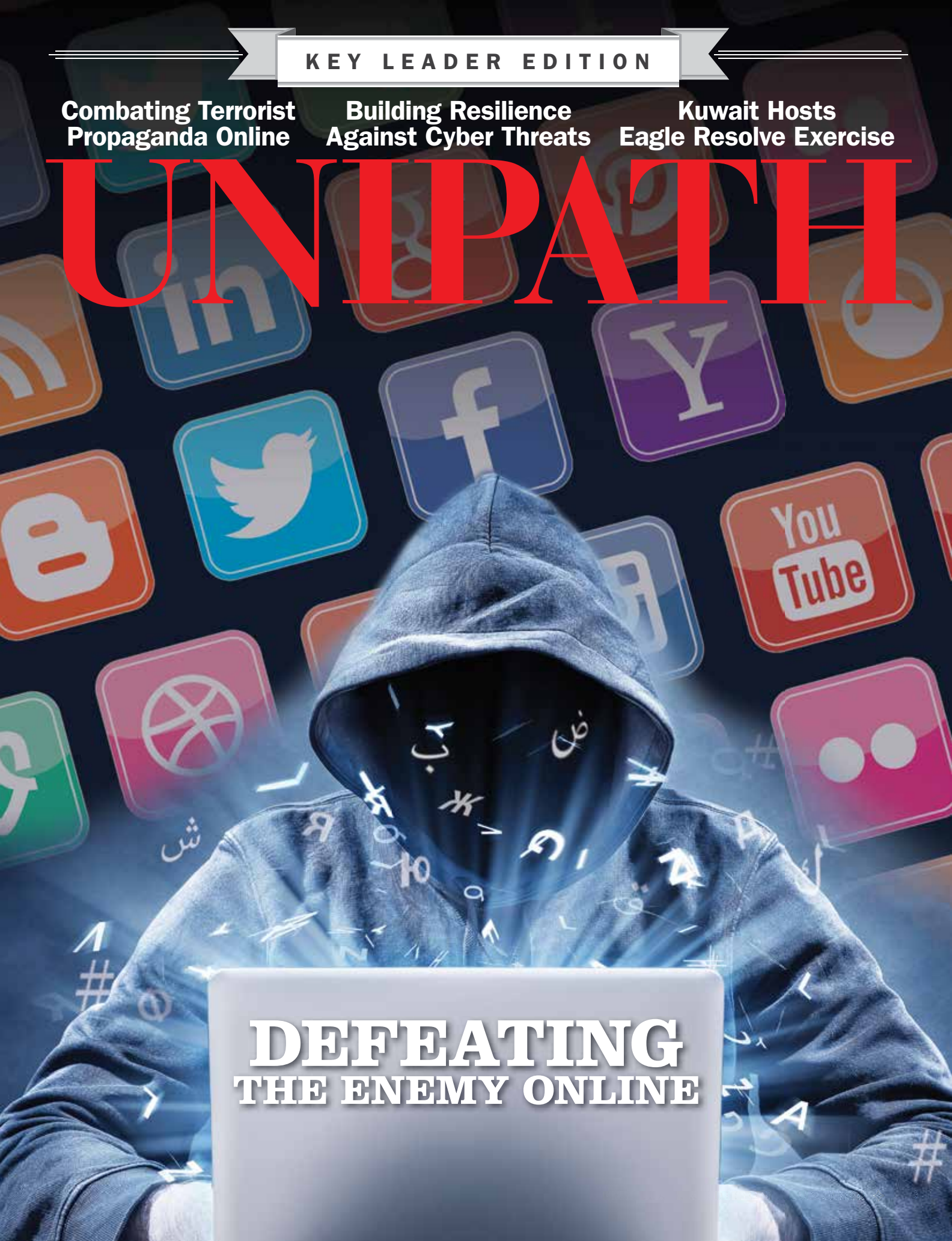
KEY LEADER EDITION

Combating Terrorist Propaganda Online

Building Resilience Against Cyber Threats

Kuwait Hosts Eagle Resolve Exercise

UNIPATH



DEFEATING THE ENEMY ONLINE

OPENING
SHOTS

The National Theatre in Manama, Bahrain, opened in 2012 and is the third-largest theater in the Middle East.
ISTOCK

A Kuwaiti boy with baskets of shrimp at the main fish market in Kuwait City

GETTY IMAGES

TABLE OF CONTENTS

6 Building a Regional Cyber Partnership
USCENTCOM expands the Central Region Communications Conference

10 Combating Cyber Crime in the Kingdom of Bahrain
We are committed to continuing international collaboration and offering practical experience that supports international partnerships in combating crime
By Amer S. Mustafa, Bahrain Cyber Crime Directorate

14 Cyber Security in Afghanistan
Online threats grow as the nation adopts information technology
By Zmarialai Wafa, Afghan Ministry of Communications and Information Technology

18 Iraq battles Da'ish Online
By Haider S. Alkenani, Iraqi Counter Terrorism Office director of public relations

20 Cyber Drill Boosts Innovation in Qatar
Testing the resilience of the government, energy and financial sectors
By Khalid Al-Hashimi, assistant undersecretary for cyber security, Qatar

24 Protecting Cyberspace
The UAE leads in online national defense tactics

28 Strength in Unity
Eager Lion military exercise brings together militaries from 18 countries

34 Defending the Gulf
Kuwait hosts the largest Eagle Resolve exercise in 16 years

40 Senior Leader Profile
Dr. Sherif Hashem, vice president for cyber security at the Egyptian National Telecom Regulatory Authority

42 Around the Region

BONUS ONLINE ARTICLES

Strengthening Special Operations Partnerships
By Col. Ibrahim Alharahsheh, Jordanian Special Operations Command

Sources of Cyber Threats
Terrorists, criminals, hostile governments and disgruntled insiders pose threats to information systems

Biometrics Build Border Security
Sharing data among countries strengthens regional security

Central Asian Cyber Security
The fight against Internet crime must not undermine good governance
By Nuria Kutnaeva, independent researcher, Kyrgyz Republic

The Terrorist Use of Social Media
A successful cyber strategy combines hard and soft power

To read these stories, go to:
http://unipath-magazine.com

ON THE COVER:
Countries must target terrorists who use social media to spread their propaganda.
UNIPATH ILLUSTRATION

UNIPATH

Defeating the Enemy Online

Volume 6, Number 1

CENTCOM COMMANDER
GENERAL
LLOYD J. AUSTIN III
U.S. Army

CONTACT US

Unipath
c/o Commander
U.S. Central Command
7115 S. Boundary Blvd.
MacDill AFB, FL 33621
USA

unipath@centcom.mil

Unipath is a professional military magazine published quarterly by the Commander of the United States Central Command as an international forum for military personnel in the Middle East and Central Asia region. 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. Select articles are written by *Unipath*'s staff, with credit for other content noted as needed. The Secretary of Defense has determined that publication of this magazine is necessary for conducting public business as required of the Department of Defense by law.

ISSN 2333-1844 (print)
ISSN 2333-1852 (online)

KEY LEADER'S MESSAGE

United States Central Command (USCENTCOM) and our regional partners face a common threat in cyberspace. Various adversaries with substantial cyber offensive capabilities intend to exploit and disrupt information infrastructure essential to regional and global economies and regional security and stability. Building a strong partnership and spirit of cooperation are critical to understanding and addressing this threat. Collectively, we must operate and defend our critical information technology (IT) infrastructure and networks using common principles for responsible behavior in cyberspace.

Information sharing and continued collaboration between partner nations is critical. Likewise, relationships with private industry and academia are also important to remain on the cutting edge and continue to adapt to the dynamically changing cyberspace environment.

Many of our critical government and military IT systems depend on industry-provided network infrastructure. Therefore, the need to build reliable partners in industry cannot be overstated. Cyber security cooperation is about sharing best practices and strengthening bilateral and multilateral partnerships.

Currently, United States Central Command and our regional partners use a variety of venues to share information and best practices, generate dialogue, and make progress in building cyber security capacity within the region:

- Central Region Communications Conference (CRCC)
- Key Leader Engagements (KLE) and Cyber Subject Matter Exchanges, Assessments, and Workshops
- C2 Interoperability Working Group (CIWG)
- Command and Control Interoperability Board (CCIB)
- Coalition Military Exercises

In partnership with the Office of the Secretary of Defense and the Department of Defense Chief Information Officer, the United States Central Command engagements and partnerships illustrate that protecting vital information systems starts at the top with responsible IT governance and a whole-of-government approach. Successful implementation of a cyber security strategy relies on a trained, educated and certified work force. This begins with basic users, often the weakest link, becoming certified to a baseline standard. Training, education, and certification are even more critical for system administrators, network administrators, and cyber security professionals.

Hardening networks requires a solid architecture that identifies points of failure and eliminates vulnerabilities in the IT infrastructure, employing sensors and establishing common standards for operating, defending, and improving the IT networks. It's important to be able to rapidly respond to a cyber threat and take appropriate action to mitigate the risk and minimize the impact to operations. As such, we all need Computer Emergency Response Teams, composed of cyber security experts to rapidly respond during a significant cyber incident.

In partnership with whole-of-government and Department of Defense cyber experts, USCENTCOM conducts Cyber Security Assessments with regional ministries of defense to scope specific cyber security cooperation initiatives and prepare a tailored road map to build or enhance cyber security capacity and capabilities. These assessments provide detailed recommendations to enhance training, organizing and equipping of cyber forces, set the stage for development of foreign military sales cases and certification programs, and help to identify the need for follow-on assessments or training. Generally, these exchanges focus on four lines of effort:

Line of Effort 1 – Policy, Strategy and Organization

- Specific recommendations to improve or develop Cyber Defense Strategy, policy and organization

Line of Effort 2 – Workforce Development

- Specific recommendations to develop a cyber workforce to include a tailored training regime

Line of Effort 3 – Provide and Operate

- Specific recommendations to map out network architecture and determine network health

Line of Effort 4 – Protect and Defend

- Specific recommendations to improve system confidentiality, integrity, availability and nonrepudiation

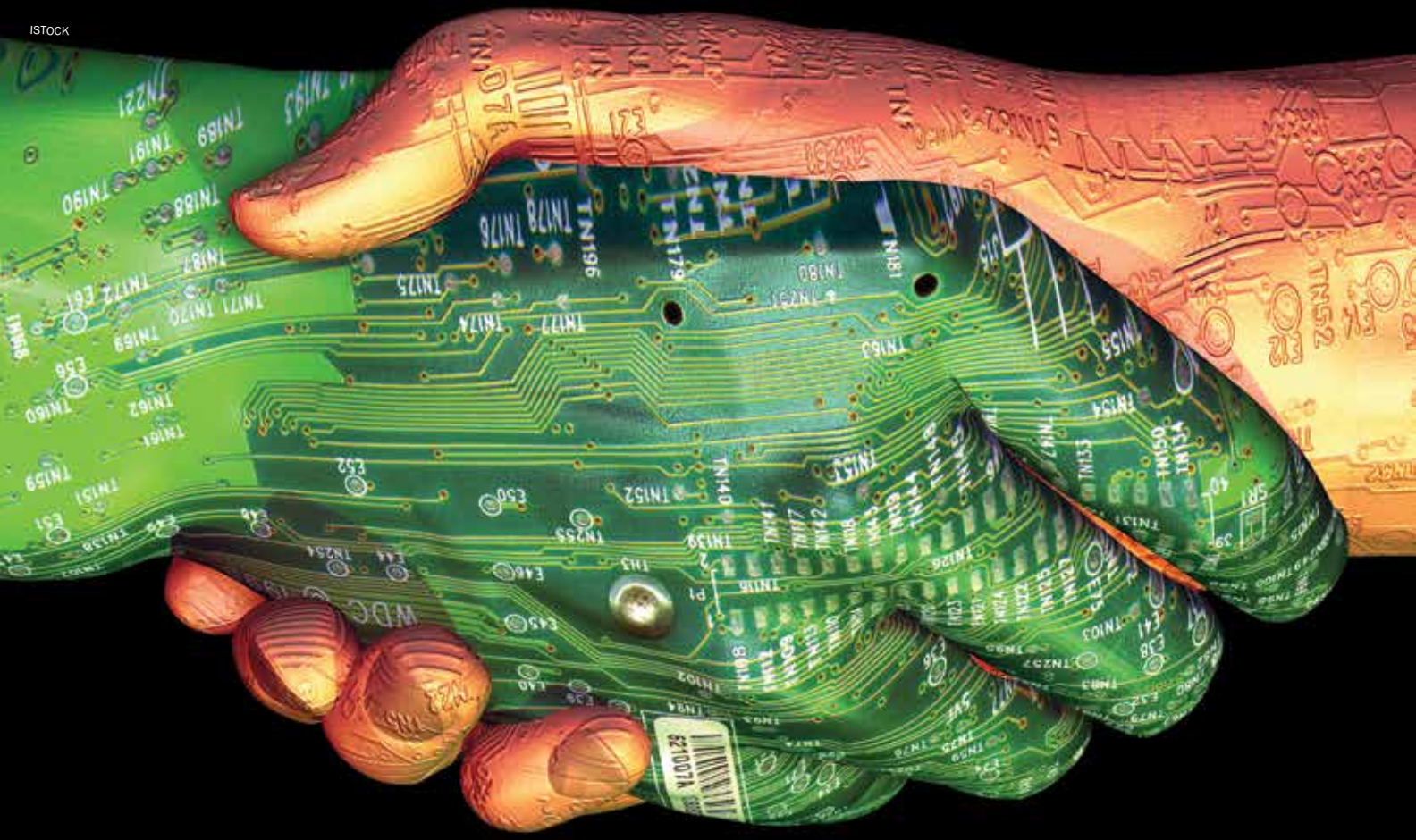
Building upon the recent Central Region Communications Conference held in Washington, D.C., May 12-14, 2015, and attended by 38 regional IT professionals from nine partner nations, USCENTCOM plans to invite government and industry leaders in the cyber field to quarterly collaborative cyber security workshops to develop plans of action and collective milestones to ensure continued progress. These quarterly workshops will be conducted virtually using the Web-based All Partners Access Network, or APAN. We anticipate the first of these collaborative workshops to take place in August 2015. Although we've collectively made great strides in strengthening our cyber security posture, the threats continue to evolve, and only through cooperative vigilance can we protect our mutual interests in cyberspace. Together, we can find a way!

The articles contained in this issue of *Unipath* — and additional material available on *Unipath's* website — provide a strong overview of what the region is doing to defend against terrorists, criminal organizations, hostile governments and hackers who operate online. *Unipath* is a forum to share ideas and articles on a wide range of military and security topics.

As always, your comments and suggestions are helpful to shape the way ahead in critically important fields such as cyber security. Please email comments or ideas to unipath@centcom.mil.

Brig. Gen. Peter Gallagher
Director of Command and Control, Communications and Computer Systems, U.S. Central Command

ISTOCK



Building a Regional Cyber

PARTNERSHIP

USCENTCOM expands the Central Region Communications Conference

UNIPATH STAFF

The fifth Central Region Communications Conference (CRCC) concluded with a multinational commitment that will expand the depth and scope of what has been U.S. Central Command's premier cyber security event.

With the concurrence of CRCC attendees from nine partner nations, U.S. Brig. Gen. Peter Gallagher, head of USCENTCOM J-6 and director of the Joint Cyber Center, promised to hold quarterly workshops in which conference participants and interested newcomers could develop joint strategies to deal with threats in cyberspace.

"We've got to take action. This just can't be the great get-along and a bunch of briefings. And then we wait till next year to come back together to rehit some of the same lessons," the general said on the final day of the conference that ran May 12-14, 2015, in Washington, D.C.

"It's hard to build and very easy to destroy. So part of our challenge is to find ways to work together to create resilience and strength."

VICE ADM. MARK FOX
Deputy commander of USCENTCOM

"We want to use the umbrella of the CRCC to conduct quarterly workshops in cyberspace. We can do these in a collaborative fashion, using what we call APAN, the All Partner Access Network. We would establish a website with access, and within the next three months, we would like to bring this collective team together. And we could also open it up to partners who weren't able to make it."

The announcement capped a busy three-day conference attended by senior cyber security leaders from Afghanistan, Bahrain, Egypt, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia and the United Arab Emirates. Delegates from Afghanistan, Egypt and Qatar gave formal presentations of the progress their domestic cyber security agencies have made defending computer networks. They were joined at the podium by senior U.S. government officials and industry experts from companies such as Google and AT&T.

A common refrain was the need for cyber partnerships, not just between nations, but between governments and the private businesses that are making most of the technological breakthroughs. Such partnerships are needed to share vital knowledge about how to repel criminals, hostile governments and terrorists lurking online.

Staff Brig. Gen. Dr. Mubarak Al Jaberi, Head of Communications and IT Department at the UAE Armed Forces, suggested building a joint "road map for the whole region" that could be "presented by our friends in Washington, D.C." Five years ago, the UAE set up the National Electronic Security Authority (NESA) to help defend cyberspace. It was the first agency of its kind in the region.

Central Region Communications Conference participants gather in May 2015 in Washington, D.C. USCENTCOM

"We need to start thinking of creating and building a task force. We need to go for rapid deployment," Gen. Al-Jaberi said. "We need to be connected. We shouldn't be disconnected. We don't need terrorists or any party to take advantage of the disconnectedness."

"It is our job as stewards and as public servants to find a way to protect our citizens and ensure our national interests are protected. That's why we're here."

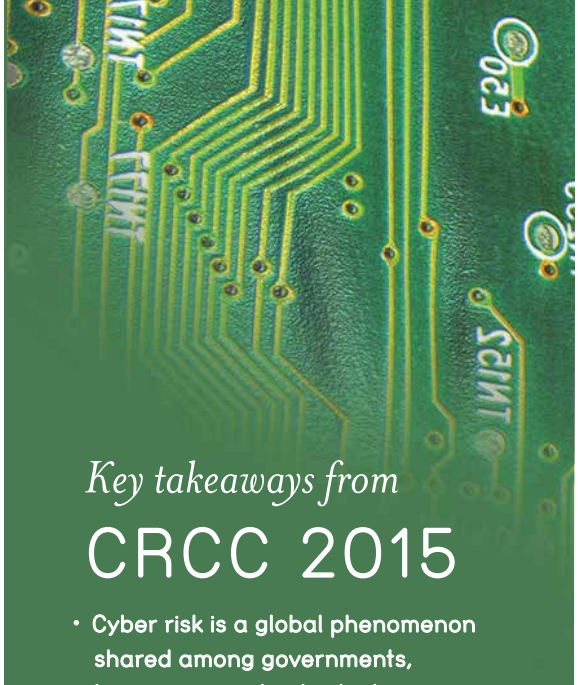
VICE ADM. MARK FOX, deputy commander of USCENTCOM

The need for cooperation was affirmed by Saudi military officers in attendance, who made a plea for a cyber alliance with countries that had learned from hard experience how best to protect computer networks from threats online. "We don't want to start the way they started years ago," said Brig. Gen. Dr. Abdullah Al-Mogbil, chairman of the E-Transactions Subcommittee in the Royal Saudi Land Forces. "We would like to start from where they stopped."

Cyber resilience — hardening network defenses against hostile penetration — occupied much of the discussion at the CRCC. Dr. Edward Amoroso, chief security officer at AT&T, told attendees that surrounding a company's or a nation's systems with general-purpose firewalls and other security software — what he termed "sandbags" — represents a less-than-ideal approach. Each of these defenses can be easily breached with proper motivation on the part of a nation's enemies. The best solution is to create a virtual cyber architecture that isolates various branches of information technology, such as email and websites, into separate, more easily defensible strongholds, he said. That way, a firewall failure won't compromise every system at once.

"It's hard to build and very easy to destroy," Vice Adm. Mark Fox, deputy commander of USCENTCOM, told conference attendees. "So part of our challenge is to find ways to work together to create resilience and strength."

Lebanese retired Brig. Gen. Joseph



Key takeaways from

CRCC 2015

- Cyber risk is a global phenomenon shared among governments, businesses and individuals.
- The world needs a common understanding and measurable metrics of what success looks like in cyberspace. If you can measure it, you can manage it.
- The cyber world requires redesigned architecture to plug vulnerabilities in cyber security defenses.
- Nations and industries must train and educate a certified pool of cyber experts to protect information systems.
- Balance security of networks with individual's privacy concerns.

Nassar, whose national delegation was attending the CRCC for the first time, picked up that theme in a plea for more cooperation.

"We cannot protect ourselves from all intruders. But we can minimize and mitigate the security risk by defining where it's coming from, whether it's terrorist organizations or from hackers," he said. "Then we can decide on the prevention and measures to be taken."

The message of public-private cooperation corresponded to Kuwait's approach. The country recently set up its first national cyber security agency and began by reaching out to technological leaders in the cyber field. "We don't have much experience in cyber security," Kuwaiti Col. Mohammed Al-Enizi announced. "That's why now we are working with the big companies and partners such as Cisco, Microsoft and HP to just establish a secure environment."

In December 2014, Egypt established a High Council for Cyber Security. Its 24 members come from various sectors of government and industry. The formation of such a body is helping the country unite around an issue that hasn't always been at the top of the agenda, said Dr. Sherif Hashem, vice president for cyber security at the National Telecom Regulatory Authority.

"People agree that security is important. But when it comes to deploying resources, developing the skills and supporting infrastructure development, that's when budgetary concerns limit participation," Dr. Hashem said.

Starting with much less than many of its partners in the region, Afghanistan has made huge strides in adopting information technology over the past 13 years, particularly in the spread of mobile phone use to a majority of the population. Zmarialai Wafa, one of the country's top cyber security officials, outlined the process by which Afghanistan has tried to defeat attacks on its fledgling networks, culminating in 2014 with passage of the National Cybersecurity Strategy of Afghanistan.

Afghanistan's efforts earned praise from Khalid Al-Hashimi, Qatar's assistant undersecretary for cyber security. Qatar's Computer Emergency Response Team has led most of the region in conducting national cyber defense drills. "I was very impressed about the activities and initiatives in the Islamic Republic of Afghanistan. Very impressive," Al-Hashimi said. "You were able to pass laws that took other nations years to do. I applaud you for that."

The work of CRCC 2015 will continue through quarterly workshops to which delegates from countries such as Jordan, Iraq and Yemen will also be invited. The moderated workshop sessions will likely occur in an interactive online format. The exact date and location of Central Region Communications Conference 2016 had yet to be determined.

Vice Adm. Fox called on his military and civilian colleagues to apply themselves to what has become one of the biggest security challenges of the 21st century.

"If we don't find a way to do this efficiently, both as nations and as partners, there are people who will do our citizens harm. They will steal, they will destroy," the admiral said at the conference's conclusion. "It is our job as stewards and as public servants to find a way to protect our citizens and ensure our national interests are protected. That's why we're here." ✦

COMBATING **CYBER** CRIME

in the kingdom of

BAHRAIN

AMER S. MUSTAFA/BAHRAIN CYBER CRIME DIRECTORATE

WE ARE COMMITTED TO CONTINUING INTERNATIONAL COLLABORATION AND OFFERING PRACTICAL EXPERIENCE THAT SUPPORTS INTERNATIONAL PARTNERSHIPS IN COMBATING CRIME

ISTOCK

Amer S. Mustafa

The misuse of technology may be risky and damaging to institutions and individuals alike. And due to the transfer of all information into electronic information, cyber crime has become the most important crime to emerge in modern times and the most dangerous type of organized crime to pose a major threat to the global economy. While highlighting the danger of this threat and due to the significant increase in cyber crime, the Kingdom of Bahrain, under the leadership of His Majesty King Hamad Bin Isa Al Khalifa and based on a sharp security vision of His Excellency Lt. Gen. Sheikh Rashid Bin Abdullah Al Khalifa, Minister of Interior, decided to establish a Cyber Crime Directorate in accordance with Royal Decree No. 109 of 2011, thus becoming one of the first countries to combat this kind of crime.

The directorate assumed its tasks, seeking to develop its staff to become capable of and well-informed in the most recent methods of combating cyber crime. In this context, the directorate held conferences and seminars for all sectors to spread awareness among the public — to individuals as well as companies — to deal with this kind of crime. This approach allows the Ministry of Interior to strengthen community partnerships and increase the mechanisms of communication with all sectors of the society. Believing in the importance of international cooperation to confront the dangers arising from these crimes, the directorate also endeavored to join the international conventions relevant to combating cyber crime and to coordinate with concerned international institutions to tackle cyber crime.

In the context of its belief in the need to establish overall security and address all attempts to disturb it, and in a qualitative shift in the area of combating crimes of information technology, His Majesty King Hamad Bin Isa Al Khalifa issued Decree No. 60 of year 2014, with regard to information technology crimes law. The decree included many legal articles that punish perpetrators of cyber crime and control the work assigned to legal authorities. Penalties for sexual exploitation of children have also been tightened, and it has been one of the most important points emphasized by Bahraini law for a long time.

Also, it has become necessary to employ a national strategy for cyber security, because of the increase of electronic threats in the world, which have been reported by the Cyber Crime Directorate in previous years. Such a strategy has become one of the main concerns for Bahrain because all modern communications depend on information technology and the Internet. The aim of the strategy is to achieve the ultimate goal of providing a safe environment in cyberspace and to maintain the gains of the country and its information technology infrastructure. In addition to drawing a road map for developing the

"THE KINGDOM OF BAHRAIN RECOGNIZED THE NATURE OF CYBER CRIME AS BEING A PART OF TRANSNATIONAL CRIME, WHICH MAKES INVESTIGATION DAUNTING. THUS, IT ENCOURAGED MORE INTERNATIONAL COOPERATION THROUGH SHARING OF DIGITAL DATA AND EVIDENCE AND THROUGH JUDICIAL COOPERATION ON CYBER CRIME-RELATED ISSUES."

official entities concerned with cyber security in the field of legislation and law enforcement, Bahrain is working proactively by promoting awareness in the community through a well-studied continuous chain of workshops and seminars.

The Kingdom of Bahrain recognized the nature of cyber crime as being a part of transnational crime, which makes investigations daunting. Thus, it encouraged more international cooperation through sharing of digital data and evidence, and through judicial cooperation on cyber crime- related issues. Bahrain has always been among the first nations to cooperate with countries that needed support or help in investigating cyber crime. Bahrain has helped many countries and took into consideration the legal justifications through which it lent a hand in the investigation of several issues that included terrorism, sexual exploitation of children and financial crimes.

An example of such cooperation on the international level occurred in 2013 when the General Directorate of Anti-Corruption and Economic and Electronic Security received information from the Serious Organized Crime Agency (SOCA) in the United Kingdom stating that an anonymous person in Bahrain was exploiting children sexually through Internet chat programs and had threatened to publish their pictures, violating public morality, and share them with their relatives and friends if the children rejected his demands. Accordingly, an investigation of the General Directorate of Anti-Corruption and Economic and Electronic Security uncovered the identities of the accused persons who engaged in blackmailing children through the Internet to satisfy their sexual desires

After obtaining permission from the Public Prosecution, a team of specialists and digital examiners was formed, the accused were arrested and their homes were searched in execution of search warrants issued by the Public Prosecution. Computers and mobile phones used in the commissioning of the crime were found in their possession. The suspects admitted to the crimes, and after obtaining forensic warrants from Public Prosecution, digital examiners analyzed the electronic belongings and a number of sexual images and video clips of children from Bahrain and outside Bahrain were seized. Children under 14 had been targeted and lured into using websites that showed pictures of girls who expressed interest in meeting them. Then the perpetrators would take indecent pictures of the victims. They also forced the victims to perform those acts by threatening to publish the pictures and expose them to their families. The court sentenced the first and second defendants to 10 years in prison, and the third and fourth defendants to three years in prison. International cooperation led to the administration of justice and punishment of cyber crime perpetrators, using special technical methods to track them.

The journey toward developing and enhancing performance rates progresses in line with the development and modernization strategy adopted by the Minister of the Interior. And in light of the rapid development of electronic devices and software, high- speed computers and smartphones, the General Directorate of Anti-Corruption and Economic and Electronic Security took a step forward and is working toward establishing a new digital laboratory to examine digital evidence similar to its counterparts in developed countries. The directorate visited countries that are advanced in this field to benefit from their experience and learn about the latest devices, equipment and programs used to examine digital evidence.

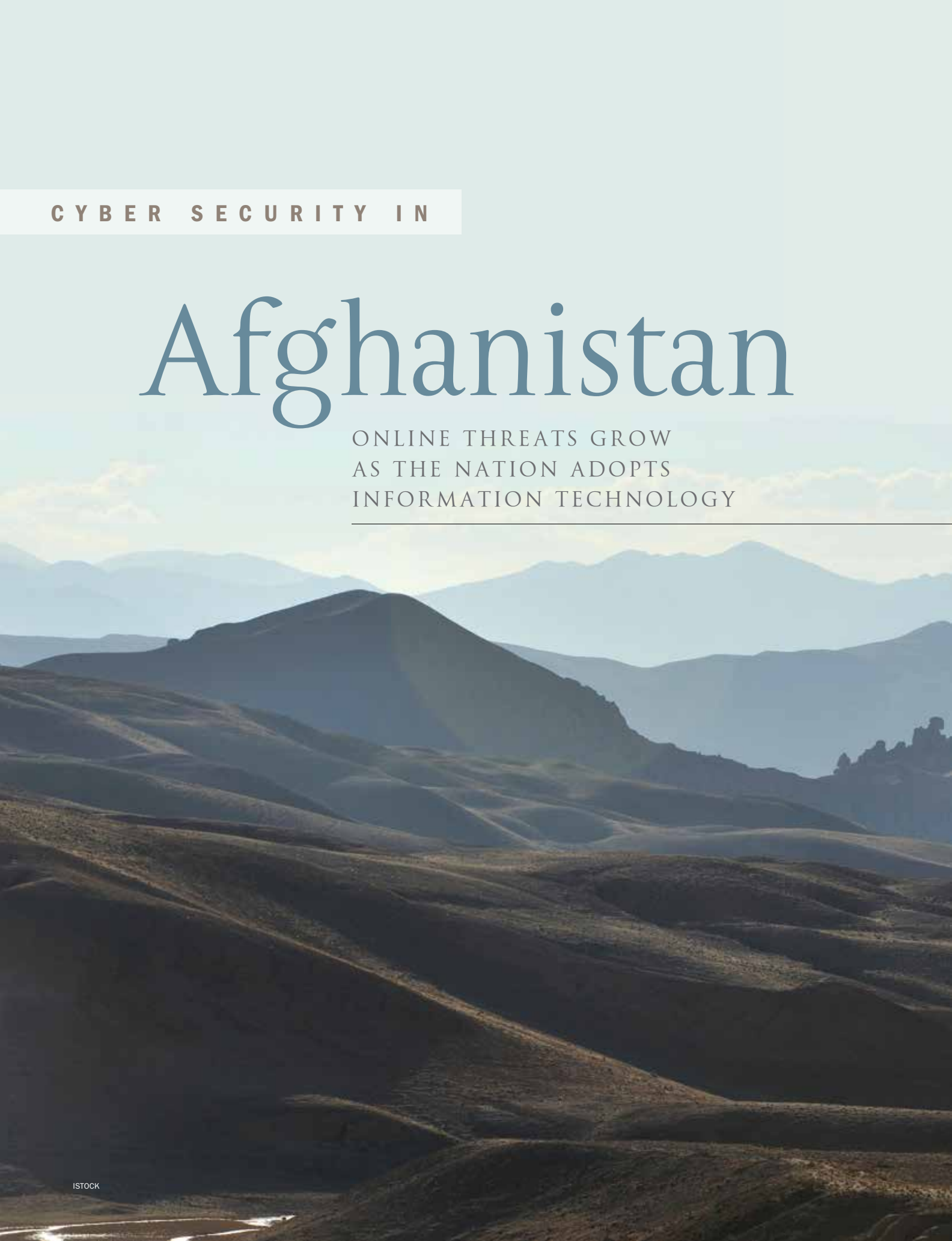
It is worth mentioning that the primary role of this laboratory is to combat and prevent crime by following strategic planning that includes committing to legal requirements within defined criteria and by relying on highly qualified staff trained regularly at the highest levels, and by educating them with policies to be followed daily in the laboratory. It will also have sophisticated equipment and software to examine electronic devices and retrieve information erased from computers, smartphones, magnetic discs and all electronic devices that exist in global markets, ensuring that electronic evidence is presented to the courts in accordance with an approved legal framework. The laboratory will also include a unit to retrieve evidence from damaged devices, and accurate training for this process is taking place within this phase.

Cyber crimes that pose a threat to the world need international cooperation, collaboration and coordination at the highest level to be confronted efficiently and effectively for global security. Therefore, the Anti-Electronic Crimes in the Ministry of Interior of the Kingdom of Bahrain renews its commitment to continue with local and international cooperation for the effective role it represents in combating crime, which is considered to be the ultimate objective of police work. ✦

CYBER SECURITY IN

Afghanistan

ONLINE THREATS GROW AS THE NATION ADOPTS INFORMATION TECHNOLOGY



ISTOCK

By ZMARIALAI WAFA, director of Information Systems Security and head of PKI Management Authority, Ministry of Communications and IT, Islamic Republic of Afghanistan

In today's virtual world, where online communication is a necessity, government and business face the likelihood of cyber attacks. In order to fight cyber crimes and mitigate the risk from those threats, we must cooperate globally to develop an effective model.

Afghanistan has achieved much in cyber security since 2002. Before 2001, the country had fewer than 15,000 local landlines. The Internet effectively didn't exist for Afghans — the country possessed no information and communications technology (ICT) institutions and no Internet service providers (ISPs). To make and receive international phone calls, Afghans usually had to travel to neighboring countries. Pakistan's country code served sections of Afghanistan.

That's not to say computer technology didn't exist in Afghanistan.

Such technology was introduced in 1973 with the purchase of a big IBM mainframe computer. The job of this first-ever computer system was to keep records on foreign trade, help issue bills for utilities and act as a national data bank. After more than 40 years, this obsolete equipment now resides in a museum.

MODERNIZING COMMUNICATIONS

Afghanistan's Ministry of Communications and Information Technology (MCIT) is playing a leading role in ICT promotion in the country. We developed an ICT policy in 2003 and followed that up with new telecom policies and laws in 2003 and 2005. Passing a comprehensive ICT law in 2009 proved more difficult. The draft submitted to the Ministry of Justice was too complicated and technical. We had no choice but to boil down the policy into separate documents, some of which have yet to get final approval: a Cyber Crime Law, an e-Transaction and e-Signature Law, and a Cyber Security Policy.

Afghanistan developed its first telephone landline in 2005, under the corporate guidance of Afghan Telecom. We now have 58 Internet service providers, where just 13 years ago we had none. Most of these ISPs act as resale points. They don't provide all services themselves; they provide no content. They just provide the ability for Afghan customers to link to the Internet. A major number of the connections are coming through the fiber optic ring of communications around Afghanistan. About 70 percent of the ISPs get their Internet from Afghan Telecom.

Fifty-eight ISPs create major concerns for security. With such a large number, how are you going to enforce laws and control traffic over the Internet? That is one of the main challenges we have in the country. We are working on a new design of Internet infrastructure. Hopefully in upcoming years, we'll be in a position to implement that design.

A total of $2.4 billion has been invested in the ICT sector since 2002. Close to 89 percent of the population has mobile phone access. That means more than 23 million Afghans out of a population of 32 million have access. The price of a SIM card (a portable memory chip used in mobile phones) was $300 years ago, but you can buy them today in Afghanistan almost for free.

I remember when I was getting my first SIM card, I had to wait three months, even though I had proper documentation. Demand was too high compared to supply. But the price for each card is dropping day by day. International calls used to cost about $2 per minute. Now they cost just 10 cents per minute.

PROTECTION MECHANISMS OF AFGHAN CYBER POLICY

- Intergovernmental support
- Proper budgeting
- Effective organizational structure
- Public private partnership
- Standards and baselines for information security
- Regulatory body, strategy, policy and best practices
- Incident response and disaster recovery
- Regular review and update of policies
- International cooperation

Afghan election workers count votes at computers in 2014. As part of an information technology upgrade, the country is instituting e-voting through national ID cards with the goal of improving the integrity of the electoral system. AFP/GETTY IMAGES

ELECTRONIC NATIONAL ID CARD (E-NID), OR E-TAZKIRA PROJECT

An important advancement has been our electronic national ID card project. The project was initially signed into being in 2010. That process was delayed temporarily because of the complexity of technological and political issues we faced in the government, but the project is rolling again.

In early May 2015, we performed an end-to-end test that produced no errors in the cards. Everything worked perfectly. We have already received a presidential decree to use biometrics and issue the national ID card. The issuing authority for the cards is the Ministry of the Interior. We at MCIT are the technical partners.

The card is a smart card technology. Most of us know how smart card technology works. It's one of the most secure mediums for authenticity. It has fairly strong encryption. The e-NID or e-Tazkira project uses state-of-the-art technology. Every card has a Public Key Infrastructure-enabled chip inside. It means that every citizen can have three keys in his or her ID card: one for signing, another for authentication and the third for encryption.

Smart card technology offers many national benefits as well. Every time a citizen encrypts a message, it generates a unique algorithm. If a single ID card is compromised, only that card is compromised, not the entire system. Every card is uniquely coded.

The e-NID card is the foundation for e-government services. We can use it for single sign-on, for e-health, e-taxation, e-wallet, you name it. In the beginning, we were thinking of installing up to 17 services on one card but feared that by doing so were creating a single point of failure.

For example, we wanted to put driving licenses on the same ID cards, but decided to issue them separately.

The ID is also being used for e-voting. The integrity of the electoral system is a major concern locally and internationally. We saw that in the previous elections in Afghanistan, when observers worked for months to ensure voting was sound. Despite this transparency, it's hard to keep everything clean and clear. Using the e-NID platform for e-voting would be the most secure way to hold elections.

MCIT PROGRAMS

MCIT also sponsors many promotional programs. The aim is to promote young

International cooperation is critical. Cyber doesn't have boundaries. It's a global issue. We need to work together. That's the only way to mitigate threats in cyberspace. One body cannot fight these threats alone."

talented students in Afghanistan. One program allows students and young people to work on special applications for governmental services. So far they have developed more than 30 apps for the government, including one that allows citizens to pay for utilities using their mobile phones.

Then we have the program that disburses innovation grants to students from various universities. They come up with special ideas in the ICT field. Last year we handed out three ICT champion awards and one student award. We also host business incubators through a program that provides students with office space, Internet service and computer equipment. They can develop their businesses and do marketing from the incubator.

Then we have Tech-Woman Afghanistan, which provides training in various programs and applications from companies such as Google and Microsoft. We've recently begun publishing a bimonthly newspaper called the *Tech Times Afghanistan*. It discusses ICT-related activities in the country.

INCREASED VIGILANCE

In 2009, MCIT established the first Computer Emergency Response Team in the country with help from an International Telecommunication Union (ITU) feasibility study. We named it AFCERT. It now resides under an information systems security directorate. It has developed a forensic lab to help government and business track cyber security problems. By the end of 2015, AFCERT will be connected to the ITU's Global Response Center. We'd like to connect to other centers as well to receive threat and incident information from them.

From 2011 to 2015 the total loss associated with cyber crimes was 1.3 billion AFN (afghani), the equivalent of $28 million. Most of these — 70 percent — were committed by internal staff at financial institutions. Another 30 percent was caused by ID theft, email forging and "spoofing." The year 2014 was our highest recorded for cyber crimes, with losses totaling 827 million AFN. Three out of four computers in Afghanistan are infected with malware, meaning roughly 75 percent of Internet traffic is infected.

During investigations of cyber crime victims, we learned some of those organizations had no security policies in place, which was shocking to everyone. Just imagine: A bank doing transactions of millions of dollars every day had no major security policies in place.

Based on all those crimes, the government decided to come up with the National Cybersecurity Strategy of Afghanistan in 2014. If you go to any country, such a strategy is usually the same: to establish safe and secure cyberspace for government and business. Our strategy is also based on all these goals.

The strategy is based on the ITU's cyber security guidelines consisting of five pillars. The first is legal measures. In Afghanistan, no such thing existed for cyber. What would our penalties be for noncompliance? Second is technical and procedural measures, which are tied to the legal measures. Third is organizational structure, something that we lack. We don't have a chief security officer in our government. This is something we'd like to have. Fourth is capacity building, and fifth is international cooperation.

International cooperation is critical. Cyber doesn't have boundaries. It's a global issue. We need to work together. That's the only way to mitigate threats in cyberspace. One body cannot fight these threats alone. ✦

IRAQ BATTLES DA'ISH ONLINE

HAIDER S. ALKENANI/IRAQI COUNTER TERRORISM OFFICE DIRECTOR OF PUBLIC RELATIONS

ISTOCK

No doubt the terrorists are trying very hard to appear victorious on the Internet in order to gain support and deceive people. During the past decade, the world witnessed Da'ish and its supporters collaborating on social media sites. In 2005, they were using the so-called Suhab Media Corp. owned by al-Qaida. Today, Da'ish owns two larger and more sophisticated media corporations, Al-Furqan Media and Aleitsam.

In the past they enjoyed the freedom to surf among extremist websites to spread their terror ideology and recruit uninformed youth. In some instances, they would exchange bomb-making formulas and lab results, and select targets.

As technology has grown more sophisticated, their tactics have changed. Today, Twitter is the application of choice to spread propaganda. They invented a sophisticated tactic for their announcements to reach the maximum numbers of readers. According to some reports, Da'ish owns 45,000 accounts on Twitter, and once a message is sent, another group will copy the announcement to its followers. Eventually these announcements reach legitimate websites like Facebook and illegitimate extremist websites. Furthermore, the use of bots to mimic visits to their websites allows extremists to claim more adherents than actually exist.

When posting a YouTube clip, they have multiple users upload the same video from different locations and under different names to make the clean-up operation harder. Da'ish's propaganda machine is completely dependent on social media, making the Internet a living artery for the terrorist group. As security officials, we must defeat them on social media and expose their lies to our citizens.

We have tracked terrorist activities online since 2005, when al-Qaida broadcast videos of executions on multiple extremist websites. Initially we acted to block violent extremist websites; however, with new technology and the increased presence of social media, we changed our tactic from blocking sites to countering propaganda. We have specialized teams to confront terrorists on social media to counter their lies. Once Da'ish promoters claim responsibility for a crime or bomb and brag about it, our team responds that the terrorists have committed crimes against innocents and

that their quotes from the Quran used to justify their actions are distortions and an insult to Islam.

Because our team contains experts in religion, Islamic history and psychology, we are able to expose all of Da'ish's lies, leading readers to condemn the crime and align with our bloggers. On many websites, Da'ish promoters claim to control Diyala and Anbar, but our team counters the lies by providing current videos and images of Iraqi troops in the regions. As a result, Da'ish supporters start avoiding some of the sites and think twice before posting lies.

We started noticing the disappearance of Da'ish promoters from their favorite forums because they were unable to convince readers with inconsistent stories that cost them popularity. The majority of Da'ish puppets are delusional, hiding behind computers repeating what their masters have taught them, especially when they reside in different countries and are uninformed about geographic locations and names of towns. On the other hand, our team is well-informed and furnishes firsthand battlefield information, making Da'ish promoters look like fools in the social media.

We are fighting a unique asymmetric war with no defined front line, and we must unite regional and international efforts to counter terrorist organizations online. This battlefront is considered vital for our enemy, since it's where they receive funds, recruit and spread lies. We must deny them the opportunity to spread their ideology, deceive uneducated youth and seed hatred among mankind.

Despite our team's massive effort in this battlespace, we continue to face challenges: Extremist websites have multiplied dramatically, come in many languages and operate throughout the world. They also use a variety of applications with different protocols such as computers, smartphones and even PlayStations.

We must stay current with cutting-edge technology and train hard so that we remain steps ahead of our enemies. These criminals are invading our homes via the Internet and using religion to claim they are defending Muslims, but in reality they are leading young people to destruction and distorting the image of Islam. All of our friends and partners must be united in this fight. ✦

IRAQ'S SOF INTERNET TEAM COUNTERS ENEMY PROPAGANDA

UNIPATH STAFF

The Iraqi Special Operation Force's (ISOF) Internet team plays a critical role in winning the trust of Iraqi citizens as well as boosting the morale of military personnel and promoting the military's professionalism and skill around the region and world. It publishes information about the readiness of the Iraqi military in general and ISOF specifically. Although information published by the team strengthens the confidence of Soldiers and gives citizens a sense of security, it also counters terrorist operations that aim to spread violence and civil disorder.

One of the important topics the team addresses is technology and weapons purchased by the Iraqi government. For instance, the team announced the arrival of Abrams tanks, giving brief information about the tactical ability of the tank and its superb resistance to anti-tank weapons. Another report detailed the purchase of an Apache attack helicopter, the aircraft's effectiveness at aerial reconnaissance and its ability to destroy mobile and stationary targets. The ISOF Internet team also promoted Iraq's acquisition of 12 unmanned aerial vehicles (UAV) and the country's negotiations to obtain the famous gunship UAV Predator.

The Iraqi Internet team is highly educated in the military spectrum — members' comments and responses showcase professionalism and expertise. For example, the team published technical comparisons based on scientific research comparing the American Apache helicopter, Abrams tank and F-16 fighter jet to the Russian Mi-28 helicopter, T-90 tank and MiG-35 fighter jet.

AFP/GETTY IMAGES

An Abrams tank rolls across the sand at a military exercise.

Many are unaware of the Iraqi military's sophisticated technology. The efforts of the Internet team shed light on this valuable information, which has generated many positive comments and more than 10 pages of responses, making it a true military-to-military forum. Forum participants include Iraqis, as well as citizens of neighboring countries who express support for and trust in the Iraqi military.

Teams like this are a first-line defense against terrorist groups that aim to undermine the military and spread propaganda and misinformation about fake terrorist victories on the ground to create panic and terrorize citizens.

CYBER DRILL BOOSTS INNOVATION *in Qatar*

ISTOCK

TESTING THE RESILIENCE OF THE GOVERNMENT, ENERGY AND FINANCIAL SECTORS

Khalid Al-Hashimi,
assistant undersecretary
for cyber security, Qatar

For the past seven years in Qatar, we've been preaching policies, procedures, technologies and incident responses. We're trying to simplify things: simplifying frameworks, simplifying technology, focusing on the human element.

Even though we're a regulatory body, we have not been too strict in enforcing all these instruments. The reason was a fear that if we push hard, there would be resistance. And when there is resistance from constituents, nothing moves. So we started with an approach that uses policies and legal instruments to help constituents in sectors such as energy, transportation, water and banking build capacity when it comes to compliance.

In 2012, things were moving more slowly than we liked, so we decided to come up with something new, something to encourage constituents to adopt, accept and progress rapidly. What we came up with was a game, a national game that took the form of a recurring cyber drill.

To test the effectiveness of safeguards applied to computer networks, we organized National Cyber Security Drill Star 1 in 2013. The objective was to assess incidents, support business continuity, control escalation and improve decision-making. We wanted to see whether our constituents were capable of addressing these issues in a timely manner.

To prepare, we did a comprehensive study of other games played by international partners such as Cyber Storm in the United States, the European Network and Information Security Agency (ENISA) in the European Union, and the Japan National Information Security Center. We studied these drills for over a year: the objectives, the content, the conclusions and the impact. We simplified all these exercises to fit Qatar. Then we drafted and presented a paper to gain international recognition of our efforts and had our paper accepted by ENISA at a conference in 2013.

QATAR NATIONAL

CYBER DRILLS 2014

320
PARTICIPANTS

120
DAYS
PREPARATION

32
ORGANIZATIONS

2667
EMAILS EXCHANGED

9
INDUSTRY SPECIFIC ATTACK SCENARIOS

We came back home and promoted our national cyber drill, stressing how we had gained that international certification.

At this point, Qatar's Cyber Security - Q-CERT Division at the ministry of ICT had two options. Q-CERT could write letters to chief executives and force them to participate. After all, the Cyber Security Divison is the national regulator in the field of cyber. The other option was to use encouragement instead of enforcement, highlighting the benefits to the CEOs. We chose the voluntary approach, and I am happy to report that 20 organizations with 120 people agreed to participate.

When these officials from government, the energy industry and finance sat down for tabletop and technical exercises, we had to overcome initial fears that the drill would expose participants to ridicule from competitors in government and industry. It took many hours, full of questions and arguments, before we persuaded participants that the Star 1 drill would ultimately benefit them.

We scheduled this first national cyber drill for December 15, 2013, right before Qatar's National Day. During our National Day you will see the Army, Navy and Air Force hold parades. We chose this date because we needed to display to the nation the existence of other forces, perhaps less visible, that were also hard at work protecting the nation's assets.

We achieved our objectives.

WE SIMPLIFIED THINGS TO OUR PARTNERS, ENCOURAGED THEM TO COMPLY WITHIN A FRAMEWORK, MOTIVATED THEM TO COME UP WITH SOLUTIONS. THEY WERE ASKED TO INNOVATE, AND THAT'S WHAT THEY DID.

We had a red team consisting of engineers devise attacks against machines we had given the organizations to protect. To relieve anxiety about capabilities, we created three levels of the drill in ascending order of difficulty: bronze, silver and gold. Some participants worried that if they sat in the same room with large banks and energy companies, they might be embarrassed if their equipment and skills were inferior.

The biggest goal of the exercise was to observe whether participants would talk to each other. So if I had Bank X sitting next to Bank Y, and they had similar issues with cyber security, our intention was for them to cooperate to solve problems during Star 1. It was a success in assembling and identifying strength yet discontent in terms of exchanging information, collaboration and sharing mitigating practices cross sectors.

We used these lessons in hosting National Cyber Security Drill Star 2 on the same date in 2014. Star 2 attracted even more attention: 32 agencies and companies comprising more than 320 participants. We changed the exercise a bit. We handed out virtual machines to members of each group to act as their network or server. Their job was to harden that virtual machine to try to protect it from the attacking red team.

The exercise took nearly 15 hours. Again, the objective was to see whether these experts would coordinate during national crises. To encourage that collaboration, we used scenarios that would affect each sector as a group: a telecom outage that would hit every government agency or an industrial control issue that would strike all energy companies at once.

We were sending out messages to these financial institutions, energy businesses and government departments announcing threats and asking them to act systematically and cooperatively.

We achieved our objectives. We simplified things to our partners, encouraged them to comply within a framework and motivated them to come up with solutions. They were asked to innovate, and that's what they did. All of this was achieved with a simple game.

Based on this success, we would like to expand such drills to the region. The majority of countries experience similar challenges: Bahrain, Oman, UAE, Jordan, Egypt, Kuwait and Saudi Arabia. We need to do something similar together in cooperation with the U.S. government, which can help set common standards we can all adhere to. ✦

This article was adapted from a presentation given by the author at the Central Region Communications Conference in Washington, D.C., in May 2015.

PROTECTING CYBERSPACE

THE UAE LEADS IN ONLINE NATIONAL DEFENSE TACTICS

UNIPATH STAFF

Hackers shut down banks by flooding websites with phony traffic, preventing customers from accessing their money. Terabytes of information are stolen from government computer systems, compromising national security. Stock exchanges are disrupted by rogue actors seeking to destabilize financial markets.

These are recent examples of cyber crimes that threaten stability and undermine the rule of law. The fight in this "fifth realm" of warfare — cyberspace — is becoming just as important as battles on land, sea, air and space. Technological advances have changed the nature of war, and military forces and governments are evolving to meet the challenge.

The United Arab Emirates (UAE) has made cyber security a priority, resulting in the country being better equipped than most nations to deal with online threats. This is critical because UAE is one of the most targeted countries in the world by cyber hackers (criminals who break into online security systems to steal or copy information) and phishers (people who attempt to disguise themselves online as representatives of banks or other organizations to obtain personal information), according to UAE security officials.

Threats such as these led to the creation of the Emirates' latest weapon: The National Electronic Security Authority (NESA) is the first of its kind in the region and streamlines the country's online defenses.

"Cyber security is one of the biggest economic and national security challenges countries face in the 21st century. The NESA was established in line with this modern reality and as soon as the authority was in place, we immediately initiated a thorough review of the federal efforts to defend and protect the nation's ICT infrastructure," said His Excellency Jassem Bu Ataba Al Zaabi, director-general of NESA.

NESA was created by His Highness Sheikh Khalifa bin Zayed Al Nahyan, president of the UAE, in a 2012 decree to address online threats to military and critical infrastructure in the region. Oil and gas installations, nuclear energy facilities and power companies are all potential targets. Medical records in hospitals and government files on personnel and citizens are also sought after, as well as intellectual property and national security vulnerabilities. Even installations as innocent as water desalination plants are constant targets of malicious attacks to disrupt or disable services. Cyber sabotage has the ability to cause so much damage that protecting the cyber realm is as critical as traditional border security.

Electric transmission cables tower over the landscape near Abu Dhabi. Protecting critical infrastructure from cyber threats is a priority in the United Arab Emirates. REUTERS

A trader works in the Dubai Financial Market stock exchange. The United Arab Emirates is linking its public and private sectors to improve the country's overall cyber security. AFP/GETTY IMAGES

"Critical infrastructure is a place where most of the attackers try to get into and disturb critical services," NESA official Dr. Saud Al Junaibi said during a 2014 Gulf Cooperation Council conference on electronic warfare. "This is because oil and gas as well as utility sectors provide major and key services to countries like the UAE, and these are usually targeted by different threats to disturb services."

That's why NESA plays such a vital role and can serve as a model for other nations. Its functions are to protect the UAE's communications networks, develop and implement network safeguard monitoring tools, propose and implement national policy to enhance security, and develop national emergency plans and risk assessment reports. The agency is also charged with uniting efforts to protect private and public entities against cyber crime and espionage.

In 2014, NESA published the National Cyber Security Strategy, Critical Information Infrastructure Policy and the UAE Information Assurance Standards. "NESA is committed to ensuring that all UAE government bodies are made fully aware of the responsibility they now have, to meet the requirements of these polices, and in turn, what this means in practice going forward," Zaabi said.

The threat is real. A sophisticated cyber espionage attack uncovered in

> *"THE UAE FIRMLY BELIEVES THAT CYBER SECURITY CAN BE ACHIEVED ONLY THROUGH COOPERATION WITH THE PEACE-LOVING COUNTRIES."*
>
> — MAJ. GEN. MOHAMMED AL ESSA, *UAE Ministry of Defense*

2012 dubbed "Red October" targeted 20 countries, including the UAE, before authorities caught on that a billion megabytes of information had been stolen over five years using computer viruses. Experts believe a cyber gang auctioned much of the data on the black market to the highest bidder. It is assaults like these that remind everyone of the economic and security damage posed by online predators.

"For governments in the Gulf Cooperation Council [GCC], cyber security is just as important as military hardware," said Theodore Karasik, director of research at the Institute for Near East and Gulf Military Analysis.

THE NEED FOR COOPERATION

Maj. Gen. Mohammed Al Essa of the UAE Ministry of Defense said that although his country's military and security agencies have made much progress to enhance cyber defense, success is a multinational effort. "The UAE firmly believes that cyber security can be achieved only through cooperation with the peace-loving countries," Al Essa said at a Gulf International Cyber Security Symposium in Dubai as reported by *The National*.

Employing advanced technology and encouraging interagency cooperation is important, he said, but sharing expertise and experiences with allies is critical. "You can't wait until a conflict erupts," said Kenneth Geers, an international cyber terrorism expert based in the U.S.

During a multinational counterterrorism conference in Germany, Geers urged world governments to prepare in peacetime against terror threats. He likened illegal hackers, terrorists and criminals to pirates who want to spring tactical surprises on their opponents. A well-prepared government with effective cyber security programs can act as a deterrent for the simple reason that criminals usually don't want to get caught, Geers said.

"Terrorists are looking for this asymmetrical pop," Geers said. "They're going to hit you in the face and run and hide."

THREAT AWARENESS

Protecting cyberspace is a multinational responsibility, but some countries and individuals minimize the threat. Countries and companies can be reluctant to disclose the extent of attacks because of the potential to reveal vulnerabilities, lose public confidence and motivate copycat criminals. Experts say even basic cyber security knowledge can help protect against the vast majority of threats. Adhering to password protection policies, opening email only from trusted sources, and updating antivirus and malware software are basic protective measures.

Community awareness campaigns that promote these practices are important, and efforts such as these are already underway in the UAE. The country's Telecommunications Regulatory Authority (TRA) teamed up with the national Computer Emergency Response Team and the Ministry of Education to educate schoolchildren on best practices for online security.

"This educational program includes online activities, lectures and case studies designed to drive home best practice to teachers, empowering them to pass it on to their students," TRA Chairman Mohamad Ahmad Al-Qamzi said. "And, of course, from students, this knowledge passes to families and friends, enabling us to reach every home in the UAE." ✦

Sources: *The National, PC Magazine,* Symantec's Internet Security Threat Report, Emirates Identity Authority, Emirates News Agency-WAM, *Defense News*

STRENGTH IN UNITY

EAGER LION MILITARY EXERCISE BRINGS TOGETHER MILITARIES FROM 18 COUNTRIES

UNIPATH STAFF

Two of Jordan's Fighting Falcon F-16s cut across the sky dropping their bombs on an enemy stronghold, signaling the start of a powerful multinational assault. Soon thereafter, two B-52 Stratofortress bombers thunder past, carpeting the ground with explosions. Cobra and Apache helicopters swoop across the sky delivering a deadly hail of missiles, rockets and heavy-caliber gunfire. All this is followed by an onslaught of firepower from ground forces, sniper teams and guided missiles from High Mobility Artillery Rocket Systems. This huge display of force in Jebel Petra, Jordan, was one of the culminating events of the Eager Lion military exercise.

Hosted annually by Jordan, Eager Lion is one of U.S. Central Command's premier military exercises, designed to facilitate a coordinated, multinational military response to conventional and unconventional threats. Now in its fifth year, Eager Lion brought together 10,000 military personnel and officials from 18 countries from May 5-19, 2015. Participants came from Australia, Bahrain, Belgium, Canada, Egypt, France, Iraq, Jordan, Italy, Kuwait, Lebanon, Pakistan, Poland, Qatar, Saudi Arabia, the United Arab Emirates, the United Kingdom and the United States. NATO's Allied Rapid Reaction Corps also joined the exercise.

"There is an increased interest this year in the Eager Lion exercise because of what it represents as being a meeting ground for all the military commanders at all strategic, operational and tactical levels," said Brig. Gen. Fahad Faleh Ahmad Al Damen, Jordan Armed Forces director of Joint Training Directorate, who led this year's exercise. "The exercise is important because of what the region and the world are experiencing from the rise of extremist groups that are far away from the

Top: Jordan Armed Forces Armored Infantry Fighting Vehicles fire rounds at a range during Eager Lion's huge military counterattack demonstration on May 18, 2015.
JORDAN ARMED FORCES

Center: Military service members from Belgium, France, Jordan, Pakistan and the United States employ various ships and aircraft to conduct a simulated assault on a target in Aqaba during Eager Lion 2015.
PETTY OFFICER 2ND CLASS PAUL COOVER/U.S. NAVY

Bottom: High Mobility Artillery Rocket Systems launch guided missiles during the exercise.
JORDAN ARMED FORCES

humanitarian values and that are committing horrible crimes for the believers from all religions. This mandates having joint cooperation and the exchange of expertise in order to fight all aspects and types of terrorism."

U.S. Maj. Gen. Rick B. Mattson, U.S. Central Command's director of exercises and training, said the exercise was a tremendous success – and not only based on meeting operational goals. "In this region relationships mean everything," Maj. Gen. Mattson said. "This exercise has forged new friendships. These relationships, which are both personal and professional, create an enduring bond between our nations and partners."

His Royal Highness Jordanian Prince Faisal bin Hussein, left and U.S. Gen. Lloyd Austin, commander of U.S. Central Command, watch the Eager Lion military exercises. This year's exercise brought together about 10,000 troops from 18 countries.

AFP/GETTY IMAGES

Each year, countries such as Lebanon have proudly joined Jordan for Eager Lion. This year the Lebanese Army brought a detachment of 60 troops, including five officers. At the command level they took part in managing crisis operations, operational planning, and other command and control functions. At the detachment level Lebanese forces took part in events such as counterterrorism and border security operations, conducted first-aid training, reconnaissance and surveillance, and close quarter combat drills.

"We can confidently say that all the forces from friend and Arab countries participating in the drill have shown great professionalism, whether at the level of groups or at the individual level," Lebanese Staff Brig. Gen. Ghassan Fadel said. "In this context, I have to highlight the key role of the Jordanian Army in the fine organization of this drill as well as its technical and operational direction. This has presented an opportunity for everyone to exchange expertise and gain the skills that characterize the Jordanian Armed Forces."

He explained that Eager Lion represents an opportunity for military commanders to discuss issues at the strategic, operational and mobilization levels and to work together. The Lebanese unit benefited from honing combat techniques requiring coordination among different units during counterterrorism and border security operations, Fadel said.

"These are the primary needs of the armies nowadays, due to the vast expansion of terrorism and the danger it poses upon human societies, notably our Arab communities, which affects their unity, security and economic stability as well as the free and secure coexistence between its constituents," Fadel said. "Confronting this danger necessitates boosting joint cooperation and coordination

between friendly armies and sharing military expertise in all the fields to the point of raising the competence level of the personnel charged with the mission of fighting terrorism, especially in urban and close areas."

EXERCISE GOALS

Eager Lion is designed to develop participants' capabilities in planning and conducting joint operations. It tests and hones relationships among military forces, government agencies, ministries, and outside organizations within an unconventional operational environment. In addition, foreign militaries can exchange expertise and improve operational interoperability.

With exercise events occurring from the northern community of Zarqa to the country's southern tip in Aqaba, Jordan offered a wide range of venues for forces to train in areas such as counterterrorism, border security, search-and-rescue operations, humanitarian operations, crisis management, information and psychological operations, strategic communications, civil-military operations, vital installations protection, and cyber defense.

Before the actual exercise began, many of the officers participated in an academic session held at the Jordan Armed Forces Peace Operations Training Center from April 20 to May 4. Jordanian Brig. Gen. Amjed Al Zoubie is the commander of the POTC and served as director of Eager Lion's Higher Command within the exercise. He said an academic focus on military decision-making processes helped ensure cohesion at Eager Lion — a process that if well understood allows officers to respond more quickly and efficiently to asymmetric events. "We work in a complex environment, and we are dealing with non-state actors, criminals, terrorists, extremists, human traffickers — all bad groups," he said. These malevolent actors produce a wide array of threats forces must be prepared to preempt and overcome.

STAFF SGT. TODD L. POULIOT/U.S. ARMY

Brig. Gen. Fahad Faleh Ahmad Al Damen, Jordan Armed Forces director of Joint Training Directorate, left, and U.S. Maj. Gen. Rick Mattson, U.S. Central Command's director of the Exercises and Training Directorate, open Eager Lion 2015 with a news conference.

DIRECTOR PROFILE: BRIG. GEN. FAHAD FALEH AHMAD AL DAMEN

UNIPATH STAFF

For the past 25 years, Jordanian Brig. Gen. Fahad Faleh Ahmad Al Damen has dedicated his career to the Jordan Armed Forces. As director of Joint Training Directorate, he led this year's Eager Lion military exercise.

Gen. Fahad holds a bachelor's degree in military science, a master's degree in public administration, and another master's degree in administration and strategic studies. He has served as the commander of the Royal Military College and commander of the Royal Armor School, in addition to many previous assignments as a staff instructor.

Command assignments have included platoon leader, company and battalion commands and commander of the Armor Brigade.

Gen. Fahad has received the following medals and military awards: the Order of Military Merit 4th Grade; Leadership Proficiency Insignia, Participation with the International Peacekeeping Forces Medal; UN Service Medal; Long Service and Good Conduct Insignia; Al-Estiklal (Independence) Medal 3rd Grade; and the Training Proficiency Insignia.

One example of an Eager Lion event designed to overcome asymmetric threats was a mass casualty training scenario held in Zarqa that tested coordination among military, police and government ministries.

"This is what you call a comprehensive approach," Gen. Fahad said. "You cannot run the world with military alone. You must work with ministries."

In the scenario, several missiles hit a residential area — one included chemical weapons that killed and injured children playing soccer in a nearby field, among others in the community. Jordanians were joined by forces from the United Arab Emirates and the U.S. as they secured the area, decontaminated victims and set up a field hospital.

"They made it look very easy. It was seamless," Gen. Mattson said, describing an event like this as a worst-case scenario that requires a complex and highly coordinated response across a multitude of agencies.

Brig. Gen. Mohammad Salem Jaradat, Jordan Armed Forces chief of staff of training, said in a scenario like this, "we are racing with the time." Seconds matter, and quick and coordinated responses are essential. "I was very proud of that exercise," Jaradat told *Unipath*. "It was one small part of the overall event, but I was very proud."

One new element to the exercise was the inclusion of two B-52 bombers from the U.S., which joined the Jordanian F-16 Fighting Falcons during the counterattack in Jebel Petra. The B-52s allowed U.S. bomber crews to practice real-time coordination with Jordanian air controllers, giving participants a better understanding of each other's tactics, techniques and procedures so that multinational crews can work together seamlessly in possible future operations.

Lt. Col. Mohammed Al-Atiyat, a fighter controller with the Royal Jordanian Air Force, said such cooperation was inspiring. "Everyone worked together — the army, ground forces, air force and navy. The whole government worked

Members of the Lebanese Armed Forces take part in Eager Lion 2015 along with forces from 17 other countries. LEBANESE ARMED FORCES

Members of the Jordan Armed Forces celebrate after a successful training event during the exercise. JORDAN ARMED FORCES

U.S., Kuwaiti and Jordanian special operators provide medical treatment to simulated wounded personnel during a combat search and rescue in the city of Jerash, Jordan. MAJ. TIFFANY COLLINS/U.S. SPECIAL OPERATIONS COMMAND CENTRAL

JORDAN'S COMMITMENT TO TRAINING

UNIPATH STAFF

Beyond the Eager Lion military exercise, constant training constitutes a large part of the activities of the Jordan Armed Forces (JAF).

Brig. Gen. Mohammad Salem Jaradat, JAF's chief of staff of training, said this is because unconventional and asymmetric warfare threats demand that forces be vigilant and prepared for any situation.

"We are living in a region where we can all see the problems. Our Supreme Commander, His Majesty the King, recognizes that we are on the front lines in fighting Da'ish," Jaradat said.

"We are waging a war against them. This is a major threat. They are killing kids. They are killing women. There are displacing many people. They are destroying the values of human beings. They are just killers. We are trying to save our future from them, to protect the generations and to protect all human beings."

Jordanian Brig. Gen. Mohammad Salem Jaradat
JORDAN ARMED FORCES

Threats like those posed by Da'ish reinforce the need for continued training and partnership. That is why the JAF takes part in about 25 to 30 bilateral and multilateral military exercises each year. "The training should not stop," Jaradat said. "When you stop you are in trouble."

An important component of JAF training policy is to share and exchange students. "This is a circle. We get lots of benefits from exchanging views and training," the general said.

Exercises such as Eager Lion, along with internal JAF training events, prepare Jordan's forces for natural and man-made crises. Chemical attacks, tsunamis, terrorism and cyber attacks — these are just a few of the potential threats.

And Jordanians don't just respond to problems within their own borders. "It is part of our policy to help people around the world," Jaradat said.

More than 70 percent of the JAF have participated in peacekeeping operations, Jaradat noted. Jordanians have served in places like Afghanistan and Haiti. Such missions abroad showcase Jordan's commitment to peace and stability for all.

"Finally, at the end of the day, it's safety, security and stability — working for the benefit of the people and new generations, our daughters and sons to save them from extremists," he said. "This is our job to do."

toward the same goal. It was more efficient than working alone." Future wars, Al-Atiyat said, will not be between two countries; instead they will be coalition efforts. "We want peace with all our neighbors around us, but sometimes peace needs force, especially when other nations don't take (peace) seriously."

STRENGTHENING UNITY

Lt. Col. Ahmad Hamad Al-Rowaini of Bahrain's Special Forces said the exercise provides a great opportunity for militaries to learn from each other and build friendships.

"Strength is unity. We must stay united with our friends and allies to combine our efforts to defeat terrorism and reach security and stability in the region," Al-Rowaini said. "We are nations that live peacefully and wish for sustained security and peace."

Lt. Col. Abdullah Al-Harbi, of Saudi Arabia's Royal Air Defense, said working in a multilateral environment helps everyone gain better experience by learning differences in military tactics and cultures, while preparing against future threats: "The exercise addresses the challenges that face the region and provides the best solutions for many different scenarios. We also build trust with our friends and allies as well and meet new friends."

Pakistani Brig. Gen. Badr Yousaf headed his country's delegation which included 44 participants from the Navy, Army and Special Forces. Brig. Gen. Yousaf praised the collaboration and synchronization of forces throughout the exercise. "Everyone learns from one another," he said. "It's the exchange of knowledge."

Brig. Gen. Jaradat echoed the importance of sharing knowledge and experience. "We are very proud to be a hub of training here," Brig. Gen. Jaradat told *Unipath*. "We are supported by His Majesty, our Supreme Commander the King, in policy and at the strategic level. We are ready always to share and train, and because of the safety, stability and security we can do this. We welcome our brothers and friends in the future to come to train."

Maj. Gen. Mattson expressed gratitude for Jordan's hospitality: "I would like to thank the Kingdom of Jordan for hosting this exercise. You couldn't ask for a better partner." ✦

Defending THE GULF

KUWAIT HOSTS THE LARGEST EAGLE RESOLVE EXERCISE IN 16 YEARS

STORY BY *UNIPATH* STAFF | PHOTOS BY KUWAIT ARMED FORCES

The helicopters came in low, raising clouds of dust as they settled on the desert floor and dispensed multinational response forces. The commandos came in many stripes: Kuwaitis and Jordanians in beige camouflage, Qataris all in black, Bangladeshis in deep green, Americans uniformed to match the surrounding sand.

The terrorists who were holding hostages at the Kuwaiti seawater desalination plant were caught off guard. Before the assault began, they had felt secure enough to kick around a soccer ball in the compound. Minutes later they were rooted out of buildings, handcuffed and whisked into armored personnel carriers.

But a closer look at the scenario — part of the Eagle Resolve 2015 multinational military exercise hosted by Kuwait in March 2015 — revealed it wasn't just a showcase for special forces. Off in the distance, blue-clad Kuwaiti police had formed a perimeter sealing off the compound, assisted by Kuwaiti National Guardsmen who swooped onto the scene aboard trucks equipped with machine guns.

When special forces discovered that the hostage takers had also been brewing noxious chemicals in a clandestine laboratory, medical teams from the United Arab Emirates and Saudi Arabia, and decontamination squads from Jordan, Kuwait and Qatar arrived in ambulances and mobile labs.

Multinational special forces conclude a hostage rescue mission at Eagle Resolve 2015.

A Kuwaiti firefighting boat responds to a crippled tanker leaking oil during a simulation.

Multinational forces advance off Failaka beach near the end of the exercise in Kuwait in March 2015.

FOR Kuwaiti exercise director Brig. Gen. Mohammed Al-Kandari, this demonstration of proficiency unfolding in a desert miles from Kuwait City accomplished a primary goal of Eagle Resolve: to highlight cooperation not just between multinational militaries but also between Soldiers and civilian agencies. Gen. Al-Kandari said that in the past some Kuwaiti military and civilian officials had never spoken to each other professionally, a deficiency that Eagle Resolve corrected.

"The exercise is conducted at a national level involving all agencies and government entities that are related to the military and security field to prepare for real-life scenarios to defend the nation," Gen. Al-Kandari said.

Eagle Resolve brought together thousands of Soldiers from 29 partner nations to address the challenges of asymmetric and unconventional warfare. As always, most of the main participants came from Gulf Cooperation Council (GCC) nations: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates.

The exercise began with a command post exercise to build multinational integration in a simulated headquarters environment. Air defense and border security played large roles in the nearly 100 events created to challenge participants. Egypt, Jordan and Pakistan were among the non-GCC countries involved. The next phase was a field training exercise that tested the mettle of troops on the ground, in the air and on the seas. After most of the exercise participants had dispersed, top commanders concluded Eagle Resolve with a senior leader seminar.

Aside from the hostage-taking event, forces were asked to respond to crises that included a crippled oil tanker in the Arabian Gulf, an airplane crash involving hazardous materials at Abdullah Al-Mubarak Air Base and an attack by missiles carrying chemical warheads. The crowning event was an amphibious landing on Failaka Island, 20 kilometers from Kuwait City, in which multinational forces wrested control of a beachhead from armed terrorists.

A Kuwaiti Air Force helicopter dispenses commandos during an assault on Failaka Island at the end of Eagle Resolve.

"This joint exercise is considered as one of the largest exercises in the Middle East, and it is part of Saudi Arabia's training and programs, which aims to develop and enhance Saudi forces' skills, raise combat readiness and learn techniques from other participating forces," said Saudi Col. Saleh bin Abdullah Al-Harbi. "It will strengthen regional cooperation in the field of joint operations toward achieving the desired goal of countering challenges and crises."

Many of the events called on the specialized skills of paramedics, physicians, police, national guardsmen, firefighters and crisis management agencies — exactly as Eagle Resolve's Kuwaiti planners intended.

For example, at the mock missile attack that produced dozens of sick and dying victims of chemical exposure, military and civilian responders arrived on the scene, quickly establishing a cordon and triaging victims. Personnel erected decontamination tents like desert flowers after a spring rain. Doctors fed intravenous fluids to moaning victims on stretchers. Qatari medics rolled up in two fully equipped mobile surgical buses they had brought to Kuwait aboard ships, earning the admiration of partner nations and setting the bar high for how medical treatment drills should be conducted.

"If we go back to the history of Eagle Resolve, we will see that the exercise began with fewer participants, and it has witnessed huge expansion and participation from all regional and international nations," said Qatari Staff Brig. Gen. Jassem Ahmed Al-Mohanadi, commander of National Defense & Crisis Management Center. "The nations' shared interest to improve was obvious in the Eagle exercise, with the participation of more than 5,000 participants from 29 countries."

Eagle Resolve was born in 1999 as a missile air defense seminar that brought together GCC partners and United States Central Command, but it has grown to become the premier GCC/Arabian Peninsula military exercise. Although the event has rotated among GCC countries, Kuwait hadn't hosted until this year. It vowed to make the March 2015 exercise the biggest ever.

Gen. Al-Kandari viewed Kuwait's mission as more than just showcasing the abilities of his nation's forces. As he repeated throughout the exercise, he viewed each tactical scenario as an opportunity to expose potential vulnerabilities that commanders can later correct. "We want to learn," the general said during the plane crash event at Abdullah Al-Mubarak Air Base.

Delegation QUOTES

"In the framework of cooperation between the Gulf Cooperation Council, U.S. Central Command and the United Arab Emirates Armed Forces, this joint exercise aims to enrich the experience of various participating units and refine and develop requirements of joint military action because of its importance and its active role in raising military efficiency through exchange of experiences and skills among participating countries."

~ Col. Sultan Al-Ketbi, head of the UAE delegation

"By hosting this event, Kuwait confirms its leading status in the world."

~ Brig. Gen. Hamed Al-Ghamdi, head of the Peninsula Shield Forces delegation to Eagle Resolve

"The exercise is conducted at a national level involving all agencies and government entities that are related to the military and security field to prepare for real-life scenarios to defend the nation."

~ Brig. Gen. Mohammed Al-Kandari, Kuwaiti exercise director

"Work over the past months has produced accurate and well-organized planning for the exercise, thanks to the Kuwait Army general staff."

~ Jordanian Brig. Gen. Mohammad Salem Ali Jaradat

"We as Qatari armed forces are interested in Exercise Eagle Resolve because of large-scale participation of various Gulf countries, regional and international countries. If we go back to the history of Eagle Resolve, we will see that the exercise began with fewer participants, and it has witnessed huge expansion and participation from all regional and international nations."

~ Staff Brig. Jassem Ahmed Al-Mohanadi, Commander of Qatar National Defense Center & Crisis Management

"Eagle Resolve 2015 is the chief exercise that simulates regional threats and challenges through joint operational planning to counter potential emergencies."

~ Col. Mohammed bin Abdullah Al-Mukhaini of Oman

"The outcome has been comprehensive and integrated scenarios for exchanging expertise and unifying visions and concepts."

~ Lt. Col. Osama Hussein Ali, head of Bahrain's delegation

U.S. Air Force Maj. Gen. Rick Mattson, U.S. Central Command director of exercises and training, noted that militaries that rise to greatness are militaries that examine themselves critically.

"Each country has the ability to make inputs and adjust this exercise to develop it exactly how they want — depending on what they're most concerned about — and this is the culmination of it," Gen. Mattson said.

He also expressed admiration for the interministerial coordination Kuwait displayed at Eagle Resolve. "This is the first time we've done that. We're much stronger as a group," the general said.

A prime example of group strength occurred on the last day of field training on Failaka Island. Despite different leadership, doctrines, languages and sometimes equipment, troops from six nations formed a unified amphibious fighting force.

The scene is a quiet beach speckled with abandoned vacation cottages, some of which are enlisted to serve as fortified terrorist command posts. Kuwaiti F/A-18s fly in low to bust these enemy bunkers, followed up by low-altitude strafing by Emirati F-16s. Landing craft punch ashore from several directions, disgorging Kuwaiti Marines and special forces accompanied by Qatari and Turkish Marines. As infantry advance behind armored vehicles, green smoke grenades signal to headquarters that the beach has been captured and a foothold secured for additional operations.

As forces rush inland toward their targets, they summon extra support from Kuwaiti AS332 Super Puma helicopters, out of which commandos fast rope onto enemy positions. Action isn't restricted to the land. Out in the Arabian Gulf, Kuwaiti Navy and Coast Guard patrol boats buzz offshore with help from Saudi Arabia's Al-Siddiq guided missile gunboat. The U.S. Navy ship Fort McHenry throws squads of Marines onto the beach to support their coalition partners. Together, the troops storm a terrorist command post and plant a Kuwaiti flag on the roof.

It might have looked easy, but it was the fruit of at least three days of classroom work and three days of practical exercises for the assault troops, not to mention the logistical complexities of landing tons of military hardware from all branches of the military.

At the conclusion of the exercise, as the last wisps of smoke dissipated from the beach, Deputy Prime Minister and Defense Minister Sheikh Khaled Al-Jarrah Al-Sabah praised the ability of multinational forces to synchronize efforts.

"All have seen the final exercise and noticed the cooperation among the forces, especially in the final exercise that lasted 40 minutes. However, it took so much effort and time to plan it," the Kuwaiti minister said. "I am proud of the professional level that we reached in planning and working together with our brothers in Gulf states and our friends." ✦

A Leader in Regional Cyber Security: Dr. Sherif Hashem

UNIPATH STAFF

Protecting national boundaries goes far beyond border checkpoints in airports, seaports and land crossings. Although many military commanders must focus on beefing up lines of defense with Soldiers and tanks, those charged with cyber security must focus on preventing and patching electronic security holes to stop terror and organized crime groups from disrupting the security of cyberspace.

As nations depend on the Internet to provide services to its citizens and electronically link government agencies, this new front requires the expertise and cooperation of military and civilian leaders. There is no doubt that the mission of cyber security is daunting — it requires expertise and vigilance to identify and prevent security breaches. Just as the names of military commanders who lead their men to victory have become well-known, the names of the exemplary leaders in the field of cyber security are gaining recognition. Dr. Sherif Hashem, vice president for cyber security at the Egyptian National Telecom Regulatory Authority (NTRA), is one of the successful leaders who protects his nation's cyber boundaries against malicious attacks.

After the December 2014 establishment of Egypt's High Council for Cyber-Security, Dr. Hashem was called to serve on the 24-member body dedicated to creating a national strategy to secure the infrastructure and networks of government agencies against cyber attacks.

His professional background is filled with accomplishments, and his resume reveals the legacy of a hard-working man who has held many influential positions in his field. From 2004 to 2013, he was the executive vice president of the Information Technology Industry Development Agency. His work was essential in establishing the Egyptian Root Digital Certificate Authority for e-Signature and the Software Intellectual Property Rights Office. He was also able to facilitate cooperation between information and communications technology companies with research and development institutions.

Dr. Hashem is also responsible

for setting the framework for establishing and operating the Egyptian Computer Emergency Response Team at the NTRA. He is on leave from his professorship at Cairo University.

His academic journey started with a bachelor of science degree in communication and electronic engineering (distinction with honor), followed by a master of science degree in engineering mathematics from Cairo University. In 1993 he earned a doctorate in industrial engineering from Purdue University in the United States. Dr. Hashem also completed the Senior Executive Program at Harvard Business School.

Dr. Hashem built his team at NTRA by selecting experts and talented individuals in the field of cyber security to halt attempts to undermine Egypt's cyber security and ultimately build stability. His impressive reputation and experience in his field have led to positive and collaborative relationships with other cyber security leaders in the region and world.

"Electronic hackers do not have a specific profile and have various objectives. In Canada, for instance, a 12-year-old child successfully hacked into the minister of interior website with the motive of curiosity and meant no harm," Dr. Hashem said in an interview with Egyptian TV. "But there are many organized crime groups like the ones who attempt to hack into the financial sector in Egypt. Those are known criminals who aim to steal money and personal information. In addition, there are countries who have

"There is no one in the world who can claim they are protected 100 percent unless they unplug the Internet wires. Therefore, the agency that falls victims to hacker attacks needs to speak out and seek help from the authority. There is no shame if your network has been hacked."

— Dr. Sherif Hashem

electronic armies that use hacking as a tool for spying, and in some instances they stage attacks against other nations. Therefore, cyber security is a matter of national security."

He continued: "The goal of the center is to educate people about the dangers of hacking, especially in government agencies. The center is also responsible for setting a cyber security strategy to prepare the nation to counter any cyber attack. The government agencies must protect their websites and report any breaches or attack to the authorities and cooperate with them for the investigation and damage assessment analysis. There is no one in the world who can claim they are protected 100 percent unless they unplug the Internet wires. Therefore, the agency that falls victim to hacker attacks needs to speak out and seek help from the authority. There is no shame if your network has been hacked."

One year after Dr. Hashem assumed his position with NTRA, the Egyptian minister of communication and information technology announced that Egypt leads all other African nations in national cyberspace readiness. In addition, Egypt was ranked 27th out of 193 countries in a Global Cybersecurity Index published by the International Telecommunication Union in December 2014, on the same level with Denmark, France and Spain. This is a milestone to make Egypt proud.

Sources: Reuters, Al-Monitor

Kyrgyz Republic
Confronts Extremist Recruiting

UNIPATH STAFF

Over the past year, Kyrgyz security forces have confronted extremism head-on. They have uncovered underground extremist organizations, arrested suspected terrorists and disrupted transport routes for terrorist recruits traveling to join the wars in the Middle East.

"In 2014, the activities of three underground groups of [an extremist organization] came to light in southern Kyrgyzstan," Deputy Prime Minister Abdyrakhman Mamataliyev said in February 2015 at a meeting of the Co-ordination Council of Law Enforcement Agencies of Osh Province. "The authorities ... opened 12 criminal cases and arrested 15 suspects."

The bulk of the Kyrgyz fighters in Afghanistan, Iraq and Syria come from Osh city and Osh province, police say.

"In spite of our progress in solving such crimes, our work must continue on preventing crimes that could ... destabilize our country," Mamataliyev said. "In 2014, we detained 40 citizens affiliated with terrorist groups," he added. "The majority of them had already undergone combat training in Syria."

The Kyrgyz Republic is cracking down on extremists indoctrinating youth. For example, one fighter, Dilyorbek Makhkamov of Osh province, returned home from Syria and tried to recruit uneducated youth, including his own nephew, to fight in Syria in November 2013. He persuaded two other young men to join them, but their parents stopped them. Police arrested Makhkamov in September 2014. He was charged with committing mercenary activities and inciting interfaith hatred. Authorities also investigated his accomplices for ties to international terrorist organizations and other efforts to recruit Kyrgyz youth to fight in war zones.

Recruiters benefit from ignorance of Islam. "It's easy for the [extremists] to brainwash them by distorting ... the Quran," Jakyp Zulpuyev, chief of the Osh province police's 10th Department said. The Kyrgyz government and citizens are working together to thwart militant activities. Mosques, apartment blocks, women's councils and local youth groups have all been sites of outreach events, Zulpuyev said.

The public is trusting law enforcement more, said Mirlan Toktomushev, imam of the Osh Sheyit-Dobo Mosque. "Thanks to the continuing meetings, congregations have come to realize that the police and clergy want to protect them against reckless deeds, crimes and radical groups," he said. "The public now is willing to tell the police about strangers who are recruiting youths."

Teachers and pupils discuss religious literacy in high school and are helping to defeat extremist and terrorist recruiting, Zulpuyev said.

"Such [informational] activities are taking place among high school students in Osh city and in Aravan, Kara-Suu and Uzgen districts, where the 'jihadists' are the most active," Zulpuyev said. "The children present their own essays, poems and drawings. [These activities] lead to the children forming anti-extremism opinions and arouse patriotic spirit in them."

GETTY IMAGES

Thousands of Muslims take part in Eid al-Fitr prayer in Bishkek, Kyrgyz Republic. Leaders are making gains to stop extremists who distort Islam to gain recruits to fight in places such as Syria.

Turkmenistan Looks to Enhance Security

UNIPATH STAFF

Concerned with increasingly aggressive Russian foreign policy toward former Soviet states and the need to defeat the Taliban in neighboring Afghanistan, Turkmenistan is reaching out for alternative solutions to improve security. In March 2015, Gen. Lloyd Austin, head of U.S. Central Command, said Turkmenistan had inquired about enhanced security cooperation with Western partners.

The move comes as Turkmenistan is also trying to improve energy security. The European Union (EU), seeking to diversify energy supplies in the face of geopolitical energy instability, is working to build the Southern Gas Corridor, which would bypass Russia and bring Turkmen gas directly to European markets.

With about 10 percent of the world's proven natural gas reserves, Turkmenistan has worked diligently over the past decade to break its own dependence on Russian pipelines and reduce its exposure to the use of gas as a geopolitical weapon. Russia's Gazprom recently announced it would unilaterally reduce gas purchases from Turkmenistan, motivating Ashgabat to reprioritize ties with Western partners.

Turkmenistan's developing military cooperation with the U.S. and energy cooperation with the EU is viewed as a way for the country to develop a more independent foreign policy free of Soviet era entanglements.

Source: The Centre for Eastern Studies (Poland)

A natural gas processing plant at the Galkynysh gas field in eastern Turkmenistan sends much of its output to China.

REUTERS

QATAR HOSTS CYBER CRIME WORKSHOP

QATAR MINISTRY OF INTERIOR

Qatar's Drugs Enforcement Administration (DEA) of the Ministry of Interior hosted a workshop on cyber investigations that ended in April 2015. The course was held in association with the United States Drug Enforcement Administration Dubai Office.

Capt. Muhammad Abdullah al Khater, head of the International Affairs and Studies Section at the DEA, said the course investigated developments in cyber crimes and the latest methods to track down perpetrators and bring them to justice.

He pointed out that the workshop dealt with two aspects: a theoretical study of traditional investigative techniques, and skills of interrogation, surveillance and operations, as well as a look at Internet protocols, and use of telecommunications and social media applications such as WhatsApp and Instagram.

SAUDI ARABIA CONDUCTS MAJOR EXERCISE

UNIPATH STAFF

Saudi Arabia elevated it levels of interagency cooperation to combat the increased threat of violent extremism in the kingdom. Saudi security forces, under the leadership of Minister of the Interior His Highness Prince Mohammad bin Nayef bin abd al-Aziz, started its first multilateral exercise for security forces, called Watan 85, in February 2015.

The exercise was held near the kingdom's northern border and consisted of 1,500 personnel representing border guards, special forces, SWAT, aviation security, civil defense, and command and control of the Ministry of the Interior.

The events covered many security scenarios, including countering the use of car bombs at border checkpoints, monitoring sleeper cells planning to attack government installations, providing emergency medical care, suppressing fire, and restoring order and security during crises.

The exercise was welcomed by many Saudi citizens, who expressed confidence in their security forces on social media.

Source: alriyadh.com

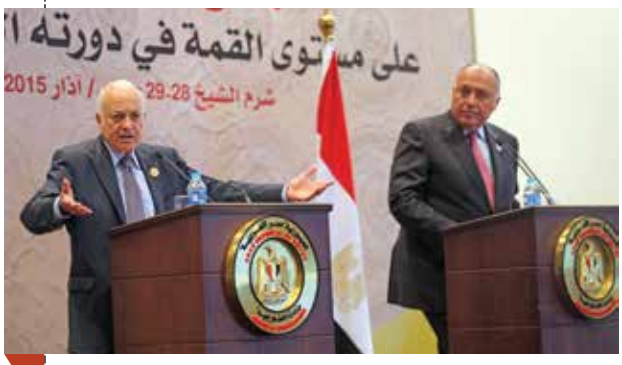
Arab League Announces Joint Military Force

THE ASSOCIATED PRESS

A two-day Arab summit in March 2015 ended with plans to discuss the formation of a joint Arab intervention force. Arab leaders took turns addressing the gathering about the threat posed to the region's Arab identity by what they called moves by "foreign" or "outside parties" to stoke sectarian, ethnic or religious rivalries in Arab states. A summit resolution said the joint Arab defense force could be deployed at the request of any Arab nation facing a national security threat and that it could also be used to combat terrorist groups.

In Yemen, the Houthis swept down from their northern strongholds in 2014 and captured Yemen's capital of Sanaa in September. Yemeni President Abed Rabbo Mansour Hadi was forced to leave.

Yemen Foreign Minister Riad Yassin said the air campaign, code-named Operation Decisive Storm, had prevented rebels from using seized weaponry to attack Yemeni cities or target neighboring Saudi Arabia with missiles.



Arab League Secretary-General Nabil Elaraby, left, speaks during a press conference with Egyptian Foreign Minister Sameh Shukri at an Arab summit meeting in Egypt in March 2015. THE ASSOCIATED PRESS

At the summit's closing session, Arab League head Nabil Elaraby said the Saudi-led air campaign would continue until all Houthi criminals "withdraw and surrender their weapons," and a strong unified Yemen returns.

"Yemen was on the brink of the abyss, requiring effective Arab and international moves after all means of reaching a peaceful resolution had been exhausted to end the Houthi coup and restore legitimacy," Elaraby said.

Egyptian President Abdel-Fattah el-Sissi said the leaders from 22 nations also agreed to create a joint Arab military force whose structure and operational mechanism will be worked out by a high-level panel under the supervision of Arab chiefs of staff.

"There is a political will to create this force and not to leave its creation without a firm time frame," Egyptian Foreign Minister Sameh Shukri told a news conference. The Egyptian military and security officials have said the proposed force would consist of up to 40,000 elite troops backed by jet fighters, warships and light armor and would be headquartered in either Cairo or Riyadh.

Omani Army **Promotes Traffic Safety**

UNIPATH STAFF

The Sultanate of Oman's Army organized a day dedicated to traffic safety in March 2015 — part of a Gulf Cooperation Council weeklong event. Using the slogan "Your decisions set your fate," the event invited guest of honor Staff Maj. Gen. Muttar Bin Salim Bin Rashid Al-Baluchi, commander of the Omani Sultanate Army. The celebration was held at the Sultanate's Armed Forces Transportation Academy.

Staff Gen. Mohamad Bin Galib Al-Jamoudi, commander of logistics in Oman's Armed Forces, gave a speech to encourage people to eliminate traffic accidents. He also expressed appreciation for the efforts of the Armed Forces' drivers to avoid accidents and the corresponding loss of life and property.

The celebration included a presentation from a traffic police officer with statistics about casualties of traffic accidents as well as an overview of the causes of accidents: excessive speed and the use of cellphones while driving.

The event concluded with awards presented to excellent drivers. Gen. Al-Baluchi encouraged all drivers in the Omani military to set examples of responsibility and to continue their respect of traffic and safety laws. Similar events took place in countries across the Gulf region.

Turkmenistan Hosts Peace Forum

NATO

Experts from five Central Asian states and Afghanistan gathered in Ashgabat, Turkmenistan, in March 2015 for a NATO-sponsored regional conference on "Peace and Stability in Central Asia and Afghanistan: A View from Neutral Turkmenistan."

This high-level event, organized jointly by the Ministry of Foreign Affairs of Turkmenistan and the office of the NATO Liaison Officer in Central Asia, was unprecedented in the history of Turkmenistan's partnership with the alliance.

It was the fourth in a series of NATO-sponsored events marking the 20th anniversary of the Partnership for Peace program in the Central Asian partner states. Moreover, it was included in Turkmenistan's official program of events celebrating the "Year of Neutrality and Peace" on the 20th anniversary of the United Nations General Assembly Resolution recognizing the country's neutrality.

Turkmenistan Deputy Foreign Minister Berdyniyaz Myatiev opened the event, while James Appathurai, the NATO secretary-general's special representative for the Caucasus and Central Asia, addressed participants by video link from NATO headquarters.

Turkmen participants included officials and experts from a wide range of institutions, including the Ministry of Foreign Affairs, the Ministry of Defense, Ministry of Interior, the Prosecutor-General's Office, the Institute of State and Law under the President of Turkmenistan, the Institute of International Relations and the International University of Humanities.

Experts from Afghanistan, Kazakhstan, the Kyrgyz Republic, Tajikistan, Uzbekistan and the United States, and representatives of the United Nations Regional Centre for Preventive Diplomacy for Central Asia, the United Nations Development Programme, the European Union, and the Organization for Security and Co-operation in Europe also spoke at the event.

> *"We are all faced with nonstate threats, which no state in the region is able to deal with on its own."*
>
> — Dr. Ulugbek Khasanov, associate professor at the University of World Economy and Diplomacy, Uzbekistan

Ambassador Sapar Berdyniyazov, special envoy of the Turkmen Ministry of Foreign Affairs underlined Ashgabat's neutral status and transparent foreign and defense policies, saying that these have helped it gain the trust of its neighbors and help prevent and resolve conflicts. He also recalled Turkmenistan's support for the stabilization of neighboring Afghanistan, both bilaterally and multilaterally, through the Heart of Asia/Istanbul Process.

Dr. Ulugbek Khasanov, associate professor at the University of World Economy and Diplomacy, Uzbekistan, stated that "we are all faced with nonstate threats, which no state in the region is able to deal with on its own."

Dr. Kuralai Baizakova, professor at Al-Farabi Kazakh National University, Kazakhstan, noted that "the degree of importance of common threats is perceived differently by different Central Asian states." She advocated the development of new regional mechanisms, for instance, on sharing water resources, which could become a factor for rapprochement in Central Asia.

Elnura Omurkulova-Ozierska, researcher at the National Strategic Studies Institute, Kyrgyz Republic, highlighted the increasing threat to Central Asian security posed by radicalization, while warning that harsh counterterrorism policies adopted by some countries can be counterproductive.

Haroun Mir, director of the Centre for Research and Policy Studies in Afghanistan, praised the international community's enormous contribution to Afghanistan. Although he saw 2015 as a major test of the ability of the Afghan National Security Forces to ensure security throughout the country, he also highlighted a window of opportunity for national reconciliation, expressing the hope that 2015 would witness a breakthrough in the Afghan peace process.

Participants also exchanged views about the threat posed by radicalization and the terrorist group Da'ish; bilateral border and energy-related tensions among Central Asian states; the narcotics problem and the importance of tackling it effectively; and other security-related topics.

IRAQI COUNTERTERRORISM UNITS FIGHT DA'ISH

MAJ. TIMOTHY CHAVIS/U.S ARMY

In March 2015, more than 700 Iraqi Soldiers graduated from the Counter-Terrorism Service (CTS) Academy's commando training after a tough two-month program in which one out of every five trainees drops out.

Multiple nations are contributing to the training of Iraqi security forces. That includes the Iraqi CTS Academy, which supports the CTS in its battle against Da'ish by providing about five courses annually. As special operations forces cannot be mass produced while maintaining their specialized skill set, the CTS is selective with its recruits, while still meeting the demands of the CTS battalions fighting Da'ish. Ensuring that the force remains representative of Iraqi society, recruits cover the range of the country's religious sects, ethnicities, tribes and regions, which has helped build trust in the fight against Da'ish.

"Before Da'ish swept into Anbar, the CTS course was about 30 days long, but the CTS leadership knew they needed more training, so the new curriculum was developed in response to the current situation," said Maj. Gen. Fallah, director of academia for the CTS Academy. "The training includes demanding physical fitness, urban warfare, multiple weapons training, tactical maneuvers and most importantly, how to work as a team and protect each other."

Fallah said the training has become more organized and tougher over the past year with the help of coalition partners, who have added crucial new lessons on providing tactical medical care and dismantling improvised explosive devices.

Fallah said the training continues to develop based on feedback from the CTS units. In 2014, each CTS battalion rotated companies through the academy for refresher training with an emphasis on urban warfare.

Twenty-four graduating students were selected for a follow-on sniper course, but according to Fallah, the rest are needed at their battalions to continue CTS gains against Da'ish.

"Many Soldiers have been wounded or killed during the fight against Da'ish, and the [CTS] battalions need new Soldiers who are ready to fight the enemy, not to protect just Iraq, but to protect all the world because Da'ish is dangerous for the whole world."

MAJ. TIMOTHY CHAVIS/U.S. ARMY

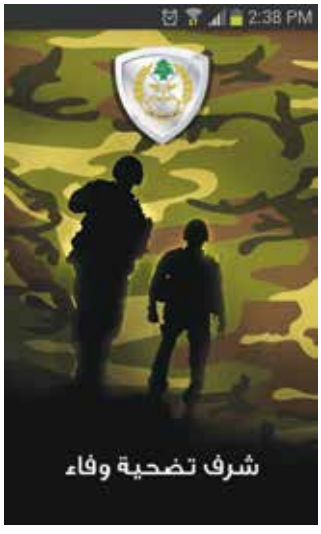
Counter-Terrorism Service Academy commando recruits receive assignments by lottery during the graduation ceremony. Assignments are distributed so that regional and sectarian distinctions are de-emphasized.

LEBANESE ARMY MOBILE APP WINS UAE AWARD

UNIPATH STAFF

A Lebanese Army mobile application was the winner of the Best Mobile Government Service Award at the Dubai Government Summit 2015, sponsored by the United Arab Emirates in February.

LAF Shield, available for Android and iOS operating systems, allows users to take pictures, record videos, and send messages to report suspicious activity and security incidents to law enforcement. The tool offers an interactive map identifying dangerous locations and can receive Army news, videos and photos.



The annual award is a product of the newly launched "Smart Government" vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum, UAE vice president, prime minister and ruler of Dubai, intended to encourage government entities to produce innovative government service solutions via smartphone applications and mobile phones.

Participants from 97 countries attended the conference, including His Highness Sheikh Mohammed, Dubai and Abu Dhabi Crown Prince Sheikh Mohamed bin Zayed Al Nahyan, United Nations Secretary-General Ban Ki-moon and Queen Rania of Jordan.

TAJIKISTAN INTERRUPTS FLOW OF FIGHTERS TO SYRIA

UNIPATH STAFF

Tajik authorities are using a media campaign, as well as the threat of prosecution, to deter citizens from going to Syria to join Da'ish terrorists.

In 2014, Tajikistan made fighting abroad a criminal offense. The government reports that about 300 Tajik nationals have joined Da'ish. Officials have emphasized they will offer amnesty to anyone returning to Tajikistan voluntarily, as long as no crime has been committed.

"We have issued instructions that [just] making a trip to such countries should not result in a criminal case against the individual concerned. A criminal case can be launched only if we have enough information and evidence to show that the individual was a member of an armed group in a foreign country," said Sharif Qurbonzoda, chief prosecutor for the northern Sughd province.

Authorities stress that they will prosecute if evidence points to a crime. For instance, in November 2014, almost 30 people from Istaravshan and Kanibadam districts were arrested for suspected involvement with a group known for recruiting foreign fighters for Da'ish.

Part of the government's strategy to fight foreign-fighter recruitment includes a media campaign. Relatives of extremist fighters and youth groups make videos to speak to the public about the dangers.

Local media say recruiters use a variety of tactics to gain more fighters. "I think they initially are offered a lot of money, and then their passports are taken away and burnt," said Rustam Davlatshoev, a Khatlon region lawyer. "They're left with no choice but to obey the orders of these radical groups, under threat of execution."

Obidjon Ahmedov, an official in Isfara district, said recruiters exploit people's understanding of the fighting in Syria to persuade them to take part in the conflict. "These groups use the fact that people are not well-informed. Sending people to Syria has become a kind of business for them," he said.

Sources: Institute for War & Peace Reporting, *Eurasia Review*

Saudi Leader Calls for Compulsory Military Service

UNIPATH STAFF

Saudi Arabia's Grand Mufti His Excellency Sheikh Abdulaziz bin Abdullah al-Sheikh has called for mandatory military service for young men.

"Compulsory military service for our youth is important and required," he said during a Friday sermon in April 2015.

In the past few years, fellow Gulf Cooperation Council members Qatar and the United Arab Emirates have introduced mandatory military service. Leaders in both countries have said the programs aim to strengthen national defense, while cultivating a spirit of national pride in youth.

In April, Kuwait passed a law that will take effect in 2017 reinstating compulsory military service for young men; the country suspended the mandatory service program in 2001.

Sources: Akhbaar24 News, Al Arabiya, *Al Defaiya*; *Gulf Business*

Saudi Soldiers exercise before a military parade.
THE ASSOCIATED PRESS

GCC Navies Participate in Union 17

UNIPATH STAFF

The naval forces of the Gulf Cooperation Council (GCC) participated in the joint exercise Union 17 in the United Arab Emirates in March 2015 to increase force readiness.

The annual exercise brought together naval forces from Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates with the goal of improving leadership and facilitating cooperation and collaboration so that they can better overcome shared threats.

The 10-day exercise was designed to increase combat efficiency and promote cooperation among GCC countries. The exercise focused on operational concepts and executing joint Navy operations, as well as exchanging best practices and experiences.

Sources: Saudi Press Agency, *Al Defaiya*

EGYPTIAN FORCES INTERCEPT 3.5 TONS OF DRUGS

UNIPATH STAFF

In cooperation with international efforts to deplete terrorist financial networks and combat drug trafficking, in March 2015 the Egyptian Navy and border protection forces captured a ship carrying about 3.5 tons of hashish destined for Egypt and a neighboring country.

After identifying and locating the suspect ship, the Armed Forces boarded and searched it 55 miles from Damietta port on the Mediterranean Sea. The vessel had tried to evade the Egyptian Navy, but firing warning shots forced the ship to stop.

Egyptian forces found that the ship carried a crew of eight along with 68 pallets of hashish. The ship and crew were seized by the anti-narcotics authority for investigation and legal review.

Drug trafficking is an important tool for terrorists to finance recruitment and attacks. The region has witnessed increased drug smuggling as a prelude to attacks in places such as the Sinai and Iraq. Such spikes in smuggling suggest that violent extremists feel the need to raise more cash.

Source: Egyptian Ministry of Defense

Partners Tackle the Problem of Violent Extremism

STORY AND PHOTO BY **MAJ. EBONY N. CALHOUN**/U.S. ARMY CENTRAL PUBLIC AFFAIRS

Military representatives from Bahrain, Egypt, Lebanon, Oman, Qatar, the United Arab Emirates and Yemen met in Washington, D.C., in April 2015 for U.S. Army Central's first Senior Strategy Session on the Arabian Peninsula and Levant. The event was held with support from the Near East South Asia Center for Strategic Studies (NESA).

The five-day session brought together some of the region's leading strategists and academic experts to exchange perspectives on what makes the Middle East such a complex region. Lebanese Brig. Gen. Calude El Hayek noted, "Holding conferences like this has positive effects in approaching perceptions, sometimes about conflicting matters taking place in various parts of the world. At the same time, it builds, nourishes and maintains partnership among nations. The conference effectively represented a free stage for every represented nation to exercise freedom of expression, exchange of ideas and an opportunity for the representatives to strengthen social and political ties among each other. Such conferences offer great opportunities for the best partnership building."

During the exchange, 30 representatives from the seven partner nations and the U.S. Army received presentations from experts from the U.S. Department of State, George Washington University, the National Defense University and other agencies. Topics included military support during humanitarian disasters and the impact of oil production on stability in the Middle East. All participants agreed that these were compelling discussion points, but several attendees mentioned that the most salient presentations addressed terrorism.

"There are many different conflicts in the Middle East. It's not only Da'ish or ISIS. It's not only the al-Qaida-affiliated organizations," said NESA professor Dr. Murhaf Jouejati, who is originally from Syria. "In that onion, there are many, many layers. We have only touched some of them this week."

During his lecture on the nature of terrorism, Dr. David Ucko, professor of strategic studies at the National Defense University, asserted that the challenges extremism pose to the political and military environment are unique and increasingly complicated.

"Insurgent groups will use terrorism as one of many different actions of strategic components. They have the political standing. They may use subversion. They use maybe the provision of government services. Maybe they might have an education section that essentially educates the next generation," said Dr. Ucko. "The reason they can do all of this is because they have a certain political following."

Leaders from Bahrain, Egypt, Lebanon, Oman, Qatar, the United Arab Emirates and Yemen take part in a panel discussion during the U.S. Army Central Senior Strategy Session on the Arabian Peninsula and Levant in Washington, D.C., in April 2015.

Throughout the exchange, members from several delegations echoed Dr. Ucko's remarks, stating that terrorism has no single source of motivation, so the problem cannot be viewed with a single focus.

Participants and event organizers felt that the foundation for confronting terrorism requires an ongoing exchange of ideas like the type of dialogue experienced in the Senior Strategy Session.

"There were some tough problem sets discussed. Tough issues. There are no easy solutions," said Maj. Gen. Dana Pittard, deputy commanding general, Operations, U.S. Army Central, in his closing remarks. "We continue the dialogue. We use this conference as yet another forum to build relationships, because this relationship building will help us eventually understand more to tackle some of these problems in the future."

Kazakhstan Hosts Steppe Eagle

STORY AND PHOTO **BY MAJ. ANGEL JACKSON**/U.S. ARMY CENTRAL

The annual Steppe Eagle military exercise kicked off with a ceremony at the Ilisky Training Area in Almaty, Kazakhstan, in April 2015. Soldiers from Kazakhstan, the United Kingdom and the United States joined forces for a two-phase training event designed to refine peacekeeping and peace support operations, while improving interoperability and military cooperation with key partner nations.

In its 13th iteration, Steppe Eagle provided multilateral forces with the opportunity to promote cooperation among participating forces, practice crisis management and enhance readiness through realistic, modern-day interactive scenarios.

Kazakhstani Soldiers march at the opening ceremony of Steppe Eagle 2015.

Gen. Maj. Daulet Ospanov, commander of the Kazakhstan Airmobile Forces, recognized the importance of the exercise.

"The experience gained by our Soldiers is very valuable," said the general. He added that with their partners, the Kazakhstanis would work on enhancing interoperability and readiness in order to participate in joint peacekeeping operations with partner nations.

Col. Andrew Berrier, U.S. defense attaché, noted Steppe Eagle is growing more important as partner nations get closer to deploying on United Nations peacekeeping missions.

"All partners in Steppe Eagle share a unifying vision of contributing to peace and stability around the world, and to ease the suffering of those less fortunate," said Berrier. "It is this common commitment to U.N. principles that sets Steppe Eagle apart as a unique venue for cooperation."

Af-Pak Officials Cooperate to Counter Terrorism

UNIPATH STAFF

Officials from Afghanistan and Pakistan are continuing to work toward a common goal of rooting out terrorism in the region and building a relationship based on trust.

"Our focus is on enhanced political engagement, security and counterterrorism cooperation, trade and economic partnership, and regional cooperation," said Pakistan Prime Minister Muhammad Nawaz Sharif, according to *The News International*. "Both the countries have paid a very heavy price at the hands of terrorism, and now we have launched the Operation Zarb-e-Azb, which has broken the backbone of terrorist networks in the country. We have a commitment not to allow territories to be used against each other."

His statement came after a March 2015 meeting with Afghan Minister for Refugees and Repatriation Sayed Hussain Alemi Balkhi. Pakistan supports an Afghan-led peace and reconciliation process and internationally endorsed plans to aid Afghan refugees, Sharif said.

Balkhi thanked Pakistan for planeloads of relief supplies for Afghans devastated by a series of avalanches in February 2015 that killed more than 250 people. He described the increasing cooperation between the neighboring countries as historic and called Sharif a visionary leader who is prioritizing peace.

Balkhi said the people of Afghanistan wish to focus on building the country through economic development.

Pakistani Prime Minister Muhammad Nawaz Sharif, left, and Afghanistan President Ashraf Ghani shake hands during the South Asian Association for Regional Cooperation summit in Nepal in November 2014. THE ASSOCIATED PRESS

UZBEKS **CONFRONT** DA'ISH

UNIPATH STAFF

Concerned about its citizens traveling illegally to Syria to support Da'ish, Uzbekistan has begun an anti-terror campaign to stem the flow.

In late March 2015, before the Nowruz holiday, the Uzbek Ministry of Internal Affairs conducted an anti-terror operation called Anti-terror Cleansing.

Abdulaziz Mansur, deputy chairman of the Muslim Board of Uzbekistan, has also urged Uzbeks to write books and articles exposing Da'ish as murderers and criminals to undermine the terrorist group's appeal to the young.

By early 2015, there was increasing evidence that Da'ish may be reaching into Afghanistan and threatening neighboring Central Asian countries. Afghan officials reported that hundreds of foreign fighters had entered the country under the black flag of Da'ish, and several Taliban leaders have declared allegiance to the terrorists.

REUTERS

Uzbeks walk by election campaign posters in Tashkent in March 2015. Authorities uncovered a terrorist plot to disrupt the elections.

Uzbekistan's homegrown extremist group, the Islamic Movement of Uzbekistan (IMU), may also have established an affiliation with Da'ish. Uzbekistan's National Security Service (NSS) believes that the IMU has provided fighters for the Syrian war.

Alisher Khamadov of the NSS sees an increased threat from the IMU, especially from fighters returning from the Middle East. Khamadov told Russian news agency RIA Novosti in February 2015 that captured IMU members had revealed a plan for a series of terrorist attacks in Uzbekistan. Afghan security officials have also reported increased IMU presence in northern Afghanistan, near the borders with Turkmenistan and Uzbekistan.

Sources: RIA Novosti, Regnum.ru, The Long War Journal, BBC News

JORDAN ENHANCES SECURITY PARTNERSHIP WITH TUNISIA

UNIPATH STAFF

In the aftermath of the horrific terrorist attack at a Tunisian museum, the head of Jordanian general security, Staff Gen. Towfeq Hamid Altwaliba, met in Amman with Tunisia's ambassador to Jordan, Afifa Al-Malah, to discuss security cooperation. The March 2015 meeting also included talk of an information exchange as well as cross training in security.

Altwaliba stated that the Directorate of General Security is continuously working to enhance its performance and expand staff capability through specialized security training. He said he invited the Tunisian national security staff to enroll in any security training offered at the Jordanian security academy.

The ambassador expressed her confidence in Jordan's Directorate of General Security and its role in the community. She cited the directorate's work in educating and informing citizens to prevent them from falling prey to terrorist ideology and using distortions of religion to deceive the uninformed. "The effort of the directorate shows in the noticeable security and stability in the kingdom," she said.

Jordanian officials have been vocal in their condemnation of the terrorist attack on the National Bardo Museum in Tunis on March 18, 2015. Minister of State for Media Affairs Mohammad Momani said Jordan stands by Tunisia against extremism and terrorism.

Momani reiterated Jordan's firm position against terrorism and called for concerted international efforts to fight this shared threat to international peace and security. The fight against terrorist organizations and their ideology is the responsibility of all countries of the world, particularly Arab and Muslim countries, he said.

Sources: Petra – Jordan News Agency, www.assabahnews.tn/

SHARING KNOWLEDGE

Unipath is a magazine provided free to those associated with security matters in the Middle East and South and Central Asia.

CONTRIBUTE TO *UNIPATH*

Send all story ideas, letters to the editor, opinion articles, photos and other content to *Unipath's* editorial staff at unipath@centcom.mil.

SUBMISSION TIPS

- Content submitted in your native language is preferred. *Unipath* will provide translation.
- Articles should not exceed 1,500 words.
- Please include a short biography and contact information with each submission.
- Photo file size should be at least 1 megabyte.

RIGHTS

Authors retain all rights to their original material. However, we reserve the right to edit articles to meet space and style requirements. Article submission does not guarantee publication. By contributing to *Unipath,* you agree to these terms.

FOR A FREE SUBSCRIPTION

Email: unipath@centcom.mil
Or write to: Unipath
U.S. Central Command
7115 S. Boundary Blvd.
MacDill AFB, FL 33621 USA

Please include your name, occupation, title or rank, mailing address and email address.

http://unipath-magazine.com {VIEW US ONLINE} **www.facebook.com/unipath**