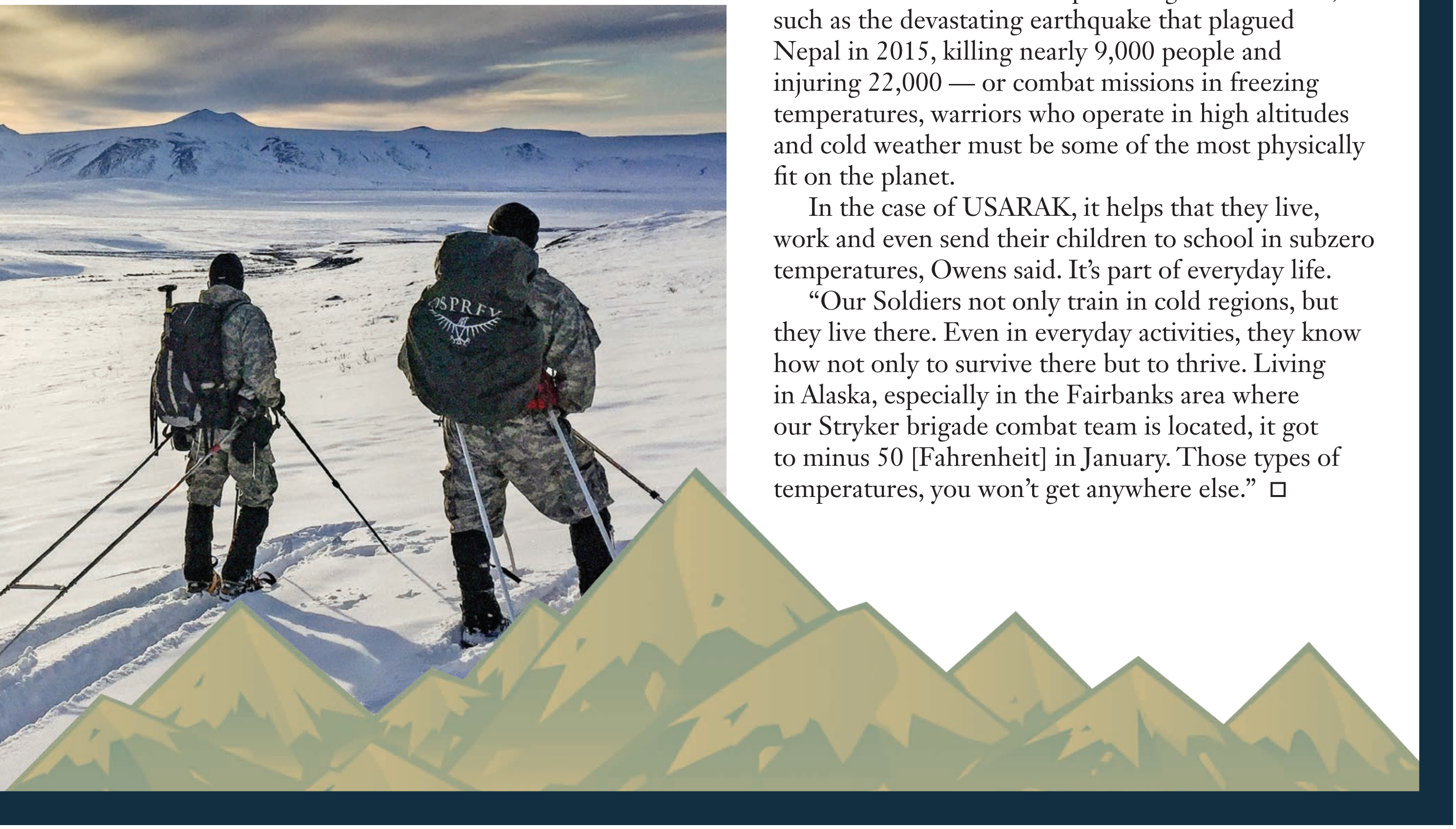
do in warmer climes. Arctic warfighting equipment is tested at the U.S. Army Cold Regions Test Center in Fort Greely, Alaska, and then assessed by Soldiers in USARAK. "We give them feedback on functionality, pitfalls, some improvements they could make," Owens said.

Soldiers assess weapons, skis, vapor-barrier boots, Canadian mukluks, which are high, soft boots traditionally worn in the American Arctic, as well as communications equipment. "In the high north, the look angles to the satellites are very challenging," Owens said.

Keeping aircraft flying is no picnic. When gearing up an Apache helicopter at high altitudes, "it takes about six hours to spool up the electronics on it," Owens said. "Batteries have very little life when you are talking about cold weather. The oils, the hydraulics, are very sluggish."

Even when a Soldier is properly trained and equipped, using a weapon in the freezing cold can be a challenge. "Operating with Arctic mittens is very difficult," Owens said. "It's slow work."

The Soldiers learn how to layer and shed clothes properly, so they don't get frostbite — and to the other extreme — heat exhaustion. Those dangers require trained leaders to detect signs of trouble. "How do you identify when one of your Soldiers is suffering from the first signs of frostbite or heat exhaustion, believe it or not?" Owens said. "There are simple leadership tasks such as making your Soldiers drink water. At minus 40, nobody wants to drink water."



A world away, the challenges of military mountaineering in the Himalayas requires different kinds of equipment. Sometimes the latest technology isn't the best option. "There is limited, almost a nonexistence of roads, in the Nepalese mountains," Chhetri said. "You can't take your vehicle there."

Military operations — whether rescuing climbers from Mount Everest or fighting a decadelong Maoist insurgency that ended in 2006 — must be conducted, regardless of the harshness of the conditions. To get the job done, the Nepalese Army often travels by foot and relies on yak, sheep and mountain donkeys to move equipment, Chhetri said.

Few landing strips exist for fixed-wing aircraft, and in cold seasons, "you can't land there because of snow and ice," he said.

VITAL COMPONENT

With a Stryker brigade combat team and an airborne brigade combat team, USARAK has deployed forces all over the world, including Kosovo, Iraq and Afghanistan. Cold-weather mountain warriors are essential in this global mission because cold regions represent 31 percent of the Earth's surface, and 27 percent of the world has mountainous terrain, Owens said.

Whether the mission is providing disaster relief, such as the devastating earthquake that plagued Nepal in 2015, killing nearly 9,000 people and injuring 22,000 — or combat missions in freezing temperatures, warriors who operate in high altitudes and cold weather must be some of the most physically fit on the planet.

In the case of USARAK, it helps that they live, work and even send their children to school in subzero temperatures, Owens said. It's part of everyday life.

"Our Soldiers not only train in cold regions, but they live there. Even in everyday activities, they know how not only to survive there but to thrive. Living in Alaska, especially in the Fairbanks area where our Stryker brigade combat team is located, it got to minus 50 [Fahrenheit] in January. Those types of temperatures, you won't get anywhere else." □

Building BRIDGES

CMDR. TOM OGDEN/U.S. NAVY

FORUM ILLUSTRATION

U.S. Pacific Fleet Commander Adm. Scott H. Swift fosters innovation with his bottom-up, solution-oriented program

The Bridge started at U.S. Pacific Fleet (U.S. PACFLT) to enable its 140,000 Sailors to share their solutions to Navy-specific challenges. The Bridge helps guide Sailors as they take their ideas from concept to reality.

Commander of U.S. PACFLT Adm. Scott H. Swift has championed this initiative that amplifies an organic Navy network to enable collaboration and idea generation by advancing education, enabling empowerment, stimulating connections and spurring transition.

The Bridge also encourages Sailors to perceive their workplace environment through the lens of innovation; to see challenges as opportunities instead of as roadblocks. The Bridge cultivates Sailors' abilities to create and sustain a culture of change, inspiration and creativity.

In its simplest form, The Bridge is a belief and a commitment — the belief that the best idea can come from anywhere, and a commitment that no Sailor is ever alone in pursuing a solution.

MISSION AND GOAL

The Bridge's mission is to explore, discover and cultivate solutions to fleet-centric challenges. The Bridge's goal is to provide a platform for the U.S. Navy to harness the intellectual surplus of its total force by transitioning combat-effective solutions from concept to prototype to program of record.

VISION

The vision of The Bridge is a future where all U.S. Sailors can contribute to the development of fleet solutions by generating, refining and transitioning their ideas freely through four key pillars: education, connection, empowerment and transition. This foundation advances the Chief of Naval Operations' focus on warfighting, learning faster, strengthening our Navy team and building partnerships. Additionally, it neatly fits into the U.S. PACFLT Commander's guidance to preserve a resilient workforce, be ready to fight, reinforce the international order, lead credibly, embrace opportunity and project power.

Adm. Scott H. Swift

The initial pilot program operated in 2016 from January through May. It consisted of a series of live events open to all uniformed and civilian Sailors on the island of Oahu, Hawaii. The first event was a rapid innovation workshop to teach Sailors how to create and present an effective pitch for their ideas. Subsequent events provided them with opportunities to pitch their ideas to larger audiences and be evaluated by experts, who not only judged the content of their ideas, but helped them refine their presentations.

From these events, two Sailors were selected to brief the U.S. PACFLT Commander and other senior Navy leaders in the Pacific on their ideas, prototypes and proposed paths to transition their concepts into a program of record. The Bridge paired these Sailors with mentors to help guide them in finding organizations that would fund and further test their ideas.

Currently, the program is in its second year and has continued with the same robust success. The Bridge will continue to bring the same excitement and energy that existed in the pilot program to the entire fleet, and it will encourage U.S. PACFLT to be a culture willing to experiment, unafraid to fail and able to solve problems.

Adm. Scott H. Swift answers questions from Sailors assigned to Arleigh Burke-class guided-missile destroyers USS Sterett and USS Dewey at Joint Base Pearl Harbor-Hickam in Hawaii in April 2017.

PETTY OFFICER 1ST CLASS BYRON C. LINDER/U.S. NAVY

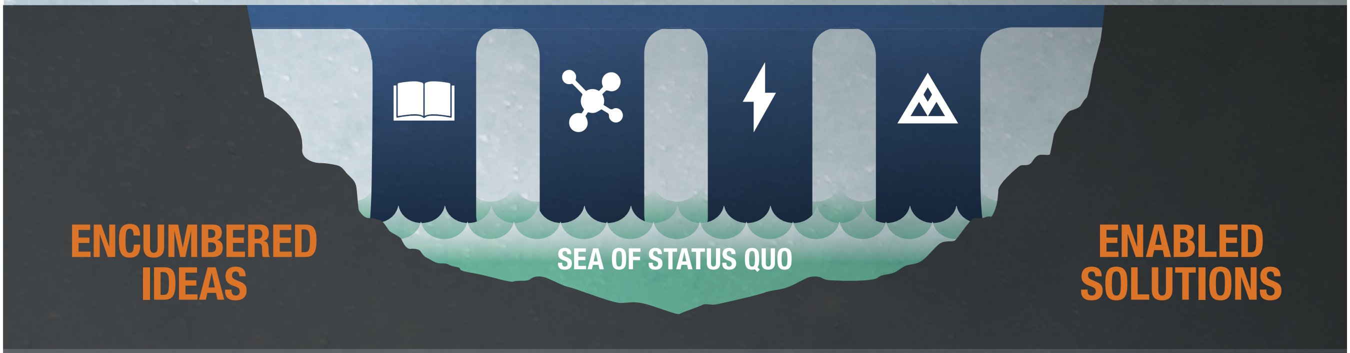
> *"IT'S NOT ABOUT THINKING OUTSIDE THE BOX … IT'S ABOUT EXPANDING THE BOX OF THINKING."*
>
> — Adm. Scott H. Swift, commander, U.S. Pacific Fleet

In the summer of 2017, a five- to six-week fellowship program in the private sector strove to build connections and exchange ideas between the Navy and industry. Another event, a five-day innovation boot camp in spring of 2018, will educate Sailors in topics related to innovation. Through these opportunities, The Bridge is propelling real world learning where high-velocity learning scenarios are examined and practiced.

The Bridge has created a sense of community among the "Bridge Builders" who participate. This community of learning and innovation breaks down barriers to ensure a culture of learning through the ideation life cycle. The Bridge is most successful when key institutional stakeholders are connected and are best positioned to influence the enhancement of our acquisition system's agility, so an idea becomes a true impact. It is a team effort among Sailors who are the problem solvers, senior leaders who endorse and support the innovation process, and the resource sponsors who make it possible to transition the ideas to a program of record.

What makes The Bridge special and successful? As an innovation program that is popular with Sailors and senior leadership

THE BRIDGE PILLARS



EDUCATE

the workforce by providing opportunities for Sailors to learn from each other, industry and through strong academic programs.

CONNECT

those with solutions to those who can enable them. A good idea is strengthened by the number of people who believe in it.

EMPOWER

Sailors to drive positive change within the force. The ability to act comes with a responsibility to act … and with that comes a leader's obligation to empower action.

TRANSITION

solutions from concept to reality.

FORUM ILLUSTRATION

support, The Bridge has demonstrated a clear Sailor-generated demand signal for this type of initiative. In addition to Sailor participation, The Bridge thrives with leadership participation and endorsement. Sailors feel more empowered to share their ideas, knowing they will be heard and supported by their leadership.

The Bridge has the endorsement, participation, and engagement of Adm. Swift and other U.S. Navy senior leaders across the fleet. This has encouraged other leaders to view ideas with an open mind and to build a tolerance for failure. Such an environment builds an entrepreneurial ethos and ecosystem of inquiry in which Sailors are encouraged to take smart risks.

Interactions are customarily face to face, from the first rapid innovation workshop to the inaugural Pitch Fest event, to the mentor meetings, and then finally to the senior leadership presentations. This has allowed meaningful connections to develop between the junior Sailors who brought forth ideas and the senior leaders who could implement them. It also provided a real-time collaborative environment. Feedback is instantaneous, usually actionable and decidedly authentic in a way that generally does not emerge in virtual environments.

The Sailor-generated ideas are notable for what they have in common as well as what differentiates them. They have come from a variety of active duty and civilian Sailors — there was no pattern for the type of applicant who proposed an idea. They also rely on different types of solutions to problems. Together these key differentiators create unparalleled value for Sailors and stakeholders solidifying The Bridge as a broad, reinforced ideation ecosystem. □

BUILDING *a* NETWORK

In tracking terrorists or surviving the jungle, Malaysian general collaborates with partners

FORUM STAFF

Lt. Gen. Datuk Azizan bin Md Delin became field commander west for the Malaysian Army in December 2016. As a commander who is well-versed in regional and domestic defense issues, Azizan spent the previous 1.5 years as chief executive of the Malaysia Institute of Defence and Security. The Defence Ministry formed the institute after a 2009 decision to create a professional think tank to provide analytical research on defense and security issues. In his role as chief executive, Azizan served as principal advisor to the Defence Ministry and to the Malaysian Armed Forces.

Azizan, 57, joined the Armed Forces in January 1979 and was commissioned to the Royal Malay Regiment in April 1981. He earned a law degree from Malaysia's MARA Institute of Technology in 1996 and a master's degree in international security and civil-military relations from the Naval Postgraduate School in the United States. He attended fellowship programs on counterterrorism at National Defense University in Washington, D.C., and international security at Harvard University.

FORUM caught up with Azizan in May 2017 at the U.S. Army Institute of Land Warfare's Land Forces of the Pacific (LANPAC) Symposium and Exposition in Honolulu, Hawaii.

Malaysia has been working with Indonesia and the Philippines to fight piracy and kidnapping for ransom in the Sulu Sea. Can you explain the Malaysian Army's role in that process and what success you are having?

We are having problems in the Sulu Sea, which borders Borneo, east Malaysia and Sabah [a northern Malaysian state]. It's not to say it's a no man's land, but it is a traditional waterway for the Sulu people. The sea is huge, and there are plenty of illegal entry points. It is basically family ties (kidnappers with family links in Malaysia, Indonesia and the Philippines), so historically it is very difficult for us to properly stop them.

There is a lot of kidnapping for ransom. They are sort of like warlords. There are so many small islands, and they are hopping from island to island because nobody's on the islands. We put up sea bases in a joint effort with our oil company, Petronas. We use an oil rig and modified that oil rig to become a sea base that can accept helicopters and then become a forward base for our Navy and Special Forces. The main aim of that base is to cut off the intruders if they are kidnapping somebody or trying to run away. We put in a deterrent factor, showing that we are there. We also have a mobile base that we can move around.

We cannot totally stop their activity. That's why we came up with a trilateral agreement. [In June 2017, Indonesia, Malaysia and the Philippines announced plans for trilateral naval patrols as a show of cooperation to stop terror groups inspired by the Islamic State of Iraq and Syria.] As for the [Malaysian] Army's role, we are occupying a small island and we are at our shore to ensure that if they

Lt. Gen. Datuk Azizan bin Md Delin MALAYSIAN ARMED FORCES

A Malaysian staff sergeant watches a U.S. Army master sergeant start a fire by using only a metal blade, a rock and dried plants during survival training in Malaysia. U.S. ARMY

A Malaysian Ranger cuts open a python as he shows U.S. Marines how to prepare the snake for food. U.S. MARINE CORPS

come in and try to kidnap anybody, we are there. We divide the area between the military and the police to cover as much territory as we can. At the moment, it seems that we can contain the activity. It is quite impossible to be successful 100 percent, but their activity is decreasing very much.

How are the Malaysian Armed Forces prepared to deal with the return of terrorists affiliated with ISIS?

We are prepared for it. We hope they stay there [in Syria and Iraq] or that somebody finishes them off over there. But if they come back, they are not going to come back to a place that is in order, so they will go maybe to the southern Philippines. It's not to say it is lawless, but the authority over there comes in and then goes out. The area belongs to them [terror groups]. Most likely they will come back to that area. That is our prediction.

How have the U.S. Army and the Malaysian Army worked together in fighting terrorism?

We have a very good bilateral relationship, especially with the U.S. Army. USPACOM [U.S. Pacific Command] always is there with us. We can undergo any training, individual training, with the U.S. Army. Then we have the collective training. Our Soldiers come over many times to Hawaii. And similarly, we also provide special-skills training, jungle training and survival training to the U.S. Army. That's been going on for a very long time.

Malaysia is known for having one of the best jungle warfare training schools in the world. You send mobile training teams to Hawaii to train Soldiers from the U.S. Army. There are elements of basic survival training in the jungle climate that can't be practiced as easily in Hawaii as in the jungles of Malaysia. What does the training in Malaysia entail?

That [jungle warfare] is our skill. The training involves how to survive when you are alone. You learn how to eat snake, how to eat frog.

What countries come to Malaysia to receive jungle warfare training?

The U.K. [United Kingdom], Australia, Singapore, Thailand, Indonesia and Vietnam. We've also brought in a few African countries.

A U.S. Marine Corps corporal drinks water from a vine during jungle survival training in Kemaman Terengganu, Malaysia. U.S. MARINE CORPS

Malaysia hosted the 40th Pacific Armies Management Seminar (PAMS) in September 2016, drawing leaders from 30 armies. How did the Malaysian Armed Forces benefit from the event?

Of course, when given the opportunity to host it, we want to put forth the very best. And when people acknowledge that we hosted PAMS successfully, we feel very satisfied about it. Secondly, whenever there is a PAMS, that means chiefs of army converse. They have exchanges of ideas. And by doing so, we improve our bilateral or multilateral relationships.

Why do you attend conferences such as LANPAC?

It's a convergence of chiefs of army. My chief attended last year. … This year, he sent me. We can gather the latest information about military strategy. By attending LANPAC, when I go back, I'll make a report and disseminate that information to the Army. □

Soldiers from the U.S. and Malaysian armies gather at the parade field during the opening ceremony for Operation Keris Strike, a bilateral exercise.

PFC. JUDGE JONES/U.S. ARMY

Finding Common Ground on Regional Security

GEN. (RET.) RYAMIZARD RYACUDU/MINISTER OF DEFENSE, INDONESIA

PHOTOS BY THE ASSOCIATED PRESS

Indonesia affirms the importance of the Shangri-La Dialogue forum as a medium to strengthen productive, interactive communication among participants as well as to seek common understandings and common grounds that lead to finding a common solution in addressing our common challenges that can undermine regional peace and stability. In the end, this forum is expected to contribute to making a defense policy aimed at the realization of the peace and prosperity for the respective people, as promised by every leader when campaigning to win election. At the same time, this forum can also help turn uncertainty into certainty.

Indonesia reiterates the need of every leader in ASEAN [Association of Southeast Asian Nations] together with its partner nations to increase our commonalities and similarities and at the same time eliminate or decrease our differences that weaken our spirit of brotherhood that align with the strong spirit of ASEAN and spirit of ASEAN Plus. With these modalities, we all can resolve any common challenges and obstruction with the peaceful spirit of ASEAN as our legacy since its establishment 50 years ago.

Some modalities and commonalities that we have in the region as the foundation of our unified cooperation among members of ASEAN and its partner nations include that we face common threats ranging from terrorism and radicalism, separatism and armed uprising, natural disasters, border violations, robbery and theft of natural resources to disease epidemics, the drug trade and abuse of narcotics.

On this special occasion today, I will focus mainly on Indonesia's perspective to cope with the development of the threatening global and regional threat of terrorism and militancy in our region. The terrorism threat in this region has turned into an unprecedented immediate level of emergency. The Daesh [Islamic State of Iraq and Syria, or ISIS] group's area of operation has gone global and is not limited to the Middle East. Now they have entered the strong perimeter of defense around Europe and Asia as we witness the terror attacks in Manchester, Indonesia and Egypt and the ISIS attack in Marawi in the southern Philippines.

Based on data from the U.S. Central Intelligence Agency, in late 2016, the strength of ISIS was more than 31,500 fighters and 11,000 sympathizers. In Southeast Asia, it's estimated there are about 1,000 sympathizers. With this amount, the world has been overwhelmed, bothered and begun to fear acts by terrorist groups. Given that Indonesia is the world's largest Muslim country, with about 200 million people, if half a percent become sympathizers of ISIS, it means about 1 million sympathizers. It is a terrible number.

ISIS' ideology is not about Islam or culture. Indonesia strongly rejects and resists ISIS and will give no room to this group in Indonesian territory. Indonesia will stay steadfast and support the intelligence and information in the region to crush terrorism.

Indonesia's large number of Muslims are prime targets for being influenced by the radicalism of this ISIS group. The results of a survey in December 2015 indicated that 96 percent of Indonesians are adamantly opposed to the ISIS ideology. However, 4 percent of the respondents chose not to answer.

In the book *The Future of Power* by Joseph Nye, it is written that physical action using guns or hard

Indonesian police guard a building where a suspected terrorist was shot during a stand-off with anti-terror police in February 2017.

ISIS' ideology is not about Islam or culture. **Indonesia strongly rejects and resists ISIS** and will give no room to this group in Indonesian territory. Indonesia will stay steadfast and support the intelligence and information in the region to crush terrorism.

~ Gen. (Ret.) Ryamizard Ryacudu,
minister of defense, Indonesia

power will only contribute 1 percent in resolving the basic root of terrorism, while 99 percent of the solution is through soft power with the involvement of all people in the nations by socializing the spirit of nationalism and love of the nation. In our country, we call this the spirit of *Bela Negara*, or defending the nations.

In my capacity as Indonesia defense minister, I have designed a heart-based and people-oriented defense strategy. I call it the Smart Power Defence Strategy, which combines our defense diplomacy approach and building our defending capability through total war, which include the strengthening of the people's power, spirit and their mindset, the *Bela Negara* program supported by defense force capability and its armament. The spirit behind this strategy is based on our traditional value of respect, tolerance, caring, sincere sacrifice for the nations. All of these values are reflected in our ideology and guidelines principle known as Pancasila.

In light of the above, I would like to take this opportunity to propose the establishment of a more concrete and pragmatic concerted platform of regional cooperation and collaboration — a broader level of cooperation and engagement than the existing one. A concrete example of this is the establishment of the trilateral arrangement on the Sulu waters between Indonesia, Malaysia and the Philippines. Initially, the objective of this establishment was to fight piracy, but note this platform has been expanded and extended to fight the development of ISIS in the region.

Currently, Indonesia and Malaysia are often faced with piracy, and crews are taken hostage by the radical Abu Sayyaf Group. Indonesia highly appreciates that the government of the Philippines has deployed its military to crack down on the radical group and release the hostages. To address threats to the stability, security and peace in the region, Indonesia, Malaysia and the Philippines have held a trilateral meeting to discuss maritime cooperation for the security and safety of the ships and people who are crossing the waters in the areas of common concern. To implement this maritime cooperation, the three countries signed the framework of arrangement (FOA) in which the standard operating procedure (SOP) on coordinated maritime patrols is one of the annexes.

The three defense ministers have held meetings several times to make a collective agreement that was followed by a joint working group to finalize the SOP for corridor transit, sea marshal, establishment of a joint command post, and so forth. A major step forward by Indonesia, Malaysia and the Philippines would be to accelerate implementation of the FOA, planning for joint exercises on land by the three armed forces, joint operations and the possibility to develop trilateral cooperation involving other countries, such as Thailand and Singapore. Trilateral cooperation is not only intended to prevent piracy and hostages but also to prevent the spread of transnational crime. Indonesia argues that the correlation between maritime domain awareness and the implementation of coordinated maritime patrols can be realized with capacity building programs. Also, it is open to other countries outside the region only for capacity building and technical assistance, according to the agreement of coastal states in the region.

The key point in responding to security threats is through security consultations undertaken bilaterally and multilaterally, with the purpose to resolve tensions and to prevent the spread of the conflict.

I believe that no single country can resolve security threats independently. It requires cooperation among countries in the region.

Currently, we have three platforms of cooperation in the region which are joint patrols in the Malacca Strait, maritime security cooperation in the Gulf of Thailand and the trilateral arrangement in the Sulu waters. In the future, we should also consider the involvement of other countries, such as Singapore, Vietnam and other ASEAN countries, to expand our capacity and our capability.

The current strength of the active military in this trilateral arrangement is 1 million personnel, a collaboration that has covered one-third of the region of South China Sea. With the ASEAN population of 569 million people as well as 2.6 million military personnel, ASEAN is more than ready to defend its own region.

The security forums in the region that we have, such as the ADMM [ASEAN Defense Ministers Meeting], the ARF [ASEAN Regional Forum], the East Asian Summit and other ASEAN regional forums and Shangri-La Dialogue and joint patrol in Malacca Strait, must be optimized to build trust and cooperation to strengthen the existing security architecture.

Respecting the sovereignty of a nation is the key point, and that can't be compromised. We can't afford to intervene in other nations' territorial integrity without their consent. Noting the current dynamic development in our region, allow me to underline the importance of common understanding in addressing our common challenges. It is imperative to enlarge our commonalities and decrease our differences in our endeavor to achieve our common security and prosperity. □

Indonesia's minister of defense, retired Gen. Ryamizard Ryacudu, delivered this speech June 4, 2017, during the Shangri-La Dialogue in Singapore. It has been edited to fit *FORUM*'s format.

REVIVAL *of a* ONCE-FORBIDDEN RITUAL *in* VIETNAM

REUTERS

Dressed in the bright silk garments of a woman and dancing with candles between his fingers, Nguyen Duy Nam leads a temple of worshippers in a ceremony honoring mystical goddesses of forest, water and heaven.

Nam, 24, is one of a growing number of spirit mediums who perform the Hau Dong ritual of blaring noise and vibrant colors, now enjoying a resurgence after once being frowned on by the ruling Communist Party.

"It's like an illusion, like a soul has taken over my body," said Nam, who works in a garage in Hanoi, the capital, when he is not performing Hau Dong.

Dating to the 16th century, Hau Dong centers on a belief in the mother goddesses of three realms: forest, water and heaven. It draws from elements of Taoism, Buddhism and other religions.

During rituals, spirit mediums dance to loud folk music while appearing to transform themselves into different characters from legend and history. They display changing personalities as if different spirits have entered their bodies. Sometimes they say it feels real. "One time I couldn't even move my body and just cried for no reason, but then I returned to normal when the next character came," Nam recalled.

Believers kneel behind mediums and cheerfully grab money thrown by the spirits. Spread on the floor are offerings for the goddesses and the spirits, which can be anything from money to instant noodles to life-size paper horses. "It's for every class of society, from rich to poor, from officials to citizens and from the mountain to the plain," said architect and researcher Doan Ky Thanh.

Thanh said the appeal of the ritual broadened because it attracts participants of either gender.

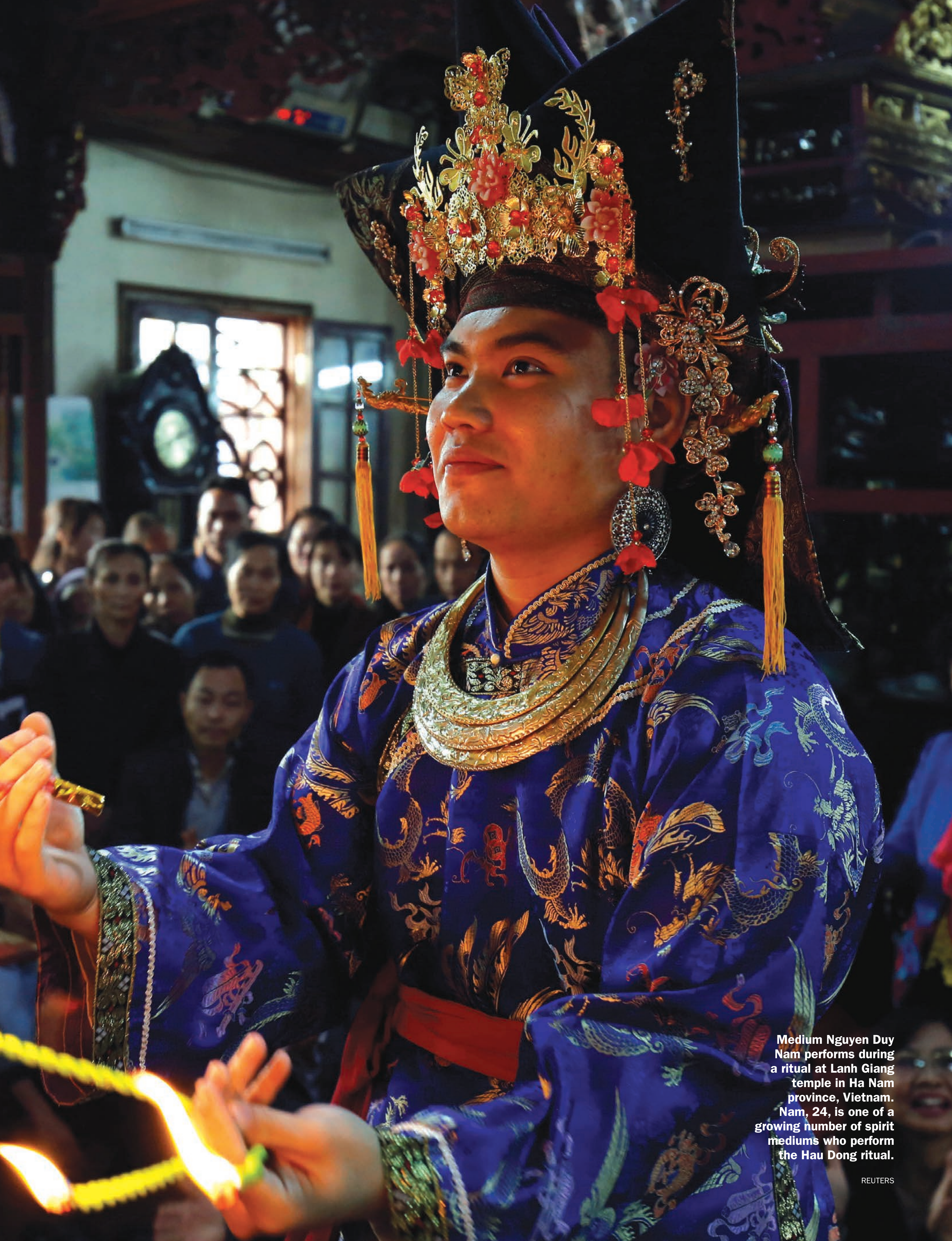
Hau Dong's status was reaffirmed in 2016 when it was recognized as part of the Cultural Heritage of Humanity by the United Nations educational, scientific and cultural organization, UNESCO.

In 2005, the Communist Party lifted a ban on Hau Dong, which until then it had regarded as superstitious. Interest in the ritual has since grown, as economic liberalization has brought greater wealth and social openness.

Hau Dong is not predominantly about money, but offerings to the spirits and temples can run into hundreds of thousands of dollars for a single ceremony. Although the state frowns on wasting money, sponsoring a ceremony can be a status symbol.

Nam said he gave up the reckless lifestyle of his youth after being called by the saints to become a medium. That spurred him to work hard in his daily occupation, paying off in the ownership of two garages.

He is dedicated to continuing as a medium, whatever anyone thinks of him dressing as a woman and summoning spirits. For now, only his close family knows it's part of his life. "It's my lifetime duty," he said.



Medium Nguyen Duy Nam performs during a ritual at Lanh Giang temple in Ha Nam province, Vietnam. Nam, 24, is one of a growing number of spirit mediums who perform the Hau Dong ritual.

REUTERS

THE LITTLE CANOE THAT COULD

UNITED STATES

No modern navigation instrumentation guided a Polynesian voyaging canoe as it followed the horizon during a three-year journey around the globe that ended in June 2017 near the Hawaiian island of Oahu.

About a dozen crew members for each leg of the voyage relied only on their understanding of nature's cues — ocean swells, stars, wind, birds — and their own *naau*, or gut, to sail across about 40,000 nautical miles (74,000 kilometers) to 19 countries, spreading a message of *malama honua*: caring for the Earth.

Ka'iulani Murphy, an apprentice navigator on Hokulea, the double-hulled canoe, said the successful journey taught her the value of ancient Polynesian maritime techniques. "We really are sailing in their [the ancestors'] wake," said Murphy, 38. "We had to relearn what our ancestors had mastered."

The toughest part of the journey was dealing with cloud cover and trying to maintain the proper speed so the boat escorting the canoe could keep pace, she said.

Bert Wong went to Ala Moana Beach Park to celebrate Hokulea's homecoming — and to celebrate his son, Kaleo, a Hokulea navigator, according to Hawaii News Now. "Just being here and feeling the *mana* [power] that's here, it's something to enjoy, which brings tears to my eyes," Wong said.

The voyage perpetuated the traditional wayfinding that brought the first Polynesians several thousand miles to Hawaii hundreds of years ago. The trip also helped train a new generation of young navigators.

Hokulea means star of gladness. The canoe was built and launched in the 1970s, when there were no Polynesian navigators left. So, the Voyaging Society looked beyond Polynesia to find one.

Mau Piailug, from a small island called Satawal in Micronesia, was among the last half-dozen people in the world to practice the art of traditional navigation and agreed to guide Hokulea to Tahiti in 1976.

"Without him, our voyaging would never have taken place," the Polynesian Voyaging Society said on the website for Hokulea. "Mau was the only traditional navigator who was willing and able to reach beyond his culture to ours."

Crew members hope the success of their journey will inspire other indigenous cultures to rediscover and revive traditions. The Associated Press

ROBOCOP To The Rescue

UNITED ARAB EMIRATES

A robotic policeman that can help identify wanted criminals and collect evidence has joined the force in Dubai, United Arab Emirates, and will patrol busy areas in the city. He is part of a government program aimed at replacing some human crime fighters with machines. If the Robocop experiment is successful, Dubai police say the department wants the unarmed robots to make up 25 percent of its patrolling force by 2030.

Clad in Dubai Police colors, the wheeled robot, which can shake hands and salute, is part of a government plan to use technology to improve services and security.

"These kind of robots can work 24/7. They won't ask you for leave, sick leave or maternity leave. [They] can work around the clock," said Brig. Khalid Nasser Al Razooqi, director general of the Smart Services Department at Dubai Police.

The first automated police officer in the Middle East, the robot comes with cameras and facial recognition software. It can compare faces with a police database and read vehicle license plates. Its video feed can help police watch for risks such as unattended bags.

The public can report a crime verbally or via a touch-screen computer embedded in its chest.

"We now see the new generations who are using smart devices," Razooqi said. "They love to use these kind of tools." Reuters

WILL GIANT SEA WALL PLAN SINK OR SWIM IN JAKARTA?

REUTERS

Indonesia's bustling capital, Jakarta, is sinking faster than any city in the world. An ambitious plan, however, to build a giant wall to keep out the encroaching sea has come under fire from fishermen who fear for their catches and homes and from water experts who say it doesn't do enough to tackle the sinking land, also known as subsidence.

The city's northern areas have sunk 4 meters in the past 40 years, Japanese experts say, while some "hot spots" are said to be dropping as much as 20 centimeters a year.

The 10 million residents of the low-lying coastal city, built on a swampy plain, are exposed to tidal and seasonal flooding. In 2013, parts were submerged under nearly 2 meters of water after a heavy monsoon storm.

A child watches a worker helping to build part of a concrete sea wall in Jakarta in August 2017.

Jakarta's vulnerability to floods, already exacerbated by population growth, urbanization and changing land use, rises with every centimeter the ground falls.

Experts and residents agree that overextraction of groundwater for drinking and commercial use is largely responsible for the land subsidence. What they don't agree on is how to tackle it. An iconic infrastructure project that is supposed to ease Jakarta's flooding woes is mired in uncertainty.

The Dutch, regarded as the foremost authorities on the concept of "living with water," are lending their expertise via the flood prevention plan involving a giant sea wall that will close off Jakarta Bay, which could cost up to U.S. $40 billion.

Critics, however, say the National Capital Integrated Coastal Development (NCICD) program does not address land subsidence, the underlying reason for flooding.

At the same time, "the government is throwing away access to the sea" for tens of thousands of people in the bay who rely on fishing and fish processing, said Ahmad Marthin Hadiwinata of the Indonesia Traditional Fisherfolk Union.

He worries that residents will be evicted from their homes to make way for the new infrastructure.

Unveiled in 2014 and better known as the "great garuda" or "giant sea wall," the project involves raising and strengthening the existing onshore embankment of Jakarta Bay, as well as constructing a 24-kilometer outer sea wall and developing real estate on artificial islands reclaimed from the ocean.

Seen from the air, the mega construction project was initially shaped like a garuda, the bird-god of Hindu mythology that is Indonesia's national symbol.

The design was changed in response to opposition and a government request to incorporate another project led by private developers to build 17 artificial islands, said Victor Coenen, Indonesia representative for Witteveen+Bos, a Dutch engineering consultancy leading the NCICD consortium.

Its partners, which also include South Korea, are now awaiting the government's decision on the final plan, he added.

A June 2017 document outlining an updated NCICD master plan confirmed the new design and emphasized the importance of stopping land subsidence, as well as addressing water and sanitation issues.

Many, including Hadiwinata, hope Anies Baswedan, who won a hard-fought election for the post of Jakarta governor in April 2017, will stop or modify the project when he takes office in October 2017. Officials suspended work for several months in 2016 amid regulatory and environmental concerns.

Coenen said stopping land subsidence is important but could take 15 to 20 years, meaning Jakarta should work on flood prevention at the same time. The future of the crowded city's flood protection lies offshore because it has no space for flood basins, he added.

"It's only a question of how far offshore you go, how big you want to build, and how long you want it to last, because the smaller the scheme, the shorter the lifetime will be," he said.

AFP/GETTY IMAGES

OUT-OF-POCKET EXPENSE

A superstitious passenger delayed a flight from Shanghai for several hours in June 2017 after throwing coins at the plane's engine for good luck, Chinese officials said.

The elderly woman was detained by police at Shanghai Pudong International Airport following the bizarre incident, forcing nearly 150 passengers to be evacuated from the plane bound for Guangzhou in southern China.

The 80-year-old threw nine coins at an engine of China Southern Airlines flight CZ380 as she was boarding on the tarmac. Eight of the coins missed their target, but one nestled inside an engine, airport police said, adding that a passenger spotted her and reported it to authorities.

The woman was traveling with her husband, daughter and son-in-law, *Beijing Youth Daily* newspaper reported.

"A senior passenger threw coins to the plane's engine and delayed the flight. The passenger involved has been taken away by police," China Southern Airlines said in a statement on its Twitter-like Weibo account.

The incident was soon trending on Weibo, and police added in a statement that the passenger threw the coins at the engines to pray for safety. Agence France-Presse

AFP/GETTY IMAGES

SUPER SUCTION

The clinging power of octopus tentacles has inspired a breakthrough adhesive patch that works on wet and oily surfaces with potentially huge medical and industrial uses, according to South Korean researchers.

Octopuses are among the most intelligent and behaviorally diverse of all invertebrates, but it was their extreme strength that attracted the interest of the research team from Sungkyunkwan University. "Two years ago, we bought an octopus from a Lotte Supermarket, put its suction cups under a microscope and analyzed how they worked," researcher Baik Sang-yul said.

The team found the octopus' impressive suction power was generated by small balls inside the suction cups that line each tentacle. The new "wet-tolerant" adhesive patch has been hailed as a breakthrough by the country's Science and Technology Ministry, and there are hopes it will be used for everything from heavy industry to dressing wounds.

Professor Pang Chang-hyun said polymer patches covered with micro suction cups are so strong that a patch the size of a thumbnail can lift an object weighing up to 400 grams in water. One patch can survive more than 10,000 cycles of attachment and detachment. Agence France-Presse

A PLEDGE TO PALAU

Visitors to the tiny Pacific nation of Palau are being made to sign a promise to respect the environment, an innovative move that authorities hope will curb ecological damage caused by booming numbers of tourists.

Claimed to be a world first, the "Palau Pledge" is stamped onto visitors' passports and must be signed upon arrival in the country, situated in the western Pacific about halfway between Australia and Japan.

"I take this pledge as your guest, to protect and preserve your beautiful island home," it reads in part. "I vow to tread lightly, act kindly and explore mindfully."

With crystal clear waters, pristine reefs and abundant sea life, Palau is regarded as one of the world's best diving spots and was once a niche tourist destination.

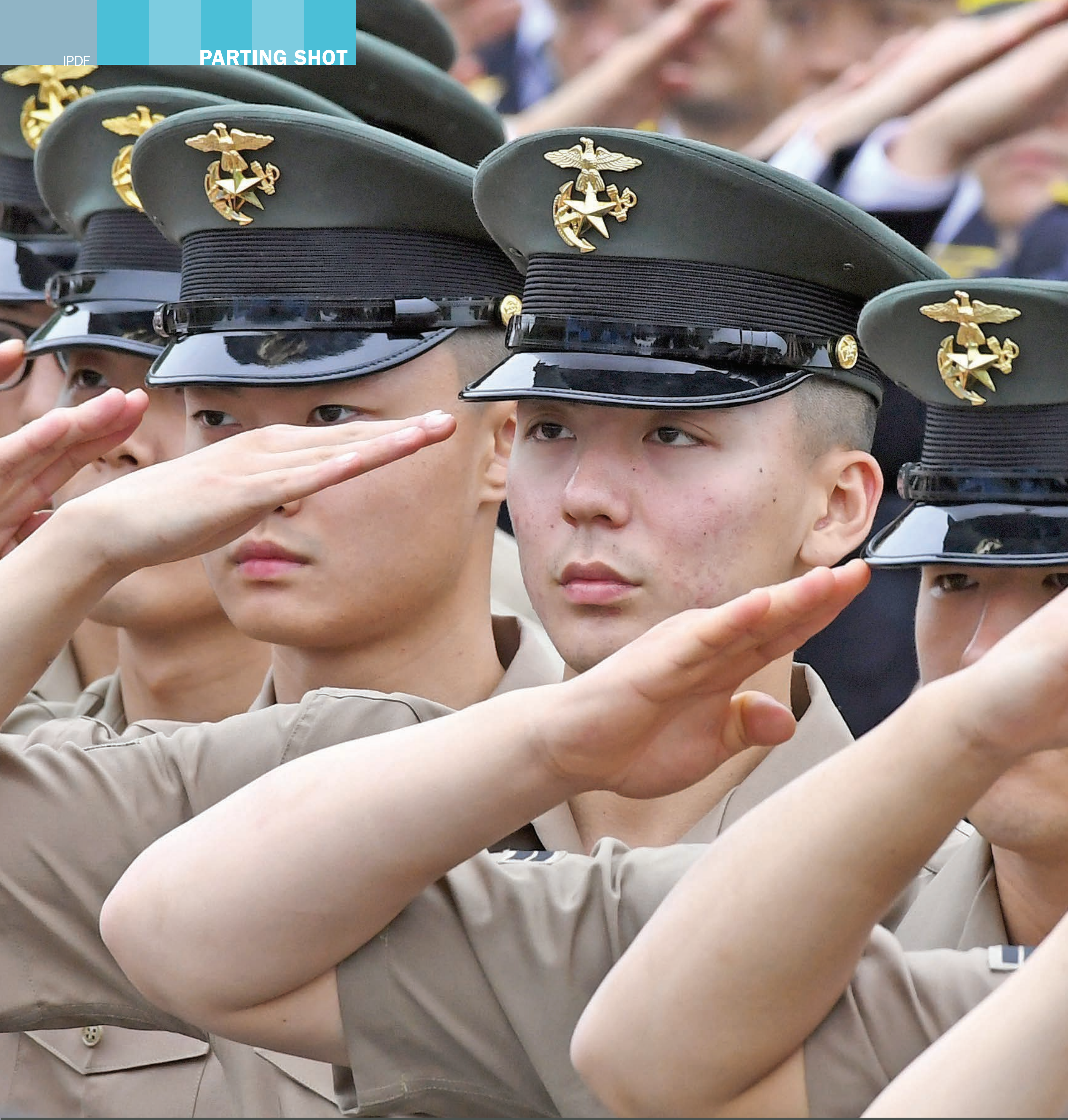
Visitor numbers have exploded in recent years, particularly from China, straining both infrastructure and the environment.

The symbolic pledge was written with the help of Palau's children, and President Tommy Remengesau said it was about preserving the environment for future generations.

"Conservation is at the heart of our culture," he said. "We rely on our environment to survive, and if our beautiful country is lost to environmental degradation, we will be the last generation to enjoy both its beauty and life-sustaining biodiversity."

Palau welcomed almost 150,000 tourists in 2016, up 70 percent from 2010 , and the nation of 20,000 has struggled to cope. Agence France-Presse

REUTERS



HONORING THE FALLEN

Republic of Korea Marines salute during a ceremony to honor those killed in the Korean War from 1950 to 1953. Participants attended the Memorial Day ceremony at the National Cemetery in Seoul, South Korea, on June 6, 2017. An estimated 415,000 South Koreans were killed during the war.

Photo By: **JUNG YEON-JE** | AFP/Getty Images

RELEVANT. REVEALING.
ONLINE.

www.ipdefenseforum.com

TRENDING STORIES
U.S. Navy says China's military buildup won't stop patrols
Four nations may collaborate on alternative to China's Belt and Road
INDO-PACIFIC DEFENSE FORUM
HOME
FEATURES
DEPARTMENTS
CONTRIBUTORS
ABOUT US
ARCHIVES
SUBSCRIBE
ENGLISH
INDONESIA
Top Stories
March 13, 2018
Australia-U.S. seek common ground on trade, China
Features
Unpredictable Behavior
Deducing Russia's South China Sea policy
What Lies Beneath
Departments
Australia: Stomping Ground for Giants
Indo-Asia-Pacific View
Follow IAPDF
Tweets
Categories
Across The Region
Contemplations
Culture & Custom
Current Issue
Departments
NEW ZEALAND: The Lost
BREAKING NEWS
U.S. ponders China's commitment
Select Menu
December 09, 2015
U.S.-donated ship to bolster Philippine presence in South China Sea
Chinese hospital ship continues goodwill tour

NEW CONTENT POSTED DAILY!

FREE MAGAZINE SUBSCRIPTION

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

FOR A FREE MAGAZINE SUBSCRIPTION:

www.ipdefenseforum.com/subscribe

write: *IPD 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 and Twitter.