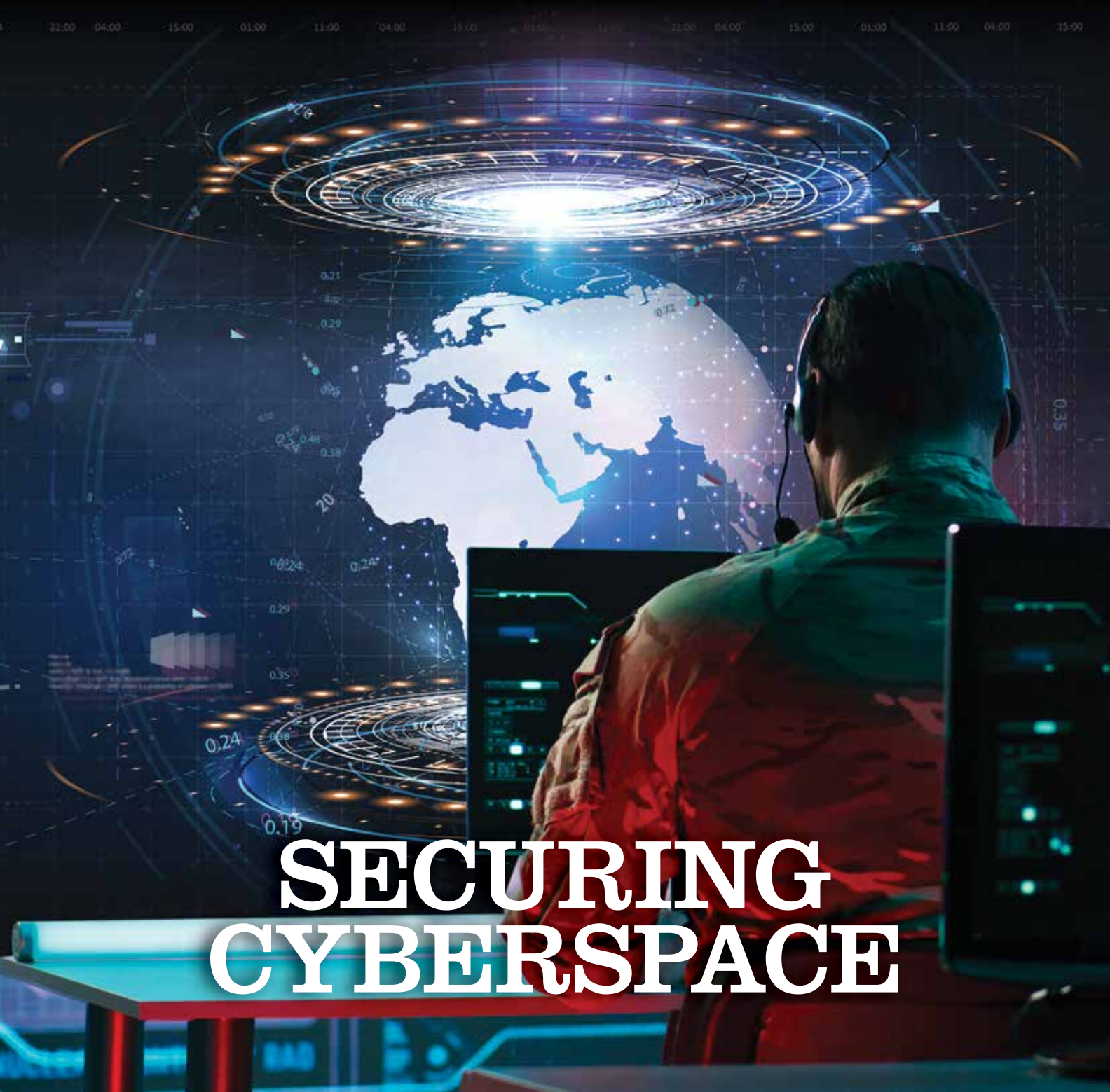
Qatar Accomplishes Refugee Rescue

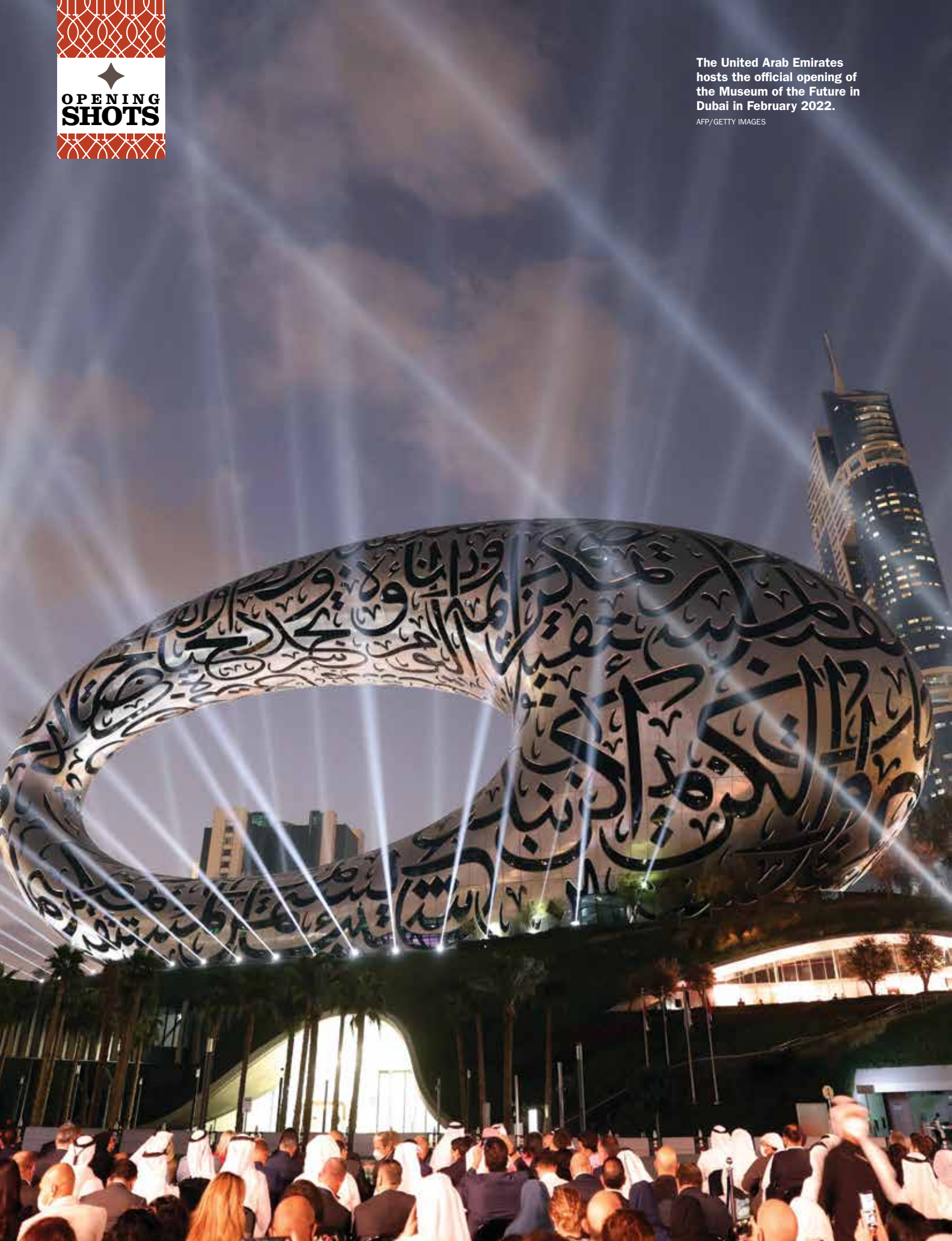
Jordanian Navy Defends Waterways

Protecting Yemen's Territorial Integrity

UNIPATH



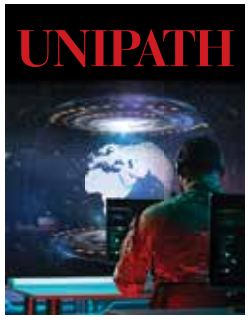
SECURING CYBERSPACE



The United Arab Emirates hosts the official opening of the Museum of the Future in Dubai in February 2022.
AFP/GETTY IMAGES

A Kazakh woman celebrates Nowruz, an ancient holiday marking the spring equinox, in Almaty in March 2022. REUTERS

TABLE OF CONTENTS



ON THE COVER:
As part of their defensive role, militaries must protect society against cyberattacks and internet-based terrorist recruitment. UNIPATH ILLUSTRATION

UNIPATH

Securing Cyberspace

Volume 11, Number 4

CENTCOM COMMANDER

GEN Michael "Erik" Kurilla
U.S. Army

CONTACT US

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

CENTCOM.UNIPATH@MAIL.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 South 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

I would like to thank United States Central Command for giving me the opportunity to write the editorial for this edition of Unipath magazine dedicated to protecting cyberspace.

The more the world advances and relies on technology, the more the risk of chaos increases if computers and servers that control the online infrastructure are destroyed. This includes transportation, electricity, gas, desalinization plants or financial services by banks, stock exchanges and financial centers, whether caused by an actor or natural disaster. It would be the stuff of nightmares and could actually mean the return of the world to the Stone Age.

The malfunction of servers belonging to some technology giants, social networking sites and applications shows how fragile the world is, with people feeling alone, isolated and empty. It also reveals the extent of our reliance on social media and exposes us to threats that endanger our very existence, putting us in a "to be or not to be" situation regarding threats we must be prepared for.

Perhaps the coronavirus pandemic and its deadly repercussions have increased fear among humanity because of the insistence on social distancing, the tendency to use remote communication, and the prevalence of visual, audio, and other applications. This has increased concerns about protecting cyberspace: In this confrontation with nature itself, cybersecurity has become an existential battle to maintain the well-being of humanity.

The world must prepare for these scenarios, considering them a global war that must be faced. The role of armies is no longer restricted to countering potential threats but also includes studying trends and trajectories to put appropriate plans in place to anticipate emerging threats, foremost among which is securing cyberspace for human civilization. This has become an existential issue: We should protect cyberspace by all means necessary.

Cyberwarfare includes spying on states, stealing trade and military secrets, attacking computers responsible for operating critical infrastructure and weapons systems, breaching critical security and economic information, and targeting critical service or national security facilities of adversarial states.

This emerging style of warfare transcends land, air and naval battlefields. Countering these attacks requires the concerted efforts of all state institutions to work as a robust system of defense that is difficult to penetrate.

In days gone by, human knowledge multiplied over decades and centuries. But now, thanks to the information revolution, this multiplication occurs every hour, and this constant and rapid advancement achieved by the world every day brings with it threats as well as opportunities.

The byproduct of the digital age lies in the tendency of some governments, organizations and individuals to abuse technology, using it detrimentally in a stark violation of human rights and international treaties and charters to exploit the lack of international consensus. This requires institutions of the international community to take responsibility by safeguarding technological achievements and protecting them from miscreants, both governmental and individual, and to work toward the creation of an entity to monitor unlawful states, organizations and or individuals, and to prosecute and punish them by international law.

In the State of Kuwait, we take the issue of protecting cyberspace seriously. The Council of Ministers, in its session of May 31, 2021, approved the creation of the National Cybersecurity Center and assigned the minister of foreign affairs and the minister of state for cabinet affairs to prepare a draft decree to formally announce the center, in coordination with a number of ministries and state institutions active in this field.

This center handles the coordination and combined efforts of all state institutions to protect its cyberspace from attacks that may occur amid global cyber chaos.

It also required all domestic institutions to have a tactical goal by securing their networks, and a strategic goal, which was to take part in protecting state cyberspace and acting as a joint entity under the umbrella of the National Cybersecurity Center.

At the Ministry of Defense level, the partnership between the Kuwait Army and U.S. Central Command in the field of information security technology is an example of desired international cooperation. Regular training courses, workshops and joint activities are held to mitigate risks and protect information security systems and domestic networks.

Cybersecurity is not just the task of one country, but one fulfilled by a coalition of international partners who possess the technology and know-how to confront the constantly evolving threats to computer systems that the world and human civilization depend on.

Maj. Gen. Mohammed Aqla Al-Anezi,
Commander of Kuwait Army Signal Corps

COLLECTIVE DEFENSE:

A U.S. Cyber Command Perspective

LT. GEN. CHARLES MOORE, DEPUTY COMMANDER OF U.S. CYBER COMMAND

In November 2020, more than 158 million Americans voted in our national elections. Because voting is so foundational to our democratic republic, Americans must have confidence that our election processes and outcomes are free of foreign interference and that covert foreign attempts to influence voters are mitigated. Four years earlier, malicious cyber actors sought to influence voters using operations in cyberspace.

Determined to prevent similar activities during the 2018 and 2020 national elections, agencies across the U.S. government established a cross-functional and collaborative team to identify threats, share information and coordinate actions. These agencies included the Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, and United States Cyber Command (USCYBERCOM).

Additionally, the team worked closely with allied nations and industry partners to advance its efforts. This is an example of the type of collective defense required to safeguard our democratic processes and nation as a whole.

To defend our nation in cyberspace, USCYBERCOM executes a "defend forward" strategic and operational approach. Because of the inherent global nature of the cyberspace domain, the majority of threats to our nation originate in foreign cyberspace, also known as red space. Combating 21st century threats requires speed and agility — and partnerships — to seek and locate adversaries in red space before they can harm U.S. and allied data systems, weapon systems and networks.

Simply put, we want to take out the archer rather than dodge the arrows. The intelligence gathered during our operations is also shared across agencies and with partners and allies to develop a common situational awareness of possible threats, advance unity of effort, and enable an integrated and synchronized response.

LT. GEN. CHARLES MOORE

Similar to our efforts in other warfighting domains, unity is critical to our success in cyberspace, and partnerships are essential part of that endeavor. It is not surprising, therefore, that partnership is a critical component of the U.S. National Defense Strategy and USCYBERCOM's strategic approach. Because cyberspace cuts across all aspects of modern society, defending it has been referred to as the "ultimate team sport." It is essential that we develop, advance and mature our partnerships across the government to include allies, industry, and academia into persistent and collaborative efforts.

One way USCYBERCOM is developing partnerships under the framework of collective defense is by using hunt forward operations (HFOs). At the invitation of a partner country, we deploy teams of skilled cyber warriors who

An American goes to vote in New York in 2020. Securing elections from foreign interference is part of USCYBERCOM's mission. GETTY IMAGES

specialize in hunting malicious cyber activities on partner networks. As part of this effort, our cyber teams gather valuable intelligence and identify potential threats to our own networks while simultaneously enabling the host nation to improve its network defense and resilience.

At the conclusion of each HFO, the team sends the host nation a report on its vulnerabilities as well as strategies to prevent hacking on its networks. The information the team gathers about adversary tactics, techniques and procedures (TTPs), as well as evidence of malware attempting to compromise systems, is also shared with the global cybersecurity enterprise. In some instances, HFOs yield malware samples that USCYBERCOM can publicly disclose so that domestic and allied networks may better defend against future compromises. HFOs began in 2018 as part of our election defense efforts and now are conducted around the globe.

An additional way to improve our partnerships for collective defense is through exercises to develop interoperability and readiness. As with any military operation, it is important that allied and partner countries continuously train together to become familiar with each other's strengths, weaknesses and TTPs. Our goal is to operate together seamlessly.

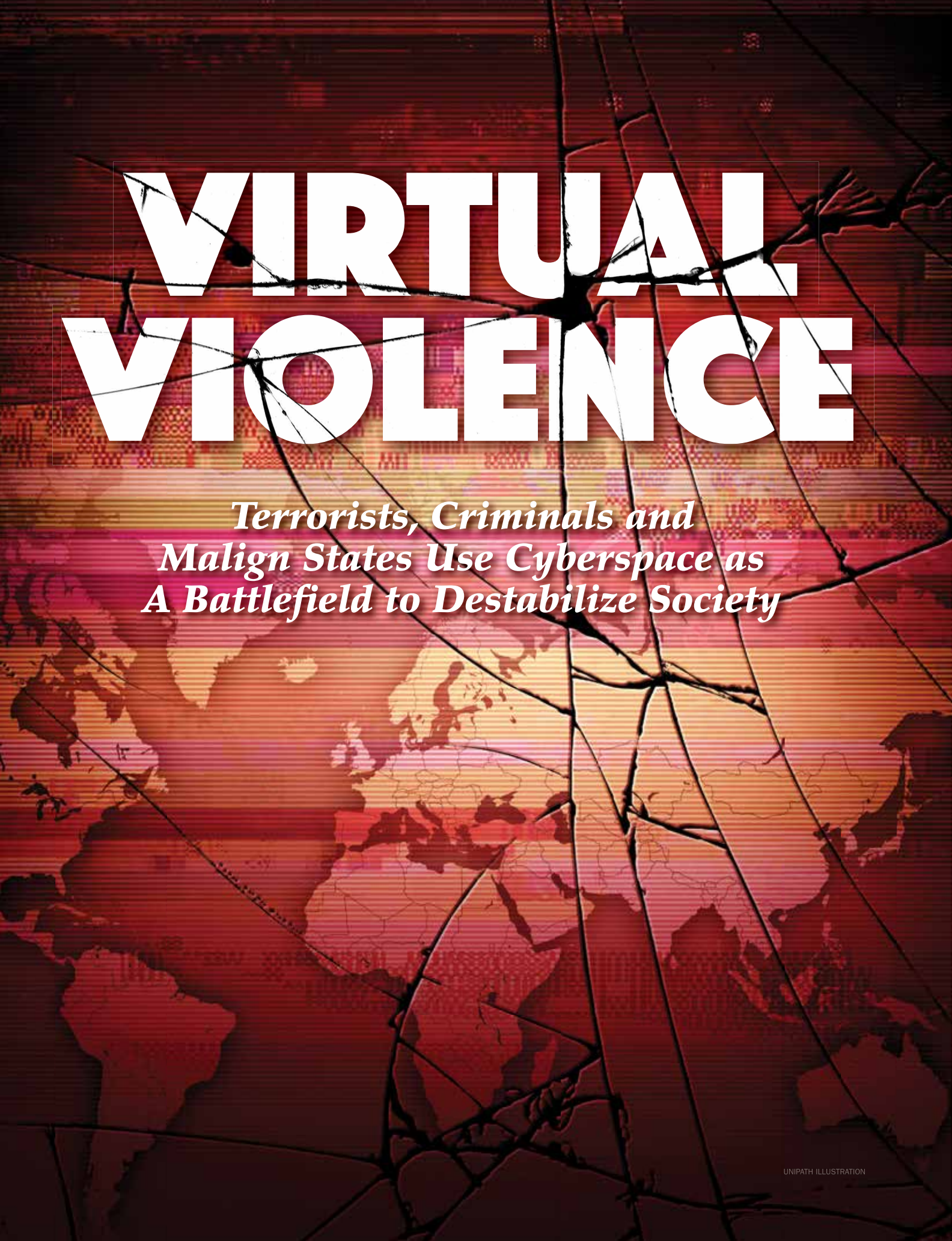
In November 2021, USCYBERCOM hosted its largest combined and multinational cyber exercise to date, Cyber Flag 21-1. This series of exercises tests and enhances the defensive skills and capabilities of more than 200 cyber warriors from 23 countries by exposing them to a challenging cyberspace scenario. With these exercises, we are honing the coalition qualities necessary — speed, precision, agility and unity of effort — to defend our nations collectively.

Adequate defense in cyberspace also requires a close partnership with private industry. USCYBERCOM interacts with private industry through two primary programs: Under Advisement and Dreamport. Under Advisement is an overt, voluntary and mutually beneficial private sector information sharing program. Dreamport is an unclassified innovation center that allows USCYBERCOM to interact with members of industry and academia to share ideas and provide innovative solutions to cybersecurity problems. Both programs directly contribute to USCYBERCOM's ability to defend our nation in cyberspace and continue to grow in scope and scale.

Dreamport is just one of the ways USCYBERCOM capitalizes on our partnerships with academia. The command recently established a formal Academic Engagement Network with 91 institutions. The network will enable collaboration on innovative solutions to technical challenges and new analytic insights about malicious cyber actors, supporting our collective defense efforts. The network will also improve workforce recruiting by highlighting opportunities for students to serve in exciting military and civilian cybersecurity careers.

Ultimately, the ability to defend the U.S. Department of Defense's networks and our nation as a whole against malicious cyber actors requires a collective approach. This collective approach requires close partnerships among governmental agencies, our allies, industry and academia.

Our ability to share information seamlessly and rapidly, persistently train and conduct operations together, and develop innovative approaches to all our cybersecurity challenges is vital to our ability to successfully execute our mission of cybersecurity and defense in the 21st century. ✦



VIRTUAL VIOLENCE

Terrorists, Criminals and Malign States Use Cyberspace as A Battlefield to Destabilize Society

UNIPATH ILLUSTRATION

The internet is globally decentralized, which allows for anonymity and contributes to its use as a platform for illegal activities, including property crimes and the promotion of violent extremism. Against such a backdrop of susceptibility — the exploitation of the internet by extremists and terrorists — governments face a challenge to contain these criminals who seek to undermine the legitimacy of the state and commit acts of violence.

Cyber terrorism is the No. 1 national threat to many governments; it brings about enormous damage because of the global dependence on information technology. The main targets of cyber terrorism may be governments and associated institutions, banks, communications infrastructure, and public utilities such as water, electricity, oil and gas. Attacks on these can cause great economic, political and physical damage.

Cyber-terrorist groups have become more cunning and coordinated. They can take advantage of any computers connected to the internet to support any attack. As such, cyber terrorism has become a threat to large organizations and all citizens who use computers.

Cyber operations attract terrorists for several reasons. They are less expensive than traditional terrorist methods, requiring little more than a personal computer and an internet connection. There is no need to buy weapons and explosives. The creation and transmission of computer viruses by traditional telephone lines or wireless communication is one of the most common electronic terrorist methods, and it can cripple systems as effectively as physical bombs.

The definition of a cyber weapon is still couched in ambiguity. It occupies a murky area of programming codes used for malicious purposes. In distinguishing between a weapon and a tool, one must consider the intent of the offender, which is to cause harm through destruction or intimidation. This is an integral part of the definition of a cyber weapon.

For instance, a hammer is a tool used for various purposes. If it is used to cause bodily or material harm, a hammer becomes a dangerous weapon. This logic can also apply to the use of software that, though harmless in certain applications, becomes a destructive weapon when misused.

The extent to which a cyber weapon causes damage depends on the population's dependence on the targeted network. Thus, the effects of cyber weapons targeting critical infrastructure such as electrical networks are more severe.

There is a constant risk that terrorist organizations will acquire such weapons. For instance, a group known as Shadow Broker hacked the U.S. National Security Agency and claimed to have stolen national cyber weapons with the intent of auctioning them off. That suggests that cyber weapons may be traded like conventional weapons by virtual "arms dealers."

Malware software programs are an overarching term for any type of software designed to harm or exploit a programmable device, service or network. They are commonly used by cybercriminals to extract data for financial gain. Targeted data includes financial and heath records, email messages and personal passwords. The types of information subject to hacking is endless.

TYPE OF ATTACKS

The use of a zero-day exploit — finding a computer software vulnerability for which a patch has not been developed — is one of the most devious ways to access and harm a system. This vulnerability can be exploited by hackers to access restricted information, in addition to creating and using malware and spyware.

Distributed denial-of-service attacks, data theft and other intrusions can be performed by a botnet. Botnets or bots are several devices connected to the internet; each device runs one or more bots. An attacker can control the robots using command and control software.

Viruses are the most notorious and oldest types of malware program. They are programs attached to computers or files that multiply to infect other files or computers and can destroy or delete data. A computer may not be infected unless the compromised program is run, and the virus may lie dormant until the infected file or attachment is opened. Viruses require the user's input to circulate and infect other files and systems, such as running an infected program in a mailing list.

THE ASSOCIATED PRESS

Identifying Extremist Platforms on Social Media

ISLAMIC MILITARY COUNTER TERRORISM COALITION

Online social networks have become dominant agents of communication: Facebook boasts many billions of users, YouTube 2.2 billion users, WhatsApp 2 billion users, Messenger 1.3 billion users, and Instagram 1.2 billion. Each month, nearly 4 billion engage on such platforms.

The use of social networking continues to snowball rapidly and is a favored recruitment method of violent extremists. Governments interested in countering terrorism ignore social networks at their peril. They must employ emerging technologies like artificial intelligence (AI) to counter these ideological extremists lurking online.

TERRORISM AND SOCIAL NETWORKS

Former British Home Secretary Amber Rudd describes combating online extremist content as an arms race between extremists and law enforcement agencies. Rudd revealed that as of November 2017, violent extremists established about 40,000 new websites and applications. Like any arms race, this requires state-of-the-art technologies. Enter a new technology called Conversation AI.

Conversation AI is a research project that aims to detect online extremist content and remove as much as possible. Of note, the use of machine learning in achieving such goals has significantly contributed to reducing such content.

The technology giants, led by Microsoft, Google, Facebook, Amazon and Twitter, have announced support for an international initiative known as Christchurch Call that advocates fighting online extremist content. These companies display complete commitment to constantly updating their terms of use and making available various methods of reporting extremist content and investing in monitoring technologies.

The United Nations Counter-Terrorism Committee Executive Directorate launched the Counter-Terrorism Technology initiative, which actively monitors more than 500 extremist channels over more than 20 content platforms and messaging applications.

Terrorist organizations use social networking for different purposes. They raise money, strengthen collective identity and combine efforts. Such groups have employed these networks to achieve a set of goals, such as coordination, recruiting followers and spreading ideologies, using such networks as a virtual training ground while obtaining financial and moral support.

ARTIFICIAL INTELLIGENCE

AI techniques have become the most prominent emerging technologies in combating online extremist content. About 99% of the content of al-Qaida and ISIS that was removed from Facebook was detected by AI systems before it was detected by people, according to Facebook.

This has made AI the best counterterrorism weapon in the world of big data in its automatic ability to detect extremist and terrorist content, individuals with extremist and terrorist susceptibility, and extremist virtual communities. AI helps anticipate, prevent and mitigate future terrorist risks.

Beyond a shadow of a doubt, the use of AI counterterrorism programs produces accurate predictions that lead to the reduction of unnecessary actions applied to large numbers of the population and reduces human bias in decision-making. AI directs its attention with greater precision, reducing the number of citizens subject to further monitoring.

AI predictive counterterrorism capabilities have been confirmed. Security and intelligence services use automated data analytics to assess the risks of air travel and reveal links between terrorist organizations and their associates. Some technology companies use advanced predictive measures to monitor and disrupt terrorist activities on social media platforms as well as using AI in the financial services sector to report suspicious money transfers.

AI is also used to analyze social networks, identify suspects and their online relationships, classify them as per characteristics, analyze their communication relationship, and detect extremist susceptibility in virtual communities. Through the SKYNET software program used by the U.S. National Security Agency, which includes an AI-based algorithm, about 15,000 out of 55 million domestic mobile phone users were identified as potential terrorists.

Facebook has improved its AI policies to combat extremist content; the company has reduced to 12 seconds the average time to identify videos that violate Facebook's terms of use in a live broadcast.

Another technique for weeding out radical content is natural language processing technologies, which potentially raises the efficiency of combating online extremist content, said Dr. Majdal bin Sultan bin Safran, professor of AI at the University of King Saud.

Such technologies help us to train devices to understand our communication with them and discover information in exceptionally large text groups without human intervention to discover the different linguistic patterns enlisted by extremists and terrorists.

AI CHALLENGES

Despite progress made by AI technologies in combating online content of extremism and terrorism, such technologies are still riddled with problems of linguistic content analytics, especially with the spread of hybrid languages such as Franco, colloquial dialects, and the analytics of nonverbal signals and images. This impedes full reliance on digital analytics of exceptionally large and highly developed content, which cannot be monitored by human experiences only.

We have a long way to go to reach models that can capture the true, precise meaning behind language and go beyond memorizing specific words and phrases. We must go a step further to interpret data in context, which has become a key factor in understanding online behavior.

Claudia Wallner, analyst at the Terrorism and Conflict Research Group at the Royal United Services Institute for Defence and Security Studies, is pessimistic about the success of the new European Union strategy to remove terrorist content.

Wallner describes it as having limited feasibility for several reasons, including the ambiguity of extremist or terrorist content due to challenges of legal definitions. Governments offer shifting definitions of violent extremism and terrorism, while national classification lists often include only a small portion of active extremist or terrorist groups.

Detecting extremist content is a gray zone. It's sometimes hard to define what is extremist and what is not. Some content from extremist groups and individuals includes no statement or insinuations supporting hate or violence, but rather employs humor and irony to feed anger and discontent.

Unfortunately, targeting online extremist content causes extremists and terrorists to migrate to large platforms and hide among the millions of sites on these platforms, making it difficult for law enforcement agencies to detect their activities.

Small social networking sites are now more polarized and exploited by al-Qaida, Daesh and other groups because of the limited resources such platforms have to efficiently remove terrorist content.

Terrorists often attack victims using a form of cyber sabotage called logic bombs, which involves inserting software to set off a malicious function when certain conditions are met. Logic bombs can also be used for less harmful reasons such as free trials of programs that are disabled after a predetermined period of usage. Terrorists understand the importance of logic bombs; the infrastructure of most of the world depends on computer networks, and a specific series of logic bomb attacks can disrupt many global banking and transportation systems.

TARGETING INFRASTRUCTURE

Critical infrastructure supports basic services that society needs, such as transportation, food production, energy and health care. Severe disruption of such services can make many people vulnerable. Reliance on electronic logistics supply chains for these services worsens the negative effects of a cyberattack because these services are the backbone of a national economy, especially security, health, energy, water, transportation, freight services, communications, banking and financial services.

Critical infrastructure can be vulnerable to cyber terrorism. The increase in the availability and interdependence of data, combined with the use of industrial control systems, public communications infrastructure and artificial intelligence, requires attention to cybersecurity at the national level. Furthermore, the increase in new electronic-physical systems, such as self-driving cars, creates new vulnerabilities.

The rapid development and interdependence of technologies is also a cause for concern, largely due to the emergence of the Internet of Things, which has created many new attack vectors for cybercriminals and terrorists to exploit.

On April 8, 2020, the Cybersecurity and Infrastructure Security Agency and the National Cyber Security Centre in the United Kingdom issued a warning about security incidents that targeted the vital infrastructure of health care and pharmaceutical agencies. Victims included companies, medical research institutions and universities, and the attacks corresponded to the emergence of the COVID-19 pandemic.

In the United States in February 2021, hackers infiltrated a water plant in a small Florida city to try to raise levels of potentially dangerous chemicals in the water supply. Fortunately, the attack was detected before anyone was hurt.

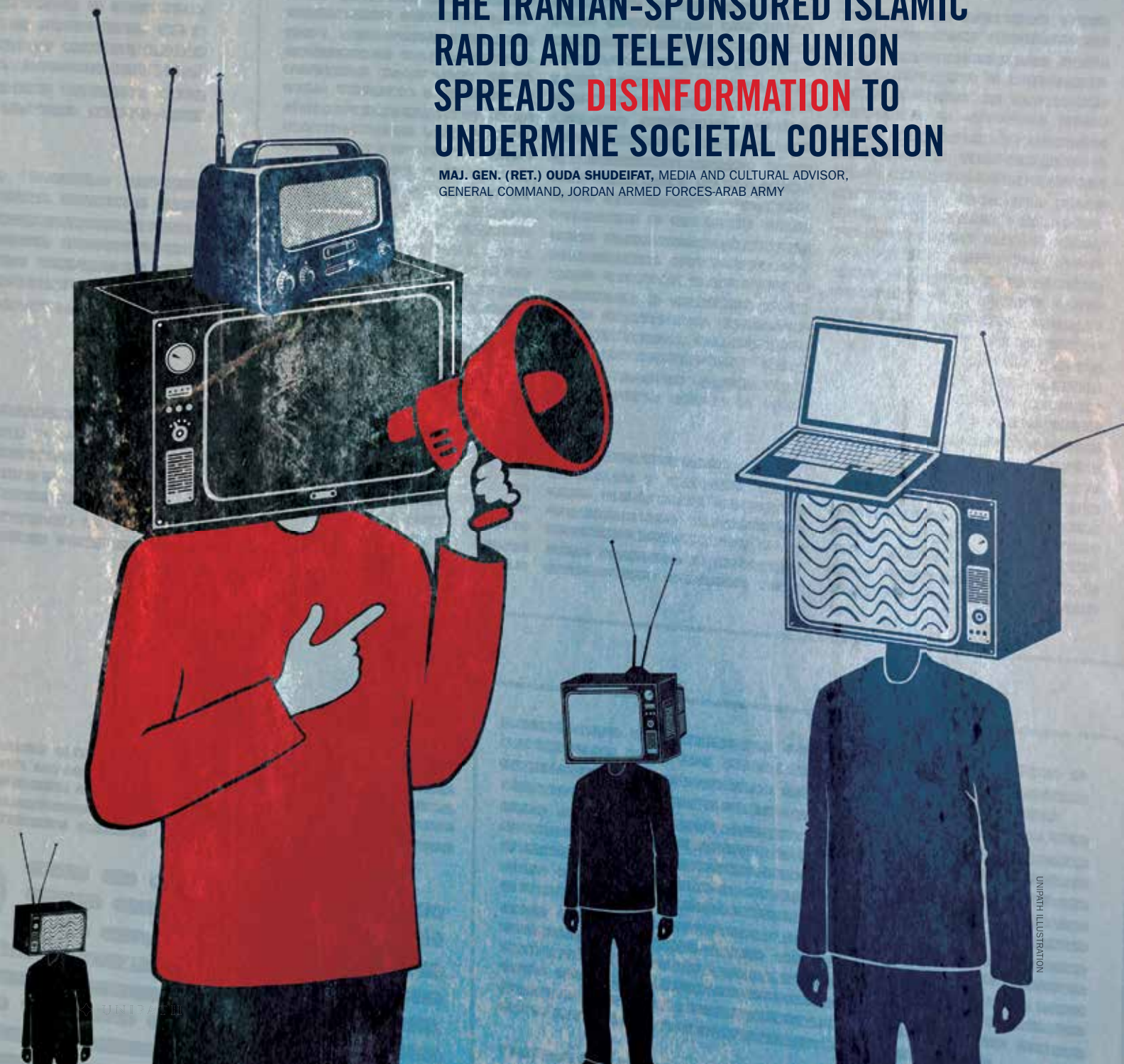
That same month, the U.S. Department of Homeland Security revealed a ransomware attack that targeted the critical infrastructure of a natural gas compression facility. The attacker used spear phishing, a targeted attack designed to trick people into providing sensitive information such as passwords to gain access to the networks of the institution, which resulted in the closure of the facility for two days.

As virtual attacks become more sophisticated, those tasked with defending national security, including the armed forces, cannot let down their guard. Not every destructive assault on national sovereignty requires the use of traditional weapons. ✦

WORDS WIELDED LIKE WEAPONS

THE IRANIAN-SPONSORED ISLAMIC RADIO AND TELEVISION UNION SPREADS DISINFORMATION TO UNDERMINE SOCIETAL COHESION

MAJ. GEN. (RET.) OUDA SHUDEIFAT, MEDIA AND CULTURAL ADVISOR, GENERAL COMMAND, JORDAN ARMED FORCES-ARAB ARMY



UNIPATH ILLUSTRATION

News flows in from far and wide, accompanied by analysis, commentary, communication and dialogue. Based on the convictions, opinions and objectives of the media outlet or guest, programs can strike an accusatory, defensive or neutral pose on issues of the day.

On many broadcasts, the features, emotions and modes of expression shift; patience wears thin and voices rise, perhaps even to the point of shouting and swearing, until the viewer gets confused. It is often difficult to come away from this melange of opinions with something factual and useful. And this scene is repeated whenever the viewer tries to track the news from one outlet to another, usually via satellite channels.

We fully acknowledge that the media, with all its disciplined outlets and content, is essential in modern life, and its role amid the totality of our lives cannot be diminished. With the rapid development of information technology and everything that goes along with it, media content has become available to everyone living in something resembling a global village.

What gives me pause, however, is the presence of an army of satellite channels funded by the Islamic Radio and Television Union that broadcast hateful sectarian programs, disguising the ugliness of armed groups and calling affiliated gangs "holy."

The union operates about 210 media companies in 35 countries, mostly in the Middle East. It encompasses research and survey centers, psychological warfare teams, and news sites. These institutions target a specific segment of society to brainwash people with disinformation that inculcates a sense of injustice and deprivation and push them to rebel against their governments.

In my view, this is a clear act of aggression and a declaration of war against the civil peace of Arab societies. Iran uses these media tentacles as a bargaining chip with the countries of the region and the world, exposing countries to the contagion of war and destruction. International sanctions should be imposed on this entity because it incites violence and terrorism just like the Islamic Revolutionary Guard Corps in Iran and security institutions.

You will often see a specific topic dominate headlines, news talk shows and the like. These days, a person following news networks in the region, and some networks elsewhere in the world, may not find a single news item or report that does not mention Iran and its regime, goals, objectives, influence, weapons and impact on many societies, as well as its misconduct and interference in other countries' domestic and foreign affairs.

Iran even manipulates the future of those societies — the futures of their children, their growing ambitions, and their specific agendas — using all means available. For example, at the level of global concerns, the Iranian nuclear program worries everyone and is a prominent topic, and information on it confronts you morning and evening. This has caused some countries of the region to allocate huge budgets, amounting to $1.5 billion, to deal with the Iranian threat.

Malaysia ceased all relations with Iran and, in an unprecedented move, shut down all forms of cooperation with Iran. Lebanon suffers greatly because of Iranian interference. Likewise, Yemen is experiencing bitter conflict because of similar interference, which is now growing more frequent in Afghanistan. The situation in Iraq and Syria is as bad or worse. Neighboring countries in the Gulf and elsewhere in the region are not exempt from similar Iranian interference that takes different forms by employing warlords, crisis profiteers and promoters of sectarianism.

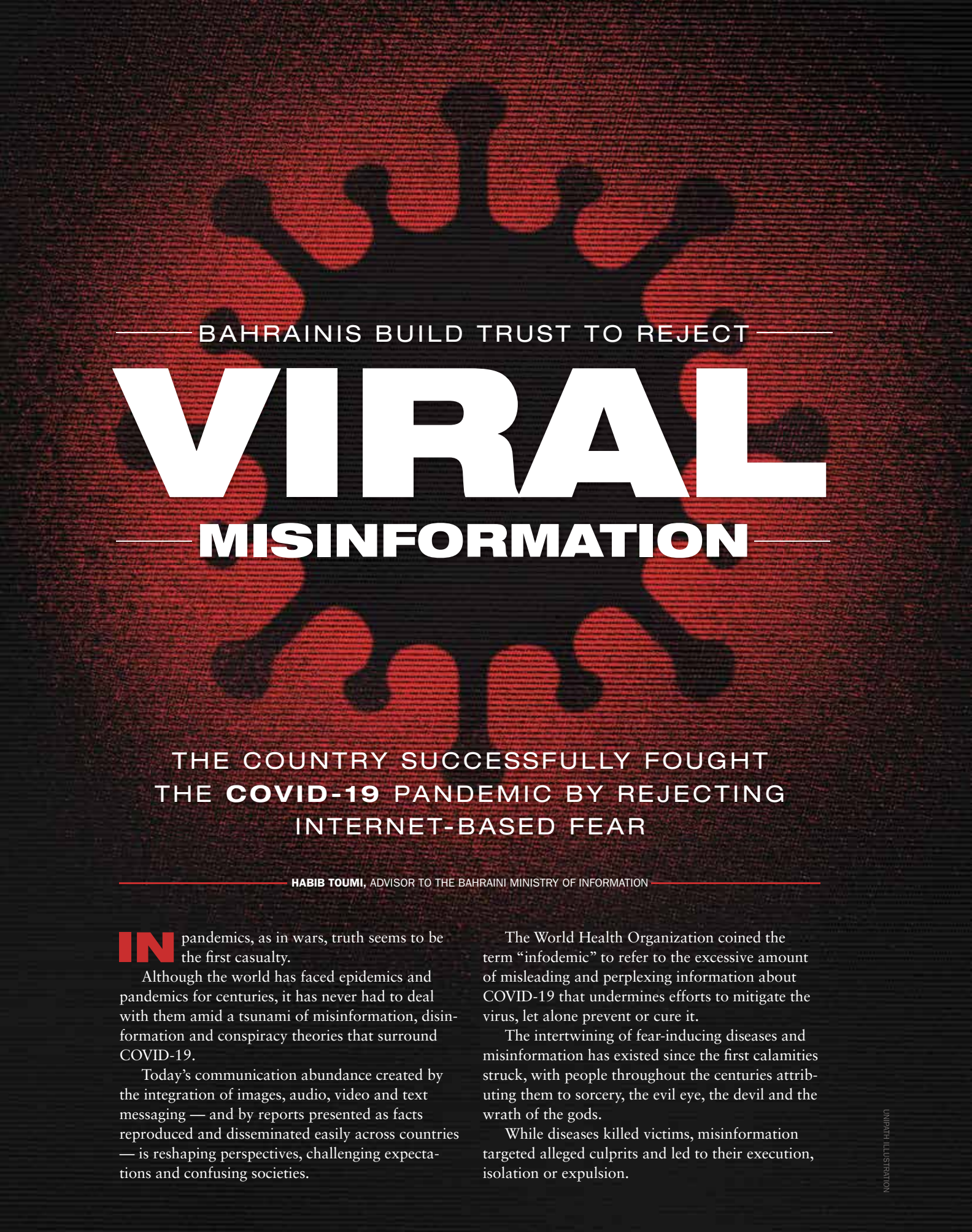
In the face of this intellectual threat — supported by weapons, militias, quick-to-react partisans, media warfare, drug dealers, extremist ideology, and permissiveness toward whatever serves the ideology of a country gripped by religious and national fanaticism — we must not stand by idly. We must maintain the safety and security of our homelands, which are in the eye of the storm of Iranian-backed terrorism.

The U.S. government seized Islamic Radio and Television Union websites used by Iran to promote violent extremism. REUTERS

We need not declare war on Iran to halt its aspirations of expansion at the expense of the countries of the region and investment in terrorist groups. Like others, I view war as a product of a failure to find a political solution to a dilemma. I am calling on us to use soft power while hoping that we will not be forced to defend ourselves. This is the only way to apply the reins to Iran's brutish ambitions. This soft power includes economic and diplomatic pressure.

We should sustain and strengthen regional and international partnerships that will deter those who would violate international law and hide behind proxies and hired guns. Iran continues its efforts to acquire nuclear weapons and represents a danger to the region before it even has acquired them. So what if a country with this sort of illogical conduct were to acquire a weapon of mass destruction?

We must continue to apply pressure to Iran and discourage it from supporting, harboring and training terrorist groups. ✦



BAHRAINIS BUILD TRUST TO REJECT

VIRAL MISINFORMATION

THE COUNTRY SUCCESSFULLY FOUGHT THE **COVID-19** PANDEMIC BY REJECTING INTERNET-BASED FEAR

HABIB TOUMI, ADVISOR TO THE BAHRAINI MINISTRY OF INFORMATION

IN pandemics, as in wars, truth seems to be the first casualty.

Although the world has faced epidemics and pandemics for centuries, it has never had to deal with them amid a tsunami of misinformation, disinformation and conspiracy theories that surround COVID-19.

Today's communication abundance created by the integration of images, audio, video and text messaging — and by reports presented as facts reproduced and disseminated easily across countries — is reshaping perspectives, challenging expectations and confusing societies.

The World Health Organization coined the term "infodemic" to refer to the excessive amount of misleading and perplexing information about COVID-19 that undermines efforts to mitigate the virus, let alone prevent or cure it.

The intertwining of fear-inducing diseases and misinformation has existed since the first calamities struck, with people throughout the centuries attributing them to sorcery, the evil eye, the devil and the wrath of the gods.

While diseases killed victims, misinformation targeted alleged culprits and led to their execution, isolation or expulsion.

UNIPATH ILLUSTRATION

Tailored accusations concocted for political, economic or social reasons have targeted Jews, Christians, Muslims, women, Africans, Asians, minorities, lepers, paupers, vagabonds and foreigners. Schemers adopting these stories, allegations and rumors never seem to lack for disinformation.

Regardless of the historical era, the aims of misinformation and disinformation have remained the same; only the narratives were updated to reflect the specifics of the latest outbreak.

In his 2014 book "An Epidemic of Rumors," author Jon D. Lee wrote that "narratives are recycled from one outbreak to the next, modified not in their themes but in the specific details necessary to link the narratives to current situations."

Some of the doctored pictures and false narratives are driven by malice that revels in crises, fear and anxiety, while others are stimulated by a distorted sense of play and an aberrant idea of fun.

Technology has made twisting facts and inventing stories simple and effective. Applications have empowered people to create a fictional world that is replacing the real world and superseding facts. The exponential leap in technology, presumably to make the world a better place, is instead being used abusively.

In the first days of 2020, as the world was becoming aware of COVID-19, people were bombarded with messages from their inner networks — relatives, friends, colleagues, neighbors — and outside information from doctors, health experts, celebrities, officials and political figures.

Leaders of most countries realized that a significant component of the strategy to fight the rampant disease was to counter the avalanche of misinformation that could undermine the chances of mitigating it until a vaccine was created.

Bahrain, a small island (765 square kilometers) and one of the most densely populated in the world (about 2,052 people per square kilometer), was among the countries at high risk for contagion. Yet the "contagion" through the internet and social media could also be ominous.

According to DataReportal, internet penetration in Bahrain stood at 99% and social media penetration at 84% in January 2020. At the same time the country had 1.65 million internet users and 1.4 million social media users.

The multiministry national task force set up in early February 2020 to deal with the spread and fallout of COVID-19 included a major media component.

While officials were fighting the pandemic, the government also committed to battling misinformation and disinformation that took advantage of the local addiction to digital platforms to undermine state efforts.

People wait to receive COVID-19 vaccines at Manama's Sitra Mall. Despite Bahrain's efficient response to the viral outbreak, bad actors spread disinformation about the pandemic in the country. REUTERS

The task force urged people to use trusted sources of information and not fall for the erroneous and misleading claims disseminated by fame-seekers, conspiracy theorists and blowhards.

The task force set up a hotline to ensure smooth communication in seven languages; more than half the 1.7 million inhabitants of Bahrain are from more than 140 countries.

Bahrain has four daily newspapers in Arabic, two in English, one in Malayalam (India) and one in Tagalog (Philippines). Weekly and monthly magazines appear in several languages, as do radio and television programs.

They all appreciated the gravity of the situation and remained committed to printing and broadcasting news and reports only from trusted sources — official figures, statements from experts and police officers, and announcements by ministries.

The media invariably refused to tolerate doubtful claims and often sent reporters to talk to doctors, mainly infectious and internal disease consultants and microbiologists, who provided scientific explanations to help people understand the situation. This helped tremendously in denying misinformation.

Religious figures in their sermons and speeches equated propagating lies with violating the teachings and values of religion.

The security and justice authorities also regularly issued warnings that people who spread false information would be charged with disrupting social peace and would face legal action that included prison terms and heavy fines.

The task force held regular media conferences to give updates, issue clarifications, and call for a deep sense of responsibility while reminding everyone of the negative effects of rumors and allegations.

The high adult literacy rate (97.5% in 2018) and the "BeAware" campaign were significant in building trust between the people and the state and private institutions, which helped staunch the dissemination of conspiracy theories that usually occurs across the Middle East.

The overall resistance in Bahrain to misinformation and disinformation resulted from a combination of prompt action by the task force, stern warnings against abusers, and open communication with medical experts and committed journalists.

The bulk of the misinformation and disinformation messages reached people in Bahrain through WhatsApp, the most commonly used application for communication in the country.

The messages were mostly not tied to politics or to religious or sectarian agendas that have unfortunately dominated the Middle East because of rivalries between sects and states.

The most unsettling messages emerged February 26, two days after the first infection was detected in a Bahraini citizen who had returned from a religious trip to Iran. WhatsApp messages criticized Bahrainis who traveled to Iran, accusing them of importing the disease and putting Bahrain at risk. According to the police, 30 accounts carried messages with sectarian overtones.

However, swift intervention by His Royal Highness Crown Prince Salman bin Hamad Al Khalifa helped defuse growing fear-driven tension. He called for preserving national unity and stressed that "COVID-19 does not discriminate based on race, ethnicity, religion or social class."

His Royal Highness Crown Prince Salman bin Hamad Al Khalifa, prime minister of Bahrain, receives a booster shot against COVID. BAHRAIN MINISTRY OF INFORMATION

Bahrain enlisted public figures to coordinate its response to the COVID-19 crisis. REUTERS

Bahrainis greet Saudi visitors after the country opened its border in 2021 to people vaccinated against COVID-19.
REUTERS

Other disinformation attempts tried to deceive users or influence behavior. Examples include:

- Social media carried a report that COVID-19 cases were detected at Dragon City, a massive China-themed shopping complex, and that police had raided shops and stores selling accessories, home decor and food.
- In another case, social media circulated the claim that people with COVID-19 had escaped from quarantine centers and were roaming the country. The police promptly denied both claims.
- A user was held by the police after he posted allegations that COVID-19 was a big lie used to take people's money.
- A well-known singer ended up in legal trouble after she used WhatsApp to warn people about pizza and food deliveries to homes, claiming they were dangerously infectious.
- A claim that several prisoners were infected was denied by the National Institution for Human Rights in a report drafted after a field visit.
- Other disinformation attempts that circulated in the country referred to "credible" or "secret" reports about the origin of the virus and ways to treat it.

Today, two years after the outbreak, Bahrain topped the world on the Nikkei's COVID-19 Recovery Index for November 2021. The kingdom has continued to make great strides in confronting the pandemic and returning to normal life.

The index, first published in July 2021, assesses COVID recovery in 121 countries and regions based on nine factors divided into three categories: infection management, vaccine rollouts and mobility.

Infection management includes confirmed cases of COVID-19 versus peak case count, confirmed cases per capita and tests per case.

Vaccine rollouts cover total vaccine doses given per capita, new vaccine doses given per capita, and the share of people fully vaccinated.

Mobility deals with community mobility, the Oxford stringency index, and flight activities.

The higher the ranking, from 0 to 90, the closer a country is to recovery with low infections, higher inoculation rates and less-strict social distancing measures.

Bahrain scored 73%, followed by Kuwait at 72% and the United Arab Emirates at 70.5%.

In November 2021, Bahrain's health regulatory authority said it approved the emergency use of the Pfizer-BioNTech vaccine for children ages 5 to 11. The decision followed an evaluation of Pfizer-BioNTech data carried out by the National Health Regulatory Authority's Clinical Trials Committee and the Ministry of Health's Vaccination Committee. ✦

A COMMITMENT TO CYBERSECURITY

Protecting Iraq Against Cyber Threats Requires Developing Iraqi Talent in Information Technology

DR. HUSSEIN ALLAWI, ADVISOR TO THE IRAQI PRIME MINISTER ON SECURITY SECTOR REFORM

UNIPATH ILLUSTRATION

Cybersecurity is a strategic priority for the government of Iraq. Iraq has established a cyber incident response team (CERT), activated a cybersecurity policy and crafted an electronics crime law extensively debated in the Iraqi parliament.

The main task of the CERT is to combat cyber-attacks in all ministries, work with security and intelligence agencies to monitor hackers and terrorist groups, and pursue organized cybercrime gangs. These precautions are necessary in contemporary societies such as Iraq's that rely increasingly on the internet to transfer money and conduct the business of government.

Cyberattacks are a growing threat in the world, leading to international concern that terrorist groups are appropriating advanced technologies to carry out cyberattacks on vital installations. With that in mind, Iraq launched the Second National Conference on the Development and Building of Security Capacities in Cyberspace in Baghdad in September 2021.

The conference constituted a major shift in the work of the Iraqi CERT. The conference covered issues of concern such as electronic crime, cyber capacities to counter 5G wars, the impact of cybersecurity and modern technologies on national security, and protection of children on the internet. Further topics included the impact of cybersecurity on people in a world besieged by disinformation, digital security for students, and online money laundering and financial transactions.

The conference also included a technical demonstration by the Iraqi CERT, crowned by a security exercise in which the team rapidly intervened to repel a cyber threat.

Atheer Al-Jabber, head of the Iraqi CERT, highlighted the importance of the conference in light of business and government adopting electronic automation because of the COVID-19 pandemic.

"On the occasion of the sessions of this conference, we achieve another step toward the success of providing services in cyberspace," Al-Jabber said.

Exchanging technical expertise acquired by friendly countries when repelling a cyberattack or rehabilitating networks after a breach of the security system is considered the backbone of cybersecurity. Iraq is benefiting from the experiences of friendly countries in the technological field and is working to develop and build security capabilities in cyberspace.

On the other hand, Iraq is keen to share information it has learned regarding how terrorists abuse cyber technology to communicate, encrypt and plan attacks. Because terrorist groups and organized crime gangs share ideas and technologies, the international community must work together to thwart attackers' malicious plans.

The foundation of cybersecurity is the creation of an advanced technology sector with the resourcefulness to repel sophisticated cyberattacks. Iraq must continuously review national policies on cybersecurity and strengthen its capabilities. The Iraqi government is working to attract dynamic individuals in the security and civil services to develop Iraq's potential in cybersecurity and cooperation involving the government sector, the private sector and international companies.

Iraq would like to nurture a unified culture to confront cyber threats, reduce incidents of information hacking and dumping, stop the spread of disinformation that threatens civil peace, and reduce cybercrime employed by the unscrupulous against internet users.

The public-private partnership involving cybersecurity is a strategic necessity. Sectors such as health, education and energy increasingly rely on cyber connectivity to conduct their business. For this reason, the Iraqi government and the CERT team are keen to create new information technology solutions.

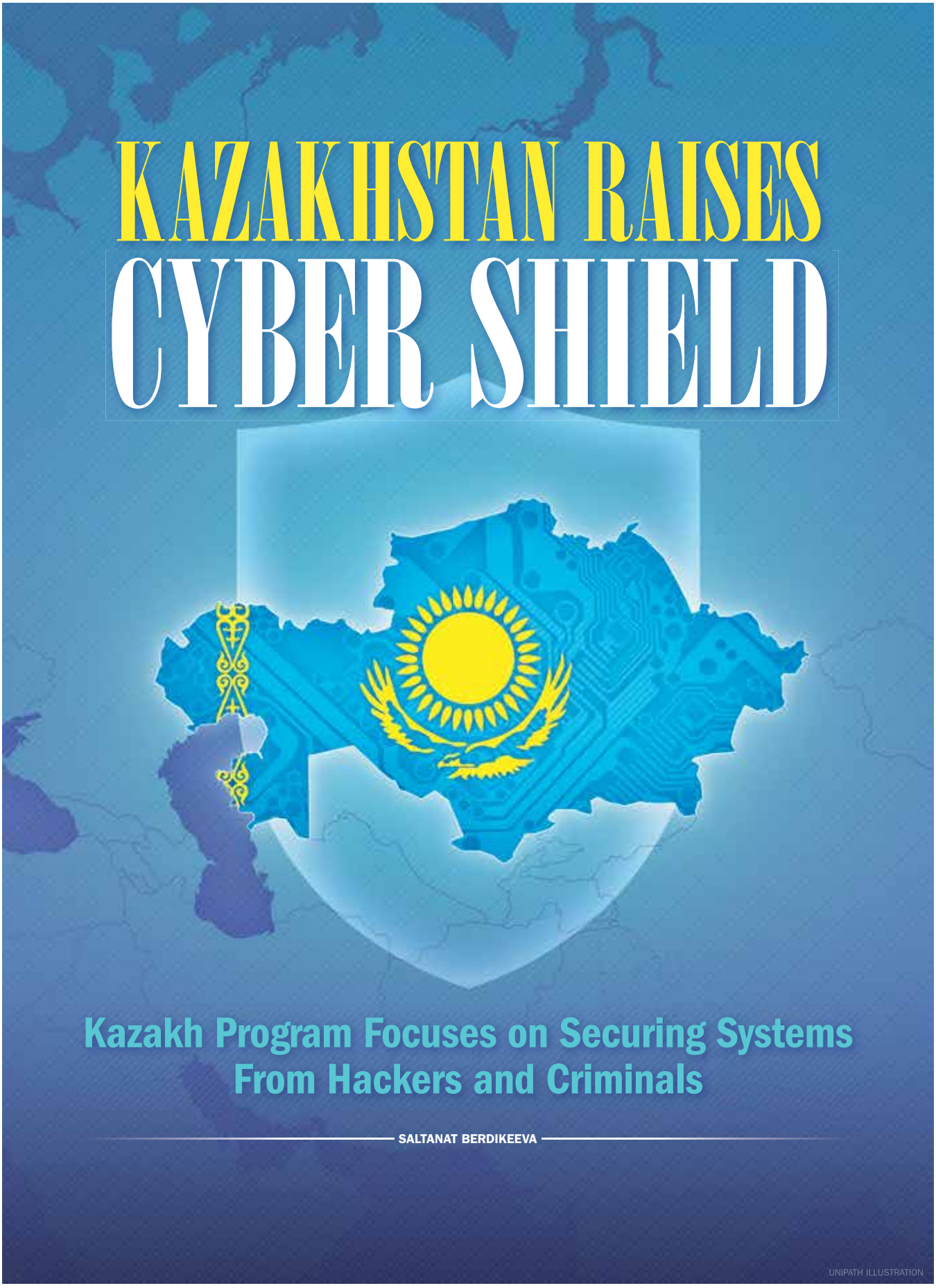
Iraq would like to nurture a unified culture to confront cyber threats, reduce incidents of information hacking and dumping, stop the spread of disinformation that threatens civil peace, and reduce cybercrime employed by the unscrupulous against internet users.

Government ministries use financial incentives to encourage entrepreneurs in information technology and cybersecurity. Iraq must also focus on preparing women to make greater contributions to this important field. They are the future force of our prosperous society, which is facing many challenges. Empowering women is an essential part of the Iraqi government's program and philosophy of work. The role of women in developed countries is prominent in the technical field, and technological progress has come about at the hands of women working at sensitive sites in social media, the software industry and e-marketing.

Today we must support significant growth in business, e-commerce, and information technology investment in every part of Iraq by developing legislation, public policies and the capability to accommodate cybersecurity requirements. We must support the Iraqi government's plans to build partnerships between Iraq and the international business community by providing a suitable environment for the growth of information technology companies with the aim of serving society and modernizing its capabilities.

Fortunately, the Iraqi government's success in supporting the Independent High Electoral Commission for free and fair elections and the commission's ability to counter cyberattacks during parliamentary elections on October 10, 2021, sent a major message about Iraq's improved capabilities in countering cyberattacks and reinforcing cybersecurity. ✦

KAZAKHSTAN RAISES CYBER SHIELD



Kazakh Program Focuses on Securing Systems From Hackers and Criminals

SALTANAT BERDIKEEVA

UNIPATH ILLUSTRATION

Kazakhstan's transformation into a digitally advanced country requires a focus on cybersecurity. Here's a view of the capital Astana, a center of technological innovation.
THE ASSOCIATED PRESS

More than 85% of Kazakhstan's population uses the internet, the highest rate in Central Asia. Major areas of the country's economy and the government have become fully digitized. In 2018, the Kazakh government launched the Digital Kazakhstan program, which has encouraged government agencies and businesses to shift from brick and mortar to online access for more efficient customer service.

But with Kazakhstan's massive transition to digital economy, cybersecurity has grown more urgent, particularly since the onset of the COVID-19 pandemic that forced many people to work and study remotely.

This has inspired Kazakh authorities to advance serious measures to counter cyber threats. While there is no shortage of challenges to addressing cybercrime, which is increasing in intensity, scope and sophistication, the results of Kazakhstan's efforts to fight cybercrime and threats in recent years have been significant.

Thanks to recent improvements in cybersecurity, Kazakhstan ranked 31st out of 182 countries in terms of commitment to cybersecurity in the 2020 Global Cybersecurity Index, issued by the International Telecommunication Union, an information and communication technologies initiative of the United Nations.

The five main pillars of the index are legal, technical, organizational, capacity development and cooperative measures. The 2020 ranking was a significant improvement from Kazakhstan's previous standing of 83rd place in the 2017 Global Cybersecurity Index.

INSTALLING CYBER SHIELD

Kazakhstan's cybersecurity policy stems from the "Cyber Shield" program rolled out by then-President Nursultan Nazarbayev in 2013. He stressed that developing a cybersecurity strategy was in the national security interests of Kazakhstan, citing the ability of criminals to shut down infrastructure like power plants and trains.

"In today's world, it is not necessary to fight using an aircraft or a tank," Nazarbayev said in 2017.

That year, Kazakhstan developed state policies on how to prevent, mitigate and fight cyberattacks and hybrid warfare and improve legal processes to do so effectively. Kazakh authorities consulted international experts and adopted best practices in cybersecurity to put together the concept. The first stage of the Cyber Shield program ran from 2017 until 2018, and the second is to last from 2019 to 2022. So far, the program has cost 28 billion Kazakh tenge (about $66 million).

The country's Ministry of Digital Development, Innovations and Aerospace became the main government agency responsible for implementing the Cyber Shield action plan along with the State Technical Service Joint Stock Co., which is now part of the Kazakh Ministry of Investments and Development.

Cyber Shield defines how state policy protecting electronic information resources, information systems, and telecommunication networks and ensuring safe use of information and communication technologies should be implemented. The concept helped unify the previous

Adoption of digital technology among Kazakhs has prompted the government to increase its focus on cybersecurity.

AFP/GETTY IMAGES

makeshift approaches to cybersecurity. Cyber Shield also advocated developing rapid response mechanisms to prevent information security incidents, including during emergency situations.

CRIMINALS TARGET KAZAKHSTAN

In the spring of 2021, a United Kingdom-based technology review and consumer website Comparitech issued a report that ranked the most and least cyber-safe countries in the world. According to the report, Central Asian countries, including Kazakhstan, were ranked near the bottom.

Kazakhstan is one of the most appealing countries for so-called cryptojackers, who create digital currency, or cryptocurrency, by gaining access to vulnerable computers. This process is known as mining cryptocurrency, or cryptomining. Without getting permission of owners of computers, cryptojackers avoid paying for massive amounts of electricity needed for cryptomining. Kazakhstan is an attractive country for cryptomining due to low electricity prices and less secure computers compared to other countries in the world.

One of the main reasons of why computers in Kazakhstan are less secure is that nearly 74% of software installed in computers in Kazakhstan was unlicensed, or downloaded from illegal sources, according to a 2019 meeting of the Kazakh working group on computer software.

Unlicensed software may carry malware that can jeopardize a user's data, and it is difficult to download security updates for such a software to prevent cyberattacks. As a result, computers running on pirated software are extremely vulnerable to hacking, cryptomining, theft of confidential information, fraud and other forms of cybercrime.

"The number of cyber threats to electronic systems of [Kazakh] government agencies are doubling every year," according to a 2017 statement by Ruslan Abdikalikov, chairman of the Information Security Committee of the former Ministry of Defense and Aerospace Industry.

Kazakhstan's national Computer Emergency Response Team, known as KZ-CERT, registered 11,432 cybercrime and information security threats in the first half of 2021, a 15% increase from 2020. According to KZ-CERT, botnets, Trojan horses and computer viruses are some of the most common malicious software used by cybercriminals to attack computers in Kazakhstan.

Cyberattacks on WordPress content management modules (software used to build websites and create content published on the internet), which are commonly used in Kazakhstan, have cost many website users confidential and sensitive information and defaced sites with terrorist and extremist propaganda messages.

Cybercriminals regularly target Kazakh businesses, government agencies and individuals for profit. In August 2021, every bank in Kazakhstan failed to demonstrate the capability to protect their web-based resources, including security of their content, data transmission, traffic encryption and security settings, against cyberattacks.

BLUNTING CYBERATTACKS

Weak cyber defense of Kazakh banks is particularly concerning, given that cyberattacks against major international banks take place every second, according to General Director of Citibank in Kazakhstan Andrey Kurilin.

Nevertheless, since the establishment of the Cyber Shield concept in 2017, the Kazakh government's increased monitoring and proactive responses to secure the country's cyberspace have significantly lowered cyber threats. By 2019, the Ministry of Digital Development, Innovations and Aerospace had sufficient knowledge about sources and timing of cyberattacks against Kazakhstan. The ministry has helped reduce the number of website defacements and infected software in the country.

Thanks to Cyber Shield, more than 300 critical infrastructure sectors, including banks, government agencies, businesses and manufacturing, improved their security systems. The State Technical Service of Kazakhstan has built enough capability to deter and prevent nearly 1 million cyberattacks a day.

In 2018, the National Security Committee of Kazakhstan established the National Information Security Coordination Center (NISCC), designed to protect information resources of state agencies and critical information infrastructure of Kazakhstan from cyberattacks. In 2020, the NISCC provided 17 government agencies with antivirus protection and monitoring of their information systems for cyber incidents and threats.

One of the key parts of the Cyber Shield is training cybersecurity specialists and educating the public about

Kazakh authorities note that the public remains largely uninformed about basic cybersecurity threats, such as risks from unintentionally downloading malicious software that can lead to phishing and online fraud.

Residents of Kazakhstan, like this man at a polling station in 2019, increasingly rely on smartphone technology, raising concerns about cybersecurity. AFP/GETTY IMAGES

information security. Because of a shortage of trained information technology professionals in Kazakhstan, the authorities have been eager to provide cyber-focused scholarships to university students. The Ministry of Digital Development, Innovations and Aerospace has been tasked with arranging training and educational campaigns about cybersecurity for the general population.

As part of the Cyber Shield action plan, the Kazakh government introduced voluntary cyber insurance for the first time in Kazakh history, which authorizes financial compensation for property damage to a legal entity from a cyberattack or data leak.

IMPORTANCE OF EDUCATION

The state realizes that the rapid transition of the country to a digital economy and governance requires greater engagement and education of the public about computer security to reduce cyberattacks and related damage. Kazakh authorities note that the public remains largely uninformed about basic cybersecurity threats, such as risks from unintentionally downloading malicious software that can lead to phishing and online fraud.

Moreover, many small and medium-size businesses in the country lack basic knowledge about protecting information and communication technologies.

Therefore, the state now emphasizes improving public awareness and holding educational campaigns to ensure that people have basic tools to protect computers and communication technologies. According to a recent survey, such efforts have been effective in raising public awareness about cybersecurity threats, knowledge of which now reportedly stands at 78%.

Kazakhstan has also been investing in training civil servants about cybersecurity, information and technology legislation, and electronic governance. Since January 5, 2021, the Academy of Public Administration under the President of Kazakhstan has organized online courses to train civil servants on digitalization of government agencies. In 2019, the Ministry of Digital Development, Innovations and Aerospace held free online training courses on cybersecurity for government officials in more than 20 state agencies and 17 local government bodies.

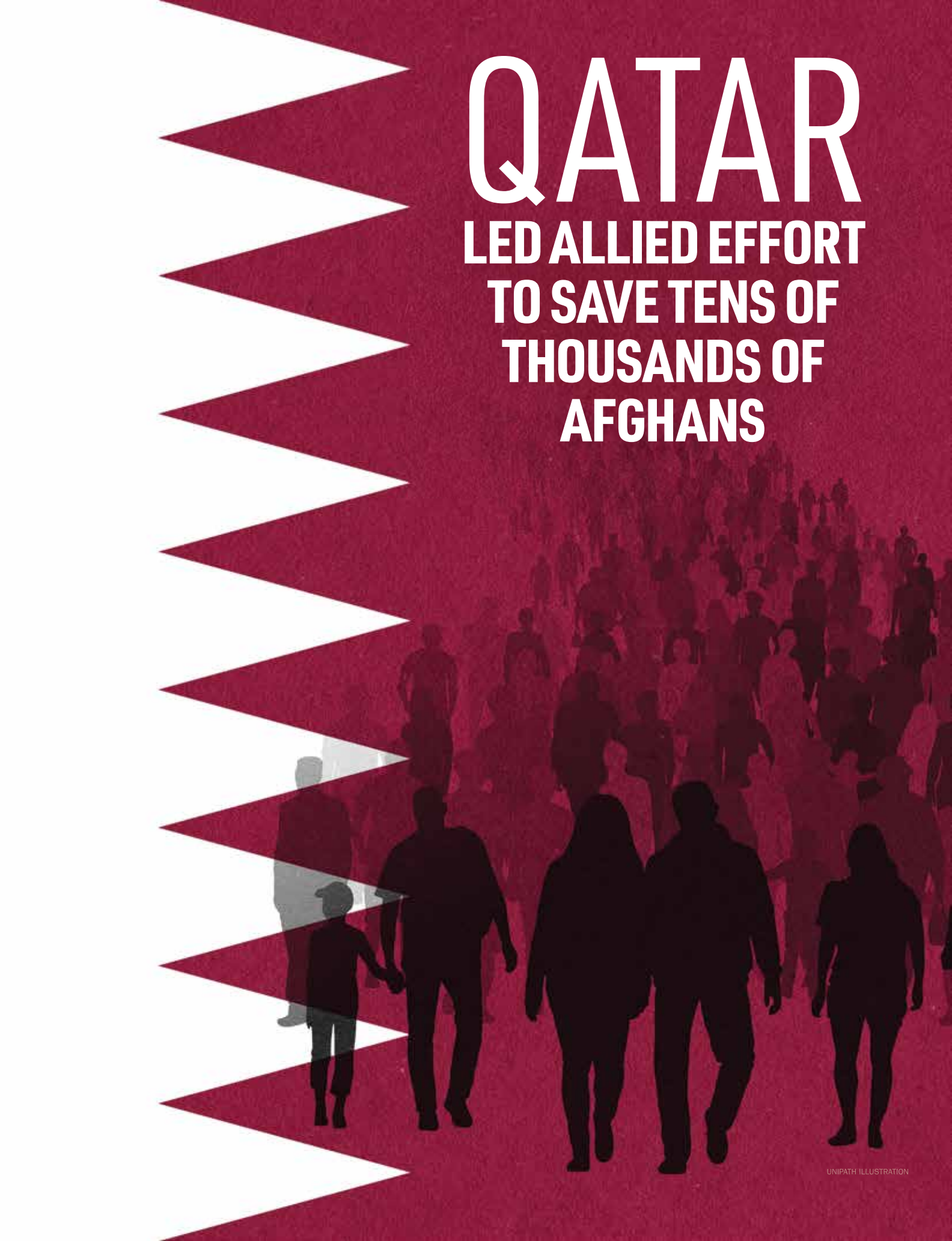
At the start of the global pandemic in 2020, many government workers in Kazakhstan switched to remote offices. To improve digital and communication skills of Kazakh civil servants, the Academy of Public Administration, the United Nations Development Program in Kazakhstan, the Astana Civil Service Hub and the Agency for Civil Service Affairs of Kazakhstan organized large-scale training for government workers in 2020.

In an address to the nation on September 1, 2021, President Kassym-Jomart Tokayev said "all information and technology initiatives of the public sector will be exclusively based on the new platform under the Kazakh state technical supervision. It will eliminate duplication, costs and bureaucracy, and provide public services to citizens from smartphones 100%."

The growing digitalization of government services will continue to require investments in educating civil servants about cybersecurity. President Tokayev's vision of a digital Kazakhstan, where just about all government services will be provided electronically and the private sector will rely on electronic commerce, is inseparable from his commitment to continuous improvement of the country's cybersecurity. ✦

QATAR

LED ALLIED EFFORT TO SAVE TENS OF THOUSANDS OF AFGHANS



UNIPATH ILLUSTRATION

U.S. Central Command's Unipath magazine interviewed Staff Brig. Gen. Abdulaziz Saleh Al Sulaiti, head of Qatari Armed Forces' International Military Cooperation Authority, who is a witness to the Afghani evacuation operation and the heroic humanitarian role of Qatari leaders, based on the directions of His Highness Emir of Qatar Sheikh Tamim bin Hamad Al Thani. Qatar rapidly responded by evacuating and sheltering tens of thousands of Afghans and nationals of other countries forced to leave Afghanistan in an extremely complex security situation in August 2021.

Staff Brig. Gen. Abdulaziz Saleh Al Sulaiti

Unipath: As a leading official in the Afghani evacuation operation, one of the largest logistic operations recently, could you explain how things started and the circumstances and arrangements of the operation?

Brig. Gen. Al Sulaiti: After coalition forces were ordered to withdraw from Afghanistan, there was a state of instability. The evacuation campaign was driven by humanitarian concerns as well as the national, regional and global role of Qatar's political and military leaders, who are part of the international community. It was also coordinated with our strategic ally, the United States. Represented by their prudent leader, His Highness emir of Qatar Sheikh Tamim bin Hamad Al Thani, Qatari authorities responded as the Emir gave directions to provide all forms of support and assistance. This had a positive and rapid impact on carrying out the largest and fastest evacuation operation in modern history.

Unipath: How did you receive directions to start the evacuation operation?

Brig. Gen. Al Sulaiti: We received a request from U.S. Central Command through the Qatari Ministry of Foreign Affairs that a group of people was coming from Afghanistan. We took action in coordination with the ministry. Initially, the request was to evacuate Qatari nationals in Afghanistan, numbering about 8,000 people, over the course of a year. Accordingly, Al Udeid and As Sayliyah camps were prepared, and the working and transportation mechanisms were agreed upon so that all arrivals would have a barcode and a travel permit from Afghanistan. We took COVID-19-related preflight precautions. The operations were highly organized, but orders changed after people indiscriminately climbed onto American aircraft before takeoff from Afghanistan.

Unipath: How did you cooperate with Central Command and respond to its requests?

Brig. Gen. Al Sulaiti: We received direct instructions from the minister of state for defense affairs to fully support the U.S. The operation was not limited to the Armed Forces. It was a unified effort by the Qatari Ministry of Foreign Affairs, the U.S. State Department, the Qatari Armed Forces, the Qatar Fund for Development and the Qatari Ministry of Health. Al-Wakra Hospital, one of the best and largest hospitals in Qatar, was equipped to receive and treat refugee patients.

Unipath: What were the most daunting challenges in the evacuation operation?

Brig. Gen. Al Sulaiti: Transporting patients to other hospitals proved difficult; some patients were either undocumented or without identification, or were in need of amenities. The speed of events prompted challenges, but His Highness Emir of Qatar Sheikh Tamim bin Hamad Al Thani himself ordered that Al-Wakra Hospital be fully allocated to serve refugee patients.

Cots were provided to Afghan refugees at Al Udeid in Qatar. REUTERS

Unipath: There were different paths for the evacuation operations. Could you explain them?

Brig. Gen. Al Sulaiti: We established four paths for evacuation operations. The first was for diplomats, which was easily accomplished because the diplomat would arrive with members of his family; some stayed in the country and others traveled farther. The second path was for journalists, students and individuals from other nations who had asked the Ministry of Foreign Affairs to evacuate certain individuals. This group of refugees was accommodated in camps prepared for them. The third path was for countries such as India and Bangladesh, which asked to evacuate their own nationals though Qatari airports onboard aircraft from those nations.

The fourth path was carried out by Central Command C-17 aircraft. This path was difficult because of the huge numbers of people and the increasing threat around the Kabul airport. What made it more challenging was that the people remaining around the airport suffered from various and intensifying health problems. We saw U.S. Soldiers carrying a number of children, helping them and lowering them over fences. It was a matter of life or death for these children because of the crowding. We did a tremendous job when they arrived, hosting them at the Qatar Orphan Care Center after they were organized based on age. We faced additional challenges in processing passports. These people were arriving in Qatar as a stopover before their final destination, and it was difficult getting them into the country. We were about to host the Arab Cup, a prelude to the World Cup. At the same time, we were surprised by the development and speed of events, especially when some nations refused or delayed hosting these people. In an effort to reduce overcrowding, the Qatar Emiri Air Force's transport component ran several C-17 flights from Al Udeid to military bases operated by the U.S. and its allies.

Unipath: How did you coordinate the mission with Central Command?

Brig. Gen. Al Sulaiti: The initial agreement with Central Command was for 8,000 refugees over 12 months. We were surprised when 16,000 refugees arrived that first week. We had orders from the chief of staff and the defense minister to establish air-conditioned, fully equipped makeshift camps. We raced to complete these camps, being tasked to do this in three days. Over these three days, the number of refugees doubled to 30,000, then 40,000, then 50,000. Our main problem was that their arrival coincided with August, when temperatures rise, and we were keen to provide cool locations. On the other hand, all the groups had to gather in one place to complete the necessary travel requirements correctly and systematically. We even faced challenges on routine matters. For example, crowding made sanitation and other measures difficult, which led to intervention from the Ministry of Municipality. We took all necessary actions

THIS IS THE ROLE OF THE ALLIES IN COOPERATING AND STANDING UP IN CRISES, ESPECIALLY IN HUMANITARIAN CRISES. ***WE ARE PROUD OF WHAT WE ACHIEVED.***

~ STAFF BRIG. GEN. ABDULAZIZ SALEH AL SULAITI

Afghan refugees pose at Al Udeid Air Base after their rescue by the joint efforts of Qatar and the United States. REUTERS

Qatar contributes to the evacuation of Afghan citizens and foreign nationals. DIRECTORATE OF MORAL GUIDANCE

Qatar provides medical care for the Afghan refugees. DIRECTORATE OF MORAL GUIDANCE

and intensified our efforts. As for food, the refugees were provided with ready-to-eat meals and we set up an operations cell within the Al Udeid Airport terminal. The cell was led by former U.S. Chargé d'affaires Ambassador Greta C. Holtz, who came specifically to head the evacuation and shelter mission. On the Qatari side were members of the Ministry of Foreign Affairs; the Armed Forces' International Military Cooperation Authority, Logistics and Medical Services; and the Ministry of Interior, Customs, the Ministry of Health, Ambulance Services and Qatar Charity. We also set up a cell in the rear section exclusively dedicated to the Armed Forces. This cell was led by Mohammed Hamad Al-Nuaimi, head of operations. A team from the Ministry of Health began work to support this cell. As there was a high evacuation demand and limited time, we were surprised the planes were only delivering refugees, and none had been evacuated as had been agreed. The aircraft continued to transport refugees from Kabul to Qatar, multiplying the numbers. We reached a stage at which we received 900 refugees every 90 minutes until midday. The number hit 4,000 per day, and we had to provide means of transport. The airport was not equipped to receive more than 10,000 refugees over five or six hours, and it was difficult to transport this crowd. The runways were full, at times with 40 C-17 planes, in addition to planes from other countries. This required a strong team spirit and high-level coordination. Thankfully, I personally enjoyed this work alongside Lt. Gen. Gregory Guillot, commander of U.S. Air Forces Central Command, and Brig. Gen. Gerald Donohue, commander of the 379th Air Expeditionary Wing. We met at the airport, where we worked together to confront challenges and overcome obstacles. U.S. Soldiers stationed at Al Udeid spared no efforts. For every 3,000 people, there was a U.S. Army colonel appointed with all his officers, working around the clock without stopping alongside members of the Qatari Armed Forces and the Ministry of Foreign Affairs. All these efforts culminated in success. I remember one day Ambassador Holtz said foreign flights would cease and flights would be limited to arrivals from Kabul. She said that after several hours, the number would increase many times over and the preparations would not be enough. She said we would face many challenges and would have the choice to either receive the flights from Kabul or refuse them. This decision had to come from supreme command, so we informed the chief of staff. He contacted the minister and then the supreme command of the state, who decided not to withdraw and we would support our strategic ally, the United States, in receiving the refugees and providing shelter. After the approval, the number of people expected to arrive was 30,000; there were 16,000 refugees already there, so the grand total was 46,000. This number was beyond the capability of the camps, so I contacted Ambassador Essa Al-Mannai, director of the Ministry of Foreign Affairs' American Affairs Department. We decided to provide additional Qatari aircraft to transport refugees.

I asked Ambassador Essa to submit a request to the Ministry of Foreign Affairs. I also contacted the Qatari Armed Forces Chief of Staff Lt. Gen. Ghanem bin Shaheen Al-Ghanem and provided him with details, especially about what the refugees had been through for five to seven days. They had been without shelter and food before their arrival, and the majority were exhausted during rising temperatures, which compounded the fatigue. I submitted a request to use a C-17, although we had a limited number and some had been on other missions. The chief of staff sent the request to Defense Minister Dr. Khalid bin Mohammed Al-Attiyah, who then submitted it to His Highness the Emir. An Emiri grant allocated 10 Qatari civil aircraft to transport the refugees, which was a giant step forward in alleviating the crowding. After transporting the refugees in the first 10 aircraft, we asked for and received 10 more aircraft to transport refugees. In addition, Al-Wakra Hospital was allocated to all personnel and their equipment, which cost the Armed Forces over $35 million.

This is the role of the allies in cooperating and standing up in crises, especially in humanitarian crises. We are proud of what we achieved. We have been allies of the United States for many years. In the 1990s, American forces assembled on the Qatari border and were hosted in camps, which

Qatar set up mobile shower rooms and sinks for Afghan evacuees during their emergency stopover at Al Udeid. REUTERS

subsequently became Al Udeid Air Base. This was, and still is, part of our preparations in support of our ally, the United States. Al Udeid is a prime example. It is a joint base between Qatari and American forces. In recent years, Qatari Armed Forces is increasingly using American weaponry. The partnership between the two nations increased the expertise of our forces, as well as the presence of U.S. forces on our base, which benefits stability in the region. We appreciate every effort made by the U.S. forces.

The development and progress of Al Udeid Air Base is in its preliminary stages. We have a plan for a comprehensive expansion of the area over several stages for both Qatari and U.S. forces (Al Udeid Air Base Development Project).

Unipath: Do you have any closing comments?

Brig. Gen. Al Sulaiti: I would like to commend the team spirit and the positive atmosphere of the evacuation operation. I must thank everyone who helped accomplish this challenging humanitarian mission. All of this would not have been possible without the support of His Highness Emir of Qatar Sheikh Tamim bin Hamad Al Thani, as well as the follow-up of His Excellency Dr. Khaled Bin Muhammad Al-Attiyah, Deputy Prime Minister and Minister of State for Defense Affairs. The operation was also under the direct guidance of then Chief of Staff Lt. Gen. Ghanem bin Shaheen Al-Ghanem, with the support and direct intervention of the Emiri Air Force, led by Lt. Gen. Salem bin Hamad Al-Nabit, the current Chief of Staff of the Qatari Armed Forces. I would like also to thank the main forces, namely the Military Police, Logistics, Operations Authority and Al Udeid Air Base. Special thanks to base commander Brigadier Youssef Shaheen Al-Ateeq, as well as the Intelligence Authority and the International Military Cooperation Authority.

With regard to non-military agencies, we cannot forget the major role of the Ministry of Foreign Affairs. Here, I would like to give special thanks to Her Excellency Lu'lu'a Al-Khater, undersecretary of the Ministry of Foreign Affairs; Essa Muhammad Al-Mannai, director of the Ministry of Foreign Affairs' American Affairs Department; and all members of the Ministry of Foreign Affairs. Special thanks also to the Ministry of Interior, especially His Excellency Maj. Gen. Abdullah Al-Mal and all his staff. Special thanks also to the Customs Authority, the Ministry of Health, the Ministry of Municipality and everyone who contributed to the success of this humanitarian mission. Without divine providence and the support of all those people and agencies, the situation would have been a humanitarian disaster. Thank you very much! May God protect Qatar's leadership, people and government. ✦

UNIPATH ILLUSTRATION

HARDENING MILITARY NETWORKS

Iraq's Ministry of Defense enlists a cybersecurity team to detect and prevent attacks

UNIPATH STAFF

With the rapid development of the internet and mobile phones, technology has become a necessity in people's daily lives. These technologies have improved all sectors of society, including education, medicine, engineering, security and economics. However, organized criminal gangs and terrorists have exploited these technologies, leading countries to form cybersecurity teams to protect networks from cyberattacks. Unipath magazine met Staff Maj. Gen. Raad Shakir al-Kanani, director of the Military Communications Directorate in the Iraqi Ministry of Defense, to discuss the tasks and accomplishments of the ministry's cybersecurity team.

Unipath: *What steps has your directorate taken to secure Iraq against cyberattacks?*

Maj. Gen. Raad: The primary mission of the Military Communications Directorate in the field of cybersecurity is to protect the Iraqi Ministry of Defense systems and networks, in addition to developing specific policies for the use of devices and networks belonging to the ministry and its units. The directorate, therefore, puts information security controls and guidelines in place to safeguard the application of procedures to prevent cyberattacks. We work with the network building and administration department to ensure that secret confidential networks remain closed to the public and are not connected to public networks like the internet, as well as other procedures with the cooperation of the relevant technical directorates. A closed network is one that contains military email, websites and contracts. We also have another online public network that is separate from the closed network. It is managed via the official website of the ministry and engages with the public.

We also conduct awareness training sessions for network users on the dangers of cyber terrorism and the need to comply with the ministry's guidelines so that the network is protected from breaches. In addition, the nonuse of personal USBs in the ministry's devices or CD-ROMs to watch movies or online gaming is emphasized, and loading external programs on the devices is strictly prohibited.

> Cooperation in this field is extremely necessary for national network security and for building good relations with other specialist security agencies, so that information is exchanged and optimal methods are adopted in the face of threats and attacks.

Unipath: *How does the ministry work with other security agencies to promote cybersecurity?*

Maj. Gen. Raad: We maintain direct cooperation with the other security agencies in the cybersecurity field through joint committees such as the Supreme Communications and Information Security Committee and the committee tasked

with formulating national cybersecurity strategy. There are also discussions on cybercrime law and cooperation with the National Computer Incident Response Team. Cooperation in this field is extremely necessary for national network security and for building good relations with other specialist security agencies, so that information is exchanged and optimal methods are adopted in the face of threats and attacks. This is in addition to the work with our friends in the coalition forces through the Joint Operations Command, where cybersecurity intelligence is exchanged, as well as the intelligence gleaned from devices in terrorist hideouts, and from hacking programs and website breaches, which give us the capability to counter terrorist attacks on our sites.

Officers specializing in information security must be assigned within all formations and be trained by the cybersecurity team, and in turn, educate and train Soldiers to follow guidelines.

***Unipath**: What is your role in protecting polling centers from online attacks?*

Maj. Gen. Raad: As a defense ministry, the assigned task is the protection of voting centers from conventional terrorist attacks or riots, and the Military Communications Directorate has not been tasked to protect them from cyberattacks. However, as I mentioned above, we work with other specialist security agencies in the cybersecurity field to protect the national network from external attacks, and we have not been aware of any abnormal breach or activity.

***Unipath**: Is your duty restricted to protecting Ministry of Defense facilities or does it also include other state and private sector installations?*

Maj. Gen. Raad: The Military Communications Directorate's duty is restricted to the protection of Ministry of Defense facilities, in cooperation with the relevant technical directorates. However, it is not possible to separate cybersecurity of the ministry's networks from other state networks; therefore we ensure that no breach of ministry devices occurs, or that the network becomes a bot to attack other sensitive government websites. This requires educating our personnel on the risks of cyber threats and how to maintain network security. Just as we are alert to protect the network from external threats, we monitor the ministry's network online inputs and outputs, and what comes out of other government networks. We have malware detection and virus protection applications, which are constantly updated.

***Unipath**: How do you prevent the use of unencrypted devices?*

Maj. Gen. Raad: The Ministry of Defense Cybersecurity Department has been newly formed to keep pace with rapid global technological developments. Because Iraq was isolated from the world before 2003, we were unable to keep up with technological developments over the last two decades. Mobile phones became the preferred form of communication. It was not possible to educate all military units that they should not use mobile phones in military communications or make contact from the battlefield regarding military operations. We have observed misconduct among some Soldiers taking images and videos of the battlefield, and also the use of mobile phones by formation commanders during battle. Necessary measures were taken in this regard. Specific instructions and guidelines exist to prevent the use of unsecured and unencrypted devices and communications. Use is exclusively intended for encrypted and secured devices authorized by the Military Communications Directorate. However, such violations occur even in the most advanced armies. Therefore, officers specializing in information security must be assigned within all formations and be trained by the cybersecurity team, and in turn, educate and train Soldiers to follow guidelines.

***Unipath**: You took part in the Cybersecurity Incident Response Team Conference in September 2021.Can you discuss the conference recommendations?*

Maj. Gen. Raad: The conference proceedings were of the utmost importance, with the topics focused on actual current threats. I was happy to participate in the conference and get to know our brothers in the security services, see their latest tactics and benefit from their experiences in this field. As for the cybersecurity conference recommendations, they were:

1. Launch an initiative to provide a cybersecurity development program to all state institutions.
2. Adopt academic and professional curricula and specialized postgraduate studies in the

field of cybersecurity within the Ministry of Higher Education and Scientific Research.

3. Attract competency through the creation of an association of experts, amateurs and specialists in cybersecurity. To do just that, the Community Initiative Development Fund was launched with the support of civil society organizations and the private sector.
4. The Iraqi Computer Emergency Response Team (IQCERT), the Ministry of Higher Education and Scientific Research, private sector companies, and international organizations adopted the training and development of local CERT teams. The IQCERT adopted regulations for cybersecurity companies and a strategic plan to raise Iraq's position in the Global Cybersecurity Index.

***Unipath**: How does the ministry select and prepare the cybersecurity team?*

Maj. Gen. Raad: Members of the team are chosen from specialist technical department personnel belonging to the Iraqi Ministry of Defense. The team's personnel are required to be experienced and skilled officers and engineers in the field of cybersecurity, and the candidates must have completed security vetting.

***Unipath**: How stringent are the laws under which cybercriminals are tried in Iraq?*

Maj. Gen. Raad: As of late 2021, Iraq has yet to pass a law against cybercrime, but a draft awaits approval by the Council of Representatives, which then must be ratified by the government. We look forward to the adoption of this law to punish and deter perpetrators of cybercrime and prevent organized cybercriminal gangs from using Iraq's national network as a launchpad to attack other state systems with the aim of extortion or sabotage.

Cybersecurity is everyone's responsibility, and even isolated breaches can directly impact all countries of the world.

***Unipath**: How much do you cooperate with friendly nations to improve cyber technologies?*

Maj. Gen. Raad: Cybersecurity is everyone's responsibility, and even isolated breaches can directly impact all countries of the world. When I say isolated, I mean geographically isolated, not electronically. The digital era has connected the whole world and has not left any place isolated. Despite its great advantages, it also brings with it great risks that have been imposed on us, so we are vigilant in deterring anyone inclined to exploit information technology for criminal purposes, whether local or transnational. The internet, email and social media pages have made the world a village, and at the same time have made malware and viruses spread much faster. Therefore, international cooperation and information exchange between allied countries is essential. Cooperation also takes place with allied countries through special cybersecurity courses and holding exercises and competitions such as the cyber warrior competition held by the Office of Defense Cooperation of the U.S. Embassy in 2020. These courses and exercises benefit participants greatly.

We are keen to attract people with outstanding skills among Iraqi university graduates and from Ministry of Defense personnel to maintain levels of performance.

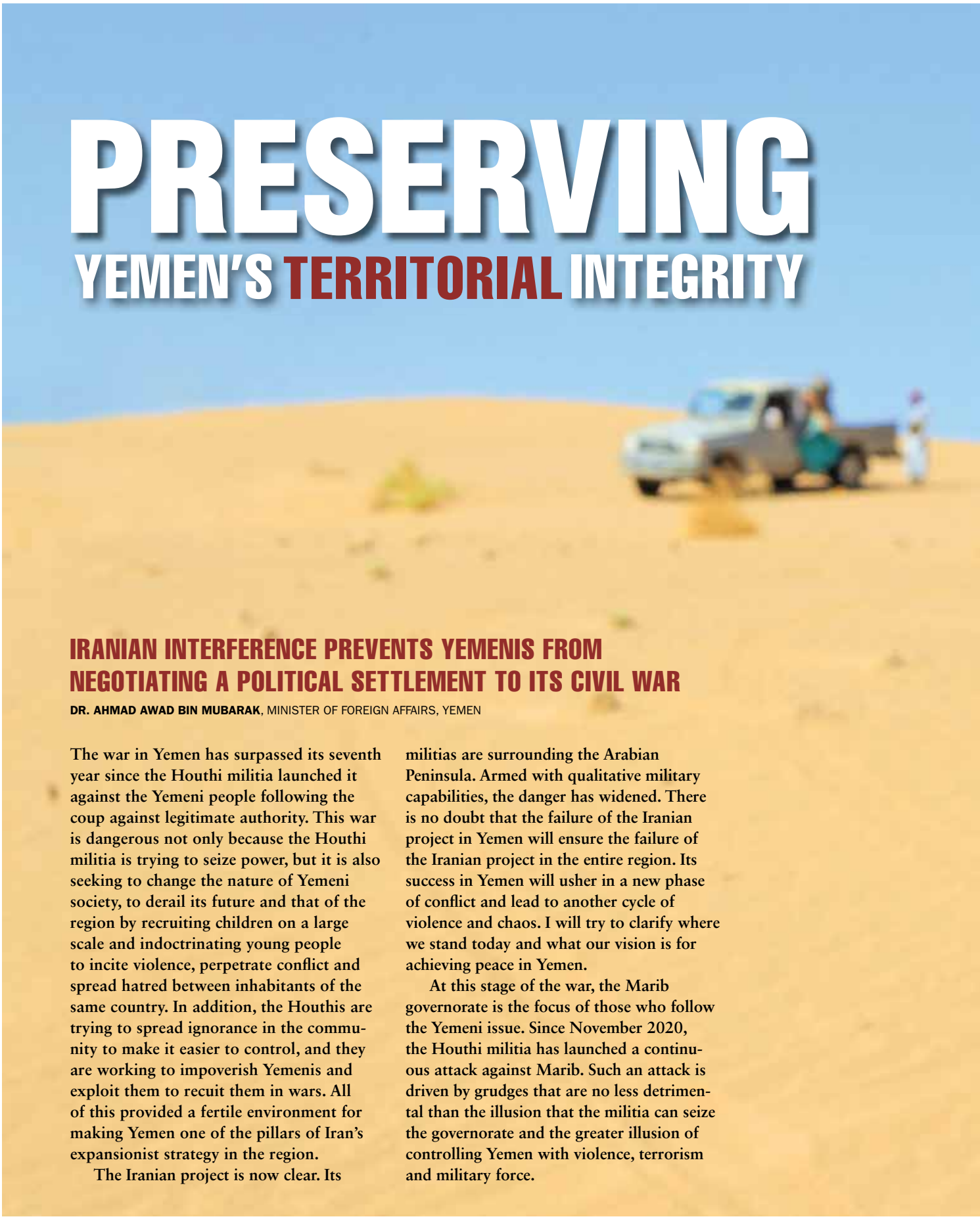
***Unipath**: How does the Ministry of Defense's Signals and Communications Directorate keep up with rapid technological development?*

Maj. Gen. Raad: We have a team that specializes in researching and tracking technological development, and we are also keen to participate in conferences and workshops specific to cybersecurity. We are working with the ministry's research and development centers and technical universities to develop our staff's skills. In addition, we plan to send our personnel to specialized courses in NATO or allied countries. We are keen to attract people with outstanding skills among Iraqi university graduates and from Ministry of Defense personnel to maintain levels of performance.

***Unipath**: Has Daesh conducted cyberattacks against Ministry of Defense websites?*

Maj. Gen. Raad: No, Daesh has not previously launched a cyberattack on Ministry of Defense sites. Perhaps the reason for this is that the ministry's network has a high level of technical fortification and an experienced information security team, in addition to the network being a closed network for movements and troops. ✦

PRESERVING YEMEN'S TERRITORIAL INTEGRITY



IRANIAN INTERFERENCE PREVENTS YEMENIS FROM NEGOTIATING A POLITICAL SETTLEMENT TO ITS CIVIL WAR

DR. AHMAD AWAD BIN MUBARAK, MINISTER OF FOREIGN AFFAIRS, YEMEN

The war in Yemen has surpassed its seventh year since the Houthi militia launched it against the Yemeni people following the coup against legitimate authority. This war is dangerous not only because the Houthi militia is trying to seize power, but it is also seeking to change the nature of Yemeni society, to derail its future and that of the region by recruiting children on a large scale and indoctrinating young people to incite violence, perpetrate conflict and spread hatred between inhabitants of the same country. In addition, the Houthis are trying to spread ignorance in the community to make it easier to control, and they are working to impoverish Yemenis and exploit them to recuit them in wars. All of this provided a fertile environment for making Yemen one of the pillars of Iran's expansionist strategy in the region.

The Iranian project is now clear. Its militias are surrounding the Arabian Peninsula. Armed with qualitative military capabilities, the danger has widened. There is no doubt that the failure of the Iranian project in Yemen will ensure the failure of the Iranian project in the entire region. Its success in Yemen will usher in a new phase of conflict and lead to another cycle of violence and chaos. I will try to clarify where we stand today and what our vision is for achieving peace in Yemen.

At this stage of the war, the Marib governorate is the focus of those who follow the Yemeni issue. Since November 2020, the Houthi militia has launched a continuous attack against Marib. Such an attack is driven by grudges that are no less detrimental than the illusion that the militia can seize the governorate and the greater illusion of controlling Yemen with violence, terrorism and military force.

A Soldier loyal to the legitimate Yemeni government surveys the battlefront in Marib governorate, where the Houthis have prolonged hostilities despite international attempts at a cease-fire.

AFP/GETTY IMAGES

Yemeni children attend school in a camp for displaced people in Hodeidah, victims of a war the Houthis have prolonged in service of Iran. Because of the war, 2 million schoolchildren have no access to regular schooling.
AFP/GETTY IMAGES

The Marib governorate, with its historic importance, has gained national and strategic importance. Many might have forgotten that this governorate defeated the Houthis in 2015 with modest combat capabilities compared to what it has today, with a population of no more than 350,000 people. It is more capable today. It has become a haven for Yemenis of various social and political affiliations, with a population of 4 million people, among which 2 million are internally displaced people. This population is supportive of an Army having a national creed and a firm and unbreakable will to end the Houthi project.

Despite this, it is necessary to point out that some stakeholders have miscalculated by starting to talk about a post-Marib scenario. If we discuss a scenario that is unrealistic for us, we will undoubtedly say that if the Houthis control Marib, it will be as bad as when its historically famous dam was destroyed. Today, Marib is the impenetrable wall for Yemen. It has become one of the strategic priorities of the Iranian regime. The fall of Marib would not only lead to a horrific humanitarian situation, but it would also mark the end of the political and peace process in Yemen. It would put an end to efforts to restore security and stability. Chaos would prevail; more violence, internal strife and waves of migration would follow. It would be the beginning of a lasting state of instability that might lead to other wars being waged from Yemen toward the rest of the region.

Our vision and approach in the Yemeni government is the following: There is no alternative to peace in Yemen. Any just, comprehensive and sustainable peace must address the political roots of the war, represented by the attempt by the Houthi militia to impose its control and hegemony by force on Yemen.

Despite the destructive Iranian intervention in Yemen, despite its military support for the Houthi militia and its financing of its war machine, treating the war in Yemen as a regional proxy war is a misconception that should be corrected. No peace settlement in Yemen can be successful without Yemenis agreeing to solve their internal problems in accordance with the outcomes of the Comprehensive National Dialogue Conference and the equitable distribution of power and wealth.

However, at the same time, it would be wrong to neglect the geostrategic dimension of Iranian interference in Yemen and Iran's desire to get closer to the Red Sea and the Arabian Sea. Such a thing will give Iran strategic added value in the conflict and will increase regional and international competition.

Iranian investment in the Houthi movement started early and increased at the beginning of the second millennium. The U.S. Navy's seizure of Iranian ships Jihan 1 and Jihan 2 on their way to the Houthis with weapons and missiles several years before the war proves that. It enables us, in fact, to debunk the claim that the current war is the reason behind the Iranian intervention in Yemen.

Among the misconceptions we can also mention that Houthis reject peace whenever they advance militarily. In

A U.S. warship seizes a boat carrying chemical fertilizer to Yemen to make explosives. THE ASSOCIATED PRESS

fact, they reject peace as a strategic principle whether they are advancing or retreating militarily, and they deal with peace as a tactic within their military strategy. We have dozens of pieces of evidence about that. The clearest is probably the Stockholm Agreement, which the Houthi militia accepted in December 2018 without implementing any of the provisions.

Understanding this helps us understand the appropriate approach to achieving peace with a group that does not base its calculations on facts, but rather on a theocratic thought based on the illusion of claiming the divine right to rule. This is the most daunting obstacle that has thwarted agreements in all peace rounds, from Geneva to Kuwait and even Stockholm. If we take into account this clear fact, we can say that the most important test for the Houthi militia — a test that it constantly rejects — is accepting a comprehensive cease-fire as the most important humanitarian step. All other humanitarian issues can be addressed before going to negotiations to find a comprehensive political solution.

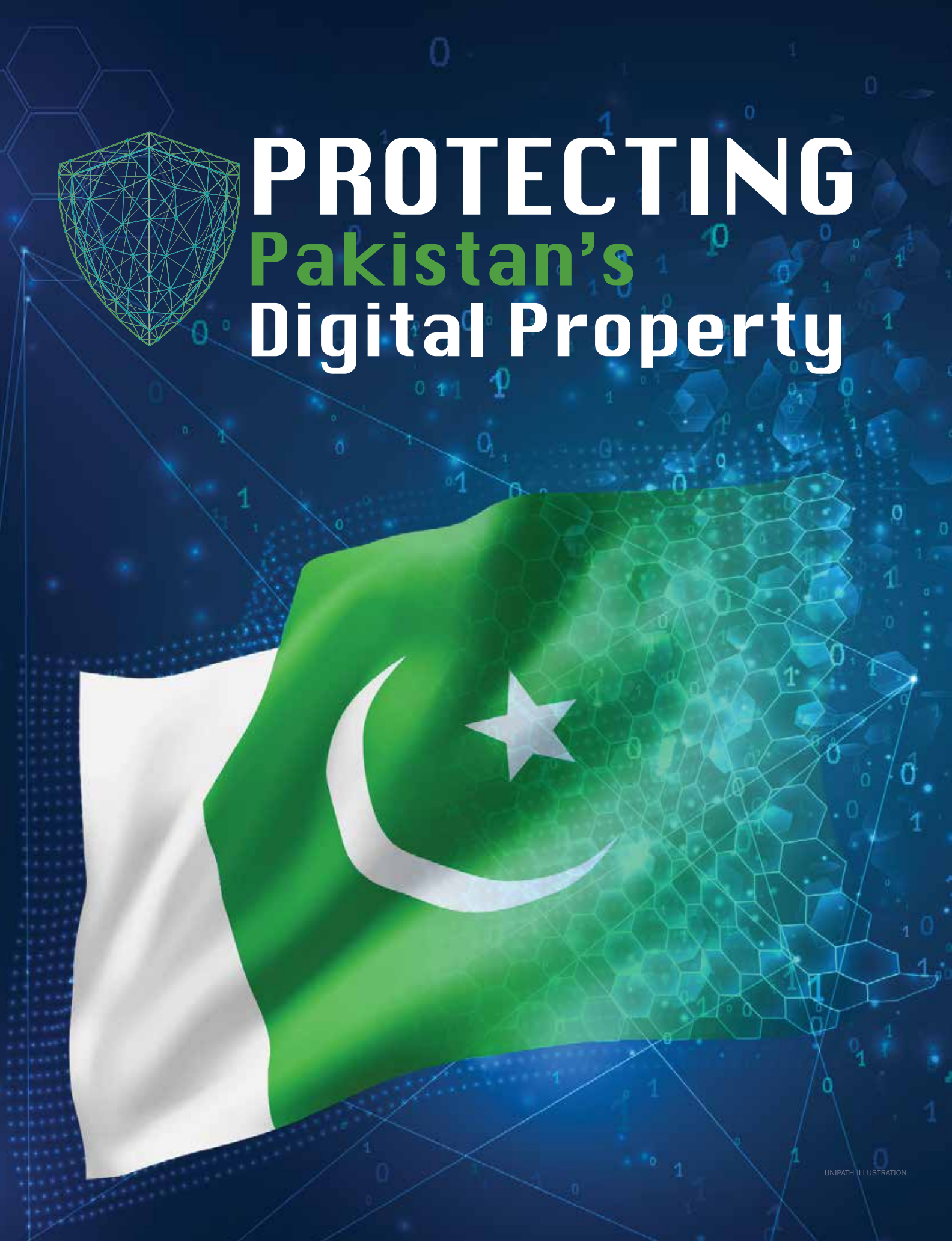
We believe that the cohesion and unity of all moderate political powers opposing the Iranian project in Yemen is the first requirement toward a political settlement. The Riyadh Agreement could be completed and implemented, in addition to the security and military annex, because they constitute an essential pillar for achieving peace, security and stability.

The regional and international support for the Yemeni government in overcoming its economic challenges and strengthening political, economic and humanitarian partnerships will enable the government to maintain a moderate Yemen that shares with the world common humanitarian values and principles. We know the importance of continued efforts among countries of the region and the world to pressure Iran to stop its subversive activities in Yemen, so that the Middle East enjoys security, peace and stability.

Achieving peace in our country is enough to curb the militias and to address the problems and issues they have caused in Yemeni society. This is why we need to deal flexibly with all endeavors aimed at achieving peace in line with our national principles, the Gulf Cooperation Council initiative and its executive mechanism, the outcomes of the Comprehensive National Dialogue Conference and United Nations Security Council Resolution 2216, to achieve a comprehensive, just and lasting peace to restore security and stability in Yemen.

In conclusion, I will reference the catastrophic environmental danger that everyone is expecting without, in fact, making any real effort to avoid it: The leakage of more than 1 million barrels of crude oil stored for seven years in the oil tanker Safer is a real disaster that will destroy the marine environment of Yemen and the region, especially the Red Sea and the Red Sea areas. The Houthis are still holding the tanker hostage. They are refusing to allow the United Nations team to maintain it. ✦

This is a slightly abridged version of a speech given at the 17th Regional Security Summit in Bahrain in November 2021 as part of the Manama Dialogue.



UNIPATH ILLUSTRATION

THE COUNTRY ADOPTS ITS FIRST NATIONAL CYBERSECURITY POLICY TO HARDEN NETWORKS AGAINST ATTACKS

UNIPATH STAFF

Concerned about cyberattacks on computer networks, Pakistan's federal Cabinet approved the country's first National Cyber Security Policy in July 2021. Pakistan's Ministry of Information Technology and Telecommunication wrote the policy to protect the nation's digital assets from cybercriminals and potential geopolitical rivals.

Pakistan breaks the policy into a series of overlapping categories — legal, technical and organizational — to improve what the country's information minister deemed an inadequate protection of devices connected to the internet. More than 65 million Pakistanis have internet service, and the country, like many around the world, is moving business and governmental services online.

Pakistan will flesh out the policy within an existing framework of government computer emergency response teams.

"The IT ministry and all relevant public and private institutions will be provided all possible assistance and support to ensure that their data, services, ICT [information and communications technology] products and systems are in line with the requirements of cybersecurity," Pakistani Information Technology and Telecommunication Minister Syed Aminul Haque announced.

Here are examples of guidelines promoted by Pakistan's new cybersecurity policy:

- Creating a Cyber Governance Policy Committee to oversee the nation's cybersecurity strategy.
- Conducting "active defense" to prevent email phishing, intrusions into government networks and malware infections.
- Protecting and improving resilience of national critical information infrastructure and government information systems.
- Encouraging public-private partnerships to take advantage of entrepreneurial innovations that benefit Pakistan.
- Conducting and sponsoring cybersecurity research and development, including improved training for personnel.
- Promoting a national culture of cybersecurity in which computer and smartphone users are encouraged and educated to protect vital information.
- Highlighting global cooperation and collaboration toward improving Pakistan's rankings on international cybersecurity indices.
- Creating a cybercrime response mechanism with improved laws and regulations.
- Establishing trust in digital transactions by using improved certification and verification mechanisms.
- Pakistani technology journalist Jehangir Mudassar, writing in Pakistani military magazine Hilal, stressed that protecting computers and cell phones against attacks requires a shift in awareness across all of society.

"Cybersecurity is not a matter of pressing a button to activate a specific protocol. It's a culture that must become a part of our lifestyle, whether as a citizen, a public servant, or people from the security forces," Mudassar wrote.

"For improving our present and future cybersecurity, a comprehensive cybersecurity policy must be a part of our rule book that all the stakeholders should endorse." ✦

Sources: Pakistani Ministry of Information Technology & Telecommunication, Hilal, Dawn, Eurasia Review

Pakistani vendors download files from computers to mobile phones in Faisalabad. The country's growing use of information technology requires the government to strengthen cyber policies. AFP/GETTYIMAGES

UNIPATH ILLUSTRATION

THE NEED TO IMPROVE INTELLIGENCE

ISSAM ABBAS AMIN, INTELLIGENCE AND SECURITY DIRECTORATE, IRAQI MINISTRY OF DEFENSE

The intelligence community suffers under the weight of unrealistic expectations about preventing unforeseen events, especially those that target state sovereignty or internal security. An example of this was the two drone attacks on the Iraqi prime minister's home on November 7, 2021.

By its very nature, intelligence failure always raises questions about the competency of intelligence services and their working methods to prevent any security breach.

The dilemma of intelligence is that it is constantly open to criticism. Even well-regarded intelligence services such as those of the United States have experienced strategic failures throughout their history. Examples that come to mind include the Pearl Harbor attack in 1941, the North Korean invasion of South Korea in 1950, the Soviet intervention in Czechoslovakia in 1968 and the September 11 attacks in 2001. Sometimes an agency fails to provide sufficient warnings, as happened in the case of September 11, or issued plentiful but incorrect warnings, as was the case regarding Iraqi possession of weapons of mass destruction.

In both cases the failure was obvious and the criticism scathing. The prevailing belief here is that intelligence should be correct across the board every time. This is impossible in the real world, which is a source of great frustration when anything unforeseen occurs.

Intelligence services can play their role relatively well if the question relates to the posture of a neighboring state such as Iran or how much Iraq would suffer were it attacked at a particular location. This type of intelligence addresses open-ended questions, and the ability to understand the topic depends more on good assumptions than credible information.

But what if the questions were, for example, when and where Daesh would launch another attack? This is different because the exact answer requires penetrating the inner circles of the organization, which depends on our ability to achieve breakthroughs in information collection methods.

In addition, it is difficult to improve the quality of intelligence work, especially in regard to analytical methods to prevent unforeseen events. Despite improvements in methods and means of information collection, that doesn't represent a shift in the degree of credibility of intelligence analysis and evaluation. Uncertainty and doubt remain even in the presence of highly credible and reliable information.

The important takeaway here is that intelligence cannot always remove the element of surprise. Intelligence is good at informing decision-makers of the facts, which enables these leaders to reach decisions with reasonable confidence. This is no small feat, and it may not happen often.

At the strategic level, intelligence services are responsible for national-level intelligence assessments that shape national security policies and strategies, security risk management, security budgets, and the composition of the Armed Forces. The Iraqi Joint Chiefs of Staff rely on such assessments in their planning.

We must also stress the difference between intelligence assessments at the national level in relation to foreign threats and those concerning the domestic environment. Iraq has focused more on this issue than the foreign one, which is an omission that must be addressed.

Another weakness is that current intelligence analysts are tied to the chain of command, right up to the top of the pyramid. This inevitably affects objectivity and impartiality. It's preferable for


우리민족
조선인민군

INTELLIGENCE ASSESSMENTS AT THE NATIONAL LEVEL ARE CRITICAL TO GUIDE THE ACTIONS OF POLITICAL LEADERS



Four examples of intelligence failures that changed the world: (opposite page) The North Korean invasion of South Korea in 1950, (above, left to right) The attack on Pearl Harbor in 1941, the Soviet invasion of Czechoslovakia in 1968 and the September 11 attack in the United States.
AFP/GETTY IMAGES

intelligence departments to maintain a certain independence when preparing intelligence assessments for strategic decision-making.

Intelligence assessments at the national level are critical to guide the actions of political leaders. These assessments should be professional, practical and usable. For example, a strategic warning of war, which is a political-military issue, can be jointly assessed by the General Directorate of Intelligence and Security and the Ministry of Foreign Affairs, each according to its mandate.

However, these two branches of government are not integrated sufficiently to draft credible warnings jointly. Doing that requires a high level of coordination and cooperation and a common bureaucratic language.

Intelligence assessment has turned into a more complex and difficult task, due to the emergence of new entities, volatile arenas, and dynamics whose outcomes are difficult to predict. In addition, complexity has grown from ongoing social and cultural processes — including the adoption of new technologies such as social media — that are new to the intelligence community. Intelligence departments often lack the necessary expertise to deal with these innovations that represent the root of numerous problems, challenges and risks.

In the current circumstances, it is difficult for the intelligence community to accurately predict what will happen tomorrow, as everything happens so quickly. Enemies can act instantly in cyberspace, and drones and missiles require little time to launch. This shortens the time it takes for the enemy to advance from idea phase to implementation. Such was the case with the attack of November 7, 2021. It surprised not just the prime minister but his intelligence services as well. ✦

An intelligence assessment consists of:

1. **Threats.** Describes the capabilities and intent of the various players and links between them, analyzes processes and trends at the organizational level and regional and global policies.
2. **Processes.** Describes the possibility of ongoing processes and trends, presents scenarios, and analyzes potential responses of actors regarding specific events. For example, how would actors (domestic and foreign) respond if our forces acted in a certain way?
3. **Recommendations**. Offers advice regarding risk and opportunity.

We regret to report the death of author Issam Abbas Amin. His passing is a great loss for Unipath readers and the Intelligence and Security Directorate of the Iraqi Ministry of Defense.

NAVY

AT THE READY

JORDAN ARMED FORCES

An interview with Commander of the Royal Jordanian Navy Col. Hisham Khalil Al-Jarrah

UNIPATH STAFF

UNIPATH: *Describe the duties of the Royal Jordanian Navy*

Col. Al-Jarrah: The Royal Navy is one of the Jordan Armed Forces' three branches (land, air and sea) and complements the national defense system by playing a dual role — the military role of the Navy and the organizational and security role of the Coast Guard. It is considered the main maritime force and is primarily responsible for Jordanian maritime security, a mission it conducts through a number of duties. These include patrols to protect and guard Jordanian maritime borders to prevent infiltration and smuggling, naval inspections conducted by qualified and trained inspection teams with state-of-the-art equipment, detection and prevention of any violation in regional waters, application of approved laws and monitoring civilian and military facilities and critical targets in Aqaba through the Naval Operations Center, in addition to search and rescue operations in regional waters and protection against marine pollution.

UNIPATH: *What maritime security challenges face the Jordanian Navy in the Red Sea?*

Col. Al-Jarrah: The challenges facing the Jordanian Navy in the Red Sea within the framework of maintaining Jordanian maritime security take various guises. This includes those of an unconventional nature, such as terrorism, which may take multiple forms such as vessel and port attacks as well as maritime piracy, which threatens the safety of shipping, and most recently the coronavirus crisis, which has cast a shadow over maritime transport operations. Some of these challenges have a conventional security aspect, such as the infiltration and crossing of maritime borders and all forms of trafficking, while some challenges are special, such as maritime incidents and disasters, vessel and port fires, maritime pollution and strike action. In light of such challenges, all agencies dealing with maritime security must increase their coordination, efficiency and readiness.

UNIPATH: *How can partner nations help develop the Jordanian Navy? What types of vessels and equipment are needed?*

Col. Al-Jarrah: International and regional partnerships undoubtedly have had a major role in improving Jordanian naval capabilities within the field of training and in gaining expertise through joint courses and exercises. They also meet the needs of the Jordanian Navy in terms of the presence of vessels capable of operating outside regional waters with the necessary high-specification equipment, which has the potential to improve rapid reaction capability and reduce emergency response time. It goes without saying that it has developed the capabilities of the 77th Marine Battalion, enabling it to carry out its duties. It is worth pointing out the close collaboration between the Jordanian Navy, the United States Navy and the United States Marine Corps in this area.

UNIPATH: *Is there security cooperation with nations bordering the Gulf of Aqaba?*

Col. Al-Jarrah: Certainly, the duty of maintaining Jordanian maritime security requires a high degree of cooperation and coordination with nations

bordering the Gulf of Aqaba. It is Jordan's only maritime port for international shipping lines and, of course, there is ongoing security cooperation with these nations through liaison officers and periodic security meetings. This coordination and cooperation translate into naval exercises conducted in these nations.

UNIPATH: *How important are joint regional and international maritime exercises?*

Col. Al-Jarrah: Conducting bilateral or multilateral naval exercises plays an important role in achieving the required level of cooperation and coordination between naval forces. This has a positive impact on the effectiveness and competency of the forces involved in these exercises. In addition, it contributes to all parties gaining expertise and exchanging skills so that concepts and procedures used by naval forces, both regionally and globally, are unified to a high degree.

UNIPATH: *As part of Combined Maritime Forces, how has Jordan benefited from the experiences of some of the other 34 countries in the coalition?*

Col. Al-Jarrah: Since the establishment of the Combined Maritime Forces in 2009, the Royal Jordanian Navy has been an active member. This involvement has highlighted the effective role and exemplary image of the Jordanian Navy, and it has undoubtedly contributed to the development of Jordanian naval ranks by exchanging expertise with participants from coalition countries, familiarizing themselves with the ways international naval forces work, and learning about the experiences of various countries in managing maritime operations. This, in turn, has had a positive impact on the standards of officers, noncommissioned officers and personnel involved, which therefore provides the Jordanian Navy with a higher standard of training, expertise and skills, as well as building friendships and achieving social and cultural awareness objectives with participants from other countries.

UNIPATH: *What exercises does the Royal Jordanian Navy participate in, and why is this participation important to you?*

Col. Al-Jarrah: The Jordanian Navy engages in various exercises at three levels: local and national, regional, and international. At the local level, the Navy organizes internal exercises within the scope of Naval Command to increase cohesion and cooperation among units. Some of the exercises and various scenarios are carried out at the national level with the involvement of military and security services and some civilian bodies with maritime

Jordanian Marines train and conduct operations in the Gulf of Aqaba. JORDAN ARMED FORCES

JORDAN ARMED FORCES

Col. Hisham Khalil Al-Jarrah, commander of the Royal Jordanian Navy, right, and Vice Adm. Brad Cooper, commander of U.S. Naval Forces Central Command, examine a new Saildrone Explorer unmanned surface vessel in Bahrain in November 2021.

PETTY OFFICER 2ND CLASS
MARK THOMAS MAHMOD/U.S. NAVY

jurisdiction. The aim is to achieve the desired level of cooperation and coordination among these groups and increase maritime disaster response capabilities. At the regional level, the Jordanian Navy regularly takes part in naval exercises alongside nations bordering the Gulf of Aqaba. Exercises have taken place in the Hashemite Kingdom of Jordan, such as Eager Lion and Infinite Defender, in Egypt with the Bright Star exercise, and in Saudi Arabia with the Red Wave and Secure Coast exercises. At the international level, the Jordanian Navy has been a constant presence at numerous international naval exercises as an active participant or as an observer. There is no doubt that a continuous permanent presence such as this allows Jordanian naval personnel to familiarize themselves with the latest naval operational management techniques and to exchange expertise and gain experience with those taking part.

UNIPATH: *How has the U.S. Marine Corps helped develop your forces?*

Col. Al-Jarrah: The Jordanian Navy, through the 77th Marine Battalion, enjoys a special relationship with the U.S Marines. This relationship was manifested in the joint harmonization program implemented over several years and has contributed to raising the readiness and training level among the battalion for defensive and offensive operations, internal security operations, as well as training navy SWAT and vessel inspection teams. It should be pointed out that through this partnership with the U.S Marines, the 77th Marine Battalion has been supplied with various equipment and sophisticated devices used in the field of naval infantry (Marines). The importance of this relationship is also highlighted through ongoing joint tasks and multilevel coordination. As the Jordanian Navy Command, we seek to preserve and develop this relationship to serve the common interests of both parties.

UNIPATH: *How does the Jordanian Navy interact with the rest of the Armed Forces and security institutions to secure Jordanian territorial waters?*

Col. Al-Jarrah: Jordanian maritime security is a joint responsibility that falls on various military and security agencies, government bodies and authorities concerned with maritime activities. Therefore, the Jordanian Navy recognizes the importance of cooperation and coordination with different agencies to achieve the desired aim of protecting Jordanian territorial waters. This cooperation and coordination is demonstrated by the exchange of information with the Maritime Operations Center, which is equipped with the latest surveillance systems and sophisticated communications networks, and continuous updating of marine disaster response and security plans for Aqaba. There is also ongoing communication with security officers and specialist authorities, and joint maritime exercises are conducted at the local and national level covering all possible scenarios, which enhances interagency cohesion and contributes to them reaching a high standard of coordination.

UNIPATH: *Please discuss the preparation and training for Jordanian naval and Marine personnel.*

Col. Al-Jarrah: Members of the Jordanian Navy, including officers, noncommissioned officers and personnel, are subject to an intensive competency and training program in line with a Soldier's basic military requirements. This includes basic training, weapons training, marksmanship, swimming, and security and awareness training. This is followed by specialized naval and technical training and training specific to Marines depending on the various trades. In addition, these members take part in training courses held at Jordanian naval and security agency institutes, as well as at civilian institutes specializing in marine science.

UNIPATH: *Do officers and noncommissioned officers undergo training outside the kingdom?*

Col. Al-Jarrah: Jordanian naval officers and noncommissioned officers take part in a number of external courses held in maritime training institutes of allied and friendly nations. These include foundation and advanced courses for naval trades (Navy, marine engineer, frogman, Marine infantry), in addition to different language courses, and training courses for staff officers and senior leadership to achieve the desired training outcome, which is to increase the effectiveness and competency of these ranks and equip them with the skills and expertise by familiarizing themselves with the experience of others.

UNIPATH: *Does the Jordanian Navy conduct missions to safeguard the marine ecosystem?*

Col. Al-Jarrah: One of the most important duties of the Jordanian Navy is to protect the marine ecosystem. Jordan has formed a specialized organization to protect the marine environment, and there is constant cooperation and coordination so that all its recommendations related to the preservation of the marine ecosystem and regulation of fishing are implemented. It must be noted that in the Jordanian Navy we monitor the fishing industry and prohibit illegal fishing methods. ✦

CYBERSECURITY THE LEBANESE WAY

The Lebanese Armed Forces Cybersecurity Department Builds Awareness About Attacks

Unipath interviewed Brig. Gen. Ali Qanso, chief spokesman of the Lebanese Armed Forces. He described how the Lebanese military combats threats to its computer networks that could affect national security.

Unipath: Cybersecurity has become an integral part of any state's national security. What cyber threats does Lebanon face?

Brig. Gen. Qanso: Lebanon is exposed to cyber threats from numerous actors, all of whom seek to breach our online systems, spy on communications and steal information. There are terrorist organizations that breach accounts to propagate extremist ideology among young people, with the aim of recruiting them, as well as the risk represented by people or groups active within Lebanon and worldwide who target governments and their institutions electronically.

In this context, Lebanon is exposed to cyberattacks 24 hours a day, including distributed denial of service and attacks on the banking sector (using malware such as Gauss and Flame), the telecommunications sector and various civilian companies.

Lebanon's capacity to counter such attacks is weakened by its lack of cyber protection systems and trained human resources capable of deterring such attacks. Consequently, cybersecurity operations and responses are limited to a reactive response and ensuring protection against these attacks as much as possible.

Unipath: What is the role of the Lebanese Armed Forces Cybersecurity Department?

Brig. Gen. Qanso: Most armed forces aim to establish cybersecurity departments to protect their resources within the various systems and networks they operate. These resources include sensitive security and military information related to weaponry, equipment, mission execution, deployment of units and personal and professional details pertaining to military and civilian personnel. These resources also include intranet, internet, and wireless communications.

As for the Lebanese Armed Forces, the Cybersecurity Department plays a very important role in deterring attempts at disruption or breaches that target military and security information systems. This is considered a significant security threat that puts the work of the Lebanese Army, its units and the lives of its personnel at great risk.

Unipath: How much impact do these kinds of attacks have on the Lebanese Army?

Brig. Gen. Qanso: The Lebanese Armed Forces use several cyber network systems, including official government websites, email services and smartphone applications, among others. It also ensures internet access for the various troops and units.

All these systems constitute areas that may be exploited by the nation's enemies or any other actor that seeks to cause damage to the Army. For example, the success of an attack may lead to the disruption of the internal communications network that links units to the command. Army websites or one of the official social media accounts may be breached, or sensitive information may be stolen from the internal network where files are exchanged.

Such matters would have serious repercussions for the Army, its units and personnel, particularly if they were in the hands of terrorist groups constantly targeting military personnel and locations.

Unipath: How important is international cooperation in protecting Lebanese computer networks?

Brig. Gen. Qanso: International cooperation is crucial in protecting Lebanese information networks. This is conducted on two levels: The first is to provide the advanced software necessary to fortify our networks from cyberattacks, and the second is to train the human element to deal with these attacks and react appropriately as quickly as possible to prevent them or limit their damage.

Unipath: How can your personnel develop skills in line with the evolution of cybersecurity?

Brig. Gen. Qanso: Our personnel take part in various training courses, lectures and conferences in Lebanon and abroad. The world of cyber is evolving at a rapid pace, and cyberattack malware is produced daily in the thousands. In addition, thousands of groups and individuals who are perfecting cyberattacks worldwide are constantly devising new methods. Our enemies also continue to improve their online capabilities with the aim of breaching our information systems.

For all of this, our personnel must keep pace with the latest developments in the field of cybersecurity so they are ready to face new challenges. On the other hand, perfecting our cyber defense also requires sophisticated equipment and software that we work to secure in cooperation with friendly states and actors. ✦

THE ROLE OF OMAN'S Maritime Security Center

From left, Brig. Gen. Ali bin Saif Al Muqbali, director general of the Royal Oman Police Coast Guard; Pakistan Navy Rear Admiral Abdul Munib, then commander of Combined Task Force 151; and Pakistan Defense Attache Capt. Kashif Farhan visit the Royal Oman Police Coast Guard headquarters in Muscat.

Rear Admiral Abdul Munib, left, and Brig. Gen. Al Muqbali, exchange gifts.

UNIPATH STAFF | PHOTOS BY COMBINED TASK FORCE 151

The Maritime Security Center, made up of Omani military, security and civilian agencies, keeps territorial waters safe and stable.

The center at Al-Murtafaa Garrison gets reports from those agencies and coordinates with the relevant authorities. Its specialized systems and equipment protect Omani waters 24 hours a day.

As part of its duties, the center:

1. Unifies efforts between the maritime security authorities.
2. Provides the necessary capabilities and assets in terms of equipment, devices, reconnaissance aircraft, ships and boats.
3. Develops procedures and plans to counter illegal activities and organized crime at ports, facilities and coastal areas.
4. Upholds procedures and measures to protect and preserve fish stocks, natural resources and aquatic life.
5. Responds to environmental and humanitarian disasters with the capabilities and assets at the disposal of the sultanate.
6. Participates in maritime crisis and disaster management planning and prepares maritime risk scenarios.
7. Educates citizens, residents and seafarers on the importance of security and cooperation to protect the natural maritime riches of the sultanate.
8. Tracks and monitors ship movements in and around Omani territorial waters.
9. Reinforces cooperation with allied and friendly nations and with regional and international organizations related to maritime security.

The center is responsible for monitoring violations in or near Omani waters. They include:

1. Maritime piracy.
2. Illegal migration or infiltration.
3. Illegal fishing and overfishing.
4. Marine pollution.
5. Obstruction of international shipping routes.
6. Maritime terrorism.
7. Tampering with and/or sabotaging offshore oil facilities.
8. Organized crime, illegal trade and smuggling. ✦

Rear Admiral Abdul Munib, center, and his staff tour Oman's Maritime Security Center.

Agile Leadership

Lt. Gen. Qais Khalaf Rahima Wrestles With Threats Both Traditional and Modern

UNIPATH STAFF | PHOTOS BY IRAQI MINISTRY OF DEFENSE

His complexion and distinctive features denote his Sumerian roots. Kindhearted, courageous and polite, he refines his words when he addresses his guest, embodying the spirit of Southern hospitality. His humility and courtesy do not stop him from providing insights on military science. The perception of him gained from the many battles he fought as a Soldier is that of a stubborn self-sacrificer with nothing on his mind other than victory.

He is Lt. Gen. Qais Khalaf Rahima, the Iraqi Armed Forces deputy chief of staff for operations and commander of Joint Operations Command-Iraq. It is a name and a history that mean a lot to political and security leaders. With professionalism and integrity, he has proved worthy of the daunting task of defending the nation.

Born in Maysan in 1962, he was raised to understand the manner of conversing among gentlemen from an early age. He graduated from the First Military College in 1984 and earned a master's degree after the first Gulf War and a Ph.D. after the liberation of Mosul, reinforcing his studies with combat experience.

"When I entered Military College in 1984, the battles in the Iraq-Iran war were at their most intense," the general said. "The college was a combat front, where students received the expertise of their professors who were returning from the front lines to share the experiences from the field and the lessons learned from battle. We learned a lot from field commanders who came to give lectures. When we graduated, we had field and academic experience as if we had actually taken part in the war."

Despite working in operational sectors, Lt. Gen. Qais aspired to get into strategic studies and joined the National Defense College in 2010.

"I was very happy to be nominated by the Ministry of Defense to study [national security strategy] and obtain a master's degree. The education was unique and taught by professors who were specialists in political and military sciences. It was a unique experience because of the expertise I had gained from the field in Tal Afar, and I began to analyze the plans I put in place to reestablish security in that city alongside the syllabus. This prompted me to study for the Ph.D. on the topic of "New Wars and Transformation in the Concepts of Power" in 2019. Despite my concerns working as the mid-Euphrates operations commander, the security conditions in the country and the postponement of my thesis

several times, I was determined to finish my studies. Especially since the specialization is linked to all the challenges Iraq is going through, and fifth- and sixth-generation warfare in particular."

Lt. Gen. Qais did not stop at traditional warfare. He has led the way by diving into the world of contemporary military science through strategic research, his awareness of the importance of cyberwarfare, and the danger of terrorist and extremist groups dominating social media channels.

"After the trauma of Daesh and their control over large swaths of land, they relied on psychological warfare by disseminating rumors on social media channels to further disrupt the security situation.

"At that point, the responses of the state's, official and nonofficial media institutions were not up to the challenge. The terrorist groups were working in a vast theater of operations that relied on spreading terror in the hearts of the population by producing scenes of beheadings, blowing up markets, capturing women, and uploading them on social media pages to act as a message to others," the general said.

"Their aim was to break the morale of their opponents and force citizens to compromise and submit, and for the security forces to surrender. We began by dismantling their cyber networks that were operating outside Iraq and from areas under their control."

The general and his colleagues worked alongside international coalition forces to track and shut down Daesh's cyberwarfare networks. Iraqi electronic warfare teams also cooperated with teams from the coalition to track people tweeting and blogging in support of Daesh and to close their accounts.

"We then focused on rebuilding the confidence of the forces and raising morale, and we succeeded in restoring the psychological combat readiness of personnel in our units," the general said. "Subsequently, our heroes stood up on the battlefield, never withdrawing from their sectors of responsibility, even in the most fierce battles. It began to become clear to them that the false

An Iraqi M1A1 tank from the 9th Armored Division takes a defensive position outside Mosul in 2017.

image created by Daesh propaganda online — that the terrorists were fighters from another planet who could not be defeated or killed by bullets — was a big lie."

He credits social media channels and young people in the defeat of Daesh. They exposed the lies of Daesh, so it became difficult for Daesh to spread any mistruth. That is how the Daesh electronic army and media machine was defeated by civilian activists, intelligence agents and coalition forces, which paved the way for Daesh to be defeated on the ground.

Aware of the fact that fourth-, fifth- and sixth-generation warfare relies on modern technology, Lt. Gen. Qais advises armies to keep up with technological development so they can confront current and future threats that usually fall under the heading of asymmetric warfare.

Armies must strengthen their online defenses and build cyber intelligence agencies capable of monitoring adversary activity to prevent any national security breach and prohibit malicious groups from launching cyberattacks. Modern technology, the internet and drones make the security agencies' work more complicated, he said.

Lt. Gen. Qais was commander of the 10th Brigade in Tal Afar district from 2004-2008, which was a hotbed for al-Qaida, taking Iraq down a dangerous path. Sectarian fighting and terrorist gangs dominated the cities.

"I was assigned complex missions and responsibilities for numerous reasons, the most significant of which was the control of al-Qaida over the city and surrounding areas, as well as the population demographics that consisted of multiple sects and creeds," he said. "I assumed command of the 10th Brigade at a time when fear and despondency were written on the face of every Iraqi, and the threat of death loomed over their heads. The police service had not been formed yet, which added a greater burden on the Army to provide security. There was a very significant gap in trust between the population and the security forces that were unable to protect the city from acts of terrorism."

A M1A1 tank from the 9th Armored Division enters the battle for Mosul in 2017.

Left: A team at the Iraqi Ministry of Defense media center monitors broadcasts to respond to any terrorist propaganda.

Right: Lt. Gen. Qais, then commander of Baghdad operations, talks to an Iraqi activist in Tahrir Square in 2019.

"Working as a team with coalition forces, the situation slowly stabilized. They focused on security and intelligence, relying on civilian and national sources to stabilize the city. They also encouraged the Sunni people in Tal Afar to join the Army and police ranks, and this was one of the important goals we were able to achieve later on. They worked to reduce the gap between the ethnic and religious aspects of the judiciary, to instill confidence, reject sectarianism and communicate with the population."

Baghdad experienced bloodshed in early October 2019, when demonstrators demanded an improved economy and an end to governmental corruption, which was met with excessive force from some ill-disciplined groups and could have led Iraq into a dangerous downward spiral. The political and military leadership had little choice but to replace the security leaders in those areas and put in place a commander who possessed self-control, patriotism and courage. It was here that the name of Lt. Gen. Qais emerged to be assigned this difficult task.

"Civilian casualties caused a profound divide in trust between the people and the security forces, and the confused security picture aggravated the situation. There was a big problem with the lack of specialized forces trained and equipped for such service. Of course, such special missions and duties require wisdom, patriotism, composure and compassion before military experience and the art of leadership. This is in addition to gaining the trust of peaceful demonstrators by protecting them and preventing security forces from provoking them."

It was also necessary to act within the powers of the Constitution and laws to combat riots and to deal with nonpeaceful demonstrators who attacked infrastructure and security sectors differently than peaceful protesters, who conducted demonstrations according to the Constitution.

"As soon as I assumed the post, I worked to establish the units of responsibility, and I defined the jurisdiction of every officer, putting clear barriers in place that observed international human rights treaties, in order to separate the demonstrators and the security forces," the general said.

"Cameras at the barriers and security checkpoints were installed to monitor any disciplinary violation. I issued strict orders and took written pledges from every officer not to use live bullets against demonstrators for any reason, and I prevented the use of rubber bullets and some tear gas canisters."

He worked on communicating daily with peaceful activists and demonstrators. The situation quickly defused.

"We restored respect for the Army and security forces," the general said. "After all, they exist for the sake of the people, and derive their strength and determination from them."

Lebanon Strengthens Electronic Surveillance Against Smuggling

UNIPATH STAFF

The Lebanese Armed Forces (LAF) have activated a cross-country surveillance system to plug security gaps along the country's border with Syria.

Smuggling and infiltration have been sufficiently serious that Lebanon has maintained four regiments on its northern and eastern borders since 2009.

To shut down smuggling routes, LAF also established a network of electronic monitoring towers linked to the Joint Operations and Information Center at the Lebanese Army Command. The system allows permanent day and night monitoring, while providing early warning to mobile units dispatched to confront violators, said Gen. Joseph Haddad, the head of Lebanon's Joint Border Security Committee.

Phase two of the plan, which began in November 2021, consists of integrating coastal surveillance radars to the inland monitoring towers. Haddad said the integrated system "plays the role of early warning in times of crisis."

LAF's 1st Land Border Regiment (LBR) operates in the area from the Mediterranean Sea to the town of Wadi Khaled. The 2nd LBR is responsible for the upper half of Baalbek-Hermel's frontier with Syria. The 3rd LBR operates in mountainous terrain near Rashaya, and the 4th LBR's area of responsibility is the lower half of Baalbek-Hermel.

Lebanon's commitment to secure borders has drawn the support of international partners. United Kingdom Ambassador to Lebanon Ian Collard, U.S. Ambassador Dorothy Shea and Canadian Ambassador Chantal Chastenay met in November 2021 with Lebanese Army Chief Gen. Joseph Aoun to discuss Lebanese-Syrian border security.

"The discussions focused on the Lebanese Armed Forces' mission to secure the entirety of the Lebanese-Syrian border and the challenges they are facing during Lebanon's many crises," the British Embassy announced.

During the meeting, Ambassador Collard announced the donation of $1.4 million to strengthen LAF's resilience with spare parts for Land Rovers previously donated by the U.K. and protective personal equipment for female Soldiers deployed in border operations.

The British contribution followed a September 2021 announcement that the United States had provided $47 million in military aid to Lebanon.

While briefing the United Nations Security Council in November 2021, U.N. Special Coordinator for Lebanon Joanna Wronecka encouraged additional international support for the Lebanese Armed Forces and praised the critical role they play in safeguarding Lebanon's security and stability.

Sources: Office of the United Nations Special Coordinator for Lebanon, defensenews.com, arabweekly.com

Lebanese security forces staff the Al-Qaa border crossing with Syria. AFP/GETTY IMAGES

Kyrgyzstan Presses Forward on Domestic Reforms

UNIPATH STAFF

Kyrgyzstan will benefit from donations from the European Union to support governmental reform, human rights initiatives and water security.

In December 2021, the European Union approved financing worth 62 million euros as part of a four-year effort to aid Kyrgyzstan.

Kyrgyz President Sadyr Japarov votes with his wife, Aigul Asanbaeva, during parliamentary elections in Bishkek in November 2021.
AFP/GETTY IMAGES

In terms of governance and digitalization, the focus of the money will be on promoting and improving the rule of law and digital transformation.

Human development, including improving the quality of education and promoting gender equality and human rights, is also part of the EU's assistance for Bishkek.

The EU also stressed Kyrgyzstan's need to integrate and share water resources within its semiarid region. Water security among Central Asian nations has been a major diplomatic issue since the dissolution of the Soviet Union.

These financial priorities were determined in consultation between Kyrgyzstan and EU member states. The priorities are also in line with the United Nations' 2030 Agenda, the Paris Climate Agreement and the EU's Global Gateway strategy.

"The EU has a long-standing partnership with the Kyrgyz Republic as a primary and reliable development partner," Ambassador Eduard Auer, head of the EU delegation to Kyrgyzstan, said at the conclusion of the funding agreement in late 2021.

"Today we celebrate a new step in our collaboration, committing to long-term support for governance, digitalization, education, green growth and other areas of mutual interest. The new multiyear program is a compelling evidence of the EU's continued support for the Kyrgyz people." **Sources: Vecherniy Bishkek, Vesti.kg**

TURKMENISTAN Announces Foreign Policy Goals

UNIPATH STAFF

Turkmen President Gurbanguly Berdymukhammedov committed his country to the pursuit of peace, security and diplomacy during an address to the United Nations General Assembly on September 21, 2021.

President Berdymukhammedov announced that his country would host an international conference in Ashgabat in December 2021 titled "The Politics of Peace and Trust — the Basis of International Security, Stability, and Development."

His U.N. speech also proposed the creation of a zone of peace, trust and cooperation called "Central Asia — Caspian region." He emphasized that Turkmenistan is interested in helping bring peace, harmony and unity to Afghanistan.

In the final part of his speech, President Berdymukhammedov affirmed Turkmenistan's readiness for a continued dialogue on achieving sustainable development goals, including continued focus on minimizing the effects of desertification near the Aral Sea. He expressed his readiness to create a U.N. Special Program for the Aral Sea Basin along with partners in the region.

Sources: Turkmenportal, United Nations

Houthis Accused of Executing Civilians

UNIPATH STAFF

Yemen's legitimate government protested the illegal execution of nine people, including a 17-year-old, that the Houthis blamed for killing one of their leaders.

The nine had been held in arbitrary detention and were subjected to torture and other abuse after they were accused of involvement in the 2018 death of Saleh al-Samad.

Warning that the Houthi militia will carry out more mass killings against innocent civilians, Yemeni Minister of Information Muammar Al-Eryani dismissed the extrajudicial executions as premeditated murder on fabricated charges.

Al-Samad was killed along with six others in an airstrike conducted by the Coalition to Restore Legitimacy in Yemen. He was the group's most prominent political official as chairman of the Houthi's Supreme Political Council.

Regional social media platforms published the names and photos of the executed Yemenis as: Ali Al-Quzi, Abdul-Malik Hamid, Muhammad Haig, Muhammad Al-Quzi, Muhammad Noh, Ibrahim Aqel, Muhammad Al-Mashkhari, Abdul-Aziz Al-Aswad and Moaz Abbas, all of whom were from the Al Qanawis district in Al Hodeida governorate.

Human rights organizations such as the Yemeni Coalition for Monitoring Human Rights Violations, SAM for Rights and Liberties, the Human Rights Radar, the Abductees' Mothers Association, and the National Association for the Defense of Rights and Freedoms jointly issued a statement strongly condemning the executions carried out by the Houthis.

An 8-year-long conflict has ravaged Yemen, inflicted immense suffering on its people and displaced over 4 million Yemenis from their homes. Since the start of the civil war in September 2014, over 233,000 people have died, including 102,000 as a direct result of hostilities and 131,000 from indirect causes such as famine and poor health care.

Serious violations of international humanitarian law and egregious human rights abuses by Houthi militia have contributed to the world's worst human-made humanitarian crisis. Moreover, Houthi obstruction of humanitarian assistance has exacerbated the spread of diseases, including a cholera epidemic and COVID-19.

Sources: CNN, Alhurra, Al Jazeera

Dialogue and Diplomacy Between Uzbekistan and the U.S.

UNIPATH STAFF

Uzbekistan hosted the first meeting in December 2021 of the Strategic Partnership Dialogue with the United States, highlighting the two countries' commitment to improving security in Central Asia.

The engagement in Tashkent was hosted by Uzbek Foreign Minister Abdulaziz Kamilov and U.S. Assistant Secretary of State for South and Central Asia Donald Lu.

Both parties stressed continued cooperation to counter the threats of terrorism and extremism and reduce insecurity in Afghanistan. Uzbekistan's loan of the Termez cargo terminal to help deliver international humanitarian aid to Afghanistan earned praise from the U.S. side.

The United Nations Office of High Commissioner for Refugees and the U.N. World Food Program have used the Termez hub to ship food, tents, dishes, blankets and other supplies to Afghanistan.

Washington agreed to host the next meeting of the Strategic Partnership Dialogue. The meeting, in 2022, could correspond with celebrations of the 30th anniversary of establishing diplomatic relations between Uzbekistan and the U.S.

Uzbek Foreign Minister Abdulaziz Kamilov, left, meets in Washington, D.C., with U.S. Secretary of State Antony Blinken in 2021. AFP/GETTY IMAGES

Uzbekistan and U.S. relations have improved during the six-year administration of Uzbek President Shavkat Mirziyoyev and have included a broadening of military cooperation and training. **Sources: Anadolu Agency, Gazeta.uz, Caravanserai**

UAE PROMOTES CYBERSECURITY

UNIPATH STAFF

United Arab Emirates company Majid Al Futtaim Retail, among the top supermarket retailers in the Middle East, South Asia and North Africa, earned top honors for following best practices in cybersecurity.

During Gulf Information Technology Exhibition (GITEX), a consumer trade show in Dubai in October 2021, Majid Al Futtaim was singled out by Trend Micro Inc. for its efforts at securing its chain of hundreds of grocery stores. Majid is franchisee and operator for the French-based Carrefour chain.

Trend Micro said Majid is responsible for protecting more than 10,000 computers, laptops and mobile devices and 2,500 servers from intrusions by hackers and criminals.

"These last five years have been nothing short of spectacular in protecting Majid Al Futtaim Retail's digital transformation journey. ... We are honored to be part of this journey," said Dr. Moataz bin Ali, vice president and managing director for Trend Micro.

Established by Majid Al Futtaim in 1992 and named after him, the company is a Dubai-based Emirati holding company that operates shopping malls and leisure establishments in addition to the deal with Carrefour.

Trend Micro Inc. is a U.S.-Japanese multinational cybersecurity software corporation headquartered in Tokyo, Japan, and Irving, Texas, United States.

Aware of growing cyber threats worldwide, the UAE exerts considerable efforts to stay ahead of the curve in addressing potential cybersecurity threats. Dr. Mohamed Al-Kuwaiti, advisor to the Emirati government on cybersecurity, urged vigilance during the International Government Communication Forum 2021 held in Sharjah in September 2021.

Al-Kuwaiti advocated information sharing among national cybersecurity task forces to raise awareness of the need to protect devices in the governmental and private sectors.

Attended by 79 experts from 11 countries, the two-day International Government Communication Forum 2021 promoted the exchange of expertise and strategies on protecting rapidly evolving global communications.

Sources: Emirates News Agency, Al Ittihad, Zawya.com

Pakistani security forces display a record cache of Afghan heroin seized at the Torkham border post.
AFP/GETTY IMAGES

Pakistan, U.S. Seize Tons of Illegal Drugs From Afghanistan

UNIPATH STAFF

The Pakistani government has reported record seizures of illegal drugs at one of the country's main border crossings with Afghanistan.

In just a few weeks in December 2021 and January 2022, Pakistani officials at the Torkham border post disrupted the smuggling of 524 kilograms of hashish, 255 kilograms of heroin, 280 kilograms of opium, and almost 22 kilograms of methamphetamine.

On January 6, 2022, Pakistan discovered two separate caches of heroin, one amounting to 100 kilograms, the other 130 kilograms. The latter seizure represented a record at Torkham. Acting on a tip, the Pakistanis discovered the heroin at Torkham's import terminal hidden inside a truck, said Ahmad Raza Khan, chief collector of customs in Peshawar.

Pakistan's Anti-Narcotics Force has also seized large amounts of illegal drugs across the country. In late December the agency announced it had intercepted 2.2 tons of drugs, including heroin and methamphetamine, followed by more than 3 tons in the first part of January.

Drugs from Afghanistan are arriving in "huge quantities," said Azlan Aslam, an official with the Department of Excise, Taxation and Narcotics Control in Khyber Pakhtunkhwa province. The rise is occurring despite promises by the recently installed Taliban Afghan government to suppress the illegal trade.

Afghanistan remains the source of almost all the world's opium and heroin. It is also a major player in methamphetamine and hashish production. Caches of Afghan drugs have also multiplied in Iran, Southeast Europe and Turkey.

In December 2021, the U.S. Navy seized 385 kilograms of heroin from an Iranian boat in the Arabian Sea. Two weeks earlier a U.S. patrol rescued five Iranian sailors from a burning dhow in the Gulf of Oman. The Iranians had set the fire to destroy evidence of their crimes, but U.S. Sailors still retrieved 1,750 kilograms of hashish, 500 kilograms of methamphetamine and 30 kilograms of heroin.

Sources: TRT World, U.S. Navy, Daily Pakistan

Omani Armed Forces Battle Cyclone Shaheen

UNIPATH STAFF

Preemptive action by the Sultan's Armed Forces saved the lives of potentially hundreds of Omanis residing in the path of Cyclone Shaheen in October 2021.

Omani authorities rescued more than 600 people as the storm hit the country with winds of up to 150 kilometers per hour and waves approaching heights of 10 meters.

People wade through a flooded street in the aftermath of Cyclone Shaheen in Oman's northern town of al-Mussanah in October 2021.
AFP/GETTY IMAGES

To diminish casualties from the approaching cyclone, Omani Internal Security Service halted traffic in the governorates of Al Batinah North and Al Batinah South, restricting movement to emergency cases and deliveries of vital goods. Power was cut as well in al-Qurm, east of Muscat, to avoid accidents, and more than 2,700 people were directed to emergency shelters.

Omani authorities furloughed public employees and postponed flights to and from Muscat International Airport until the cyclone had passed. Rainfall amounted to 369 millimeters in Al-Khaboura, northwest of the capital city, Muscat.

His Majesty Sultan Haitham bin Tariq created a ministerial committee to assess property damage from the cyclone. Oman's friends in the region responded as well. After a phone call from Omani Deputy Prime Minister for Defense Affairs Shihab bin Tariq, Kuwait dispatched military assets to Oman.

His Majesty King Abdullah II ibn Al Hussein of Jordan phoned Sultan Haitham bin Tariq, extending his condolences and sympathy and professing support for the Omani people.

Sources: BBC, Reuters, alkhaleejonline

KAZAKHSTAN'S STRATEGIC PARTNERSHIP WITH U.S.

UNIPATH STAFF

As part of an expanding diplomatic and security partnership, high-ranking diplomats from Kazakhstan and the United States committed their countries to further cooperation on counterterrorism, nuclear nonproliferation and border security.

The December 2021 meeting in the Kazakh capital of Astana occurred between Kazakh Deputy Foreign Minister Akan Rakhmetullin and U.S. Assistant Secretary of State for South and Central Asian Affairs Donald Lu.

Lu expressed gratitude to Kazakhstan on behalf of the U.S. for its strong cooperation in addressing challenges such as border security, counterterrorism, peacekeeping, nuclear nonproliferation, climate change and regional security.

He commended Kazakhstan for its leadership in repatriating foreign fighters and their families from war zones and vowed to continue bilateral cooperation on rehabilitation and reintegration of these individuals.

Both parties emphasized Kazakhstan's global leadership in containing the spread of nuclear weapons. The U.S. reiterated its long-standing commitment to aid Kazakhstan in eliminating radioactive waste from the Semipalatinsk nuclear test site, a holdover from the days of Moscow's domination of the region.

Both diplomats expressed support for deepening relations between their respective militaries, border and customs agencies and law enforcement. They intend to do that through the Fourth Five-Year Military Cooperation Plan between the Kazakh Ministry of Defense and the U.S. Department of Defense.

Sources: Baige News, Voice of America

Saudi Soldier Abeer Abdullah al-Rashed attends a news conference discussing security at the annual hajj in Mecca. REUTERS

Saudi Women Proudly Enlist in Military

UNIPATH STAFF

Making history, the first batch of female Saudi Soldiers graduated from the Armed Forces Women's Cadre Training Center of the Saudi Arabian Armed Forces in September 2021 after 14 weeks of boot camp.

"The daily training program begins with the early morning inspection, then starts a physical training period under the supervision of the fitness trainers, then trainees get dismissed for breakfast, then start field training. Once done, the theoretical classes start," trainer Manahil bint Saleh bin Humaid said.

The plan to allow Saudi women into the military was announced in 2019, though the first female Soldiers didn't appear in public until deployed as guards in Mecca during the July 2021 hajj.

"One of the reasons that prompted me to join the Armed Forces is the feeling of security I get when I see men in uniform stand guard at public places providing security," one female military graduate said. "And so when I was given the opportunity to contribute to that sense of security, I wasted no time."

During the graduation ceremony, Maj. Gen. Adel bin Muhammed Al-Belwi, head of the Saudi Armed Forces Training and Indoctrination Directorate, delivered a speech in which he outlined the function of the Women's Cadre Training Center.

Saudi Arabia's Vision 2030 includes the promotion of gender equality. Saudi decision-makers ruled that the principles of contemporary women's rights are consistent with those guaranteed by Islamic law.

Even more ambitiously, in 2018 the kingdom opened up positions for women within the General Security Directorate, the Ministry of Interior, and in seven of Saudi Arabia's 13 regions: Riyadh, Mecca, al-Qassim, al-Madina, Assir, Ash-Sharqiya and Al-Baha. Since then, female workforce participation has grown.

Sources: CNN, Al Jazeera, Reuters

Kuwait Considers Opening Door to Female Soldiers

UNIPATH STAFF

In a move to boost military recruitment, the Kuwait Armed Forces is studying the benefits of allowing women to serve in the military.

Maj. Gen. Khaled Al-Kandari, deputy chief of staff for manpower, announced that the study on female recruitment is scheduled for the end of 2021.

The debate on whether to enlist women in the Armed Forces was revived in September 2021 during a recruitment campaign, launched by the Kuwaiti Ministry of Defense, called "Be Among Them."

Kuwait considered a similar move in 2018, when Sheikh Nasser Al Sabah, then Kuwait's minister of defense, advocated admitting women to military service. "There is no objection to women joining the national military service if they so desire," Sheikh Nasser said at the time.

Women already serve in other Kuwaiti security services, but the Army remains a holdout. Women began training to be police officers in 2008 with an inaugural class of 40. In March 2016, the first five Kuwaiti policewomen joined security forces as guards at Kuwait's National Assembly.

Arabian Gulf states' effort to empower women has been making progress slowly yet steadily as women have begun assuming posts that were once the preserve of men in the military and security apparatuses.

First Lt. Sarah Al-Sarraf stands at her post outside the Kuwaiti National Assembly. AFP/GETTY IMAGES

More than 30 years ago, the Bahrain Defense Force allowed women to serve in several military branches, and some have achieved high ranks. In 2009, two Bahraini servicewomen made history by graduating from the Command and General Staff Program as staff officers at the Royal Command, Staff and National Defense College in Bahrain.

The United Arab Emirates hosts the Gulf region's first military college for women, Khawla Bint Al Azwar Military School, open since 1991. Women in Qatar were allowed to volunteer for national service for the first time in 2018.

Sources: Al Jazeera, Al Hurra

Tajikistan and Uzbekistan: Defeating Terrorism a Joint Responsibility

UNIPATH STAFF

In a boost to regional security in Central Asia, Tajikistan's parliament ratified agreements with Uzbekistan to cooperate on air defense and military intelligence.

The agreements were signed during the official visit to Tajikistan by Uzbek President Shavkat Mirziyoyev in June 2021, but achieved final Tajik approval in December 2021.

In terms of air defense, both countries agreed to share best practices in aviation and air defense, conduct joint training, assist each other's aircraft in distress, and exchange information about air traffic.

Intelligence-sharing will entail mostly exchanging information about suspected terrorists and religious extremist groups. Information includes terrorists sponsors and accomplices as well as weapons, training camps and terrorist bases.

Tajikistan and Uzbekistan also agreed to warn one another about heightened terrorist threats, including those against the sovereignty and territorial integrity of both countries. Aiding cooperation further, the agreement provides for holding joint military exercises for combat and intelligence units.

A third agreement focuses on sharing airspace and airfields, providing a mechanism for aircrews from one country to cross into the other country's airspace during disasters and emergencies. That agreement is valid for five years.

Tajikistan and Uzbekistan have improved diplomatic and security ties since President Mirziyoyev took office in 2016.

Sources: Asia Plus, Eurasia Daily, Radio Free Europe/Radio Liberty

IRAQIS SECURE PARLIAMENTARY ELECTIONS

UNIPATH STAFF

A joint effort by hundreds of thousands of Iraqi police officers and military personnel helped secure early parliamentary elections across the country in October 2021.

Employees of the Iraqi Independent High Electoral Commission count parliamentary ballots in Baghdad in October 2021.
AFP/GETTY IMAGES

The Iraqi Ministry of Interior reported no terrorist attacks, accidents or security breaches, despite the absence of a curfew imposed in previous elections.

The plan for securing the election included the deployment of 300,000 members of the Army, police, Air Force, Military Aviation and civil defense. Aerial surveillance helped ensure that many of Iraq's 8,278 polling centers were protected from potential terrorist attacks.

"This election is fundamentally different from all previous elections ... which made it nearly or completely consistent with international standards," said Brig. Gen. Ghaleb al-Attiyah, a spokesman for the Iraqi Election Supreme Security Committee.

An estimated 9 million Iraqis out of 25 million eligible voters cast ballots, choosing from among 3,200 candidates belonging to 167 parties competing for 329 parliamentary seats.

Iraq originally planned the election for 2022, but Prime Minister Mustafa al-Kadhimi moved up the vote in response to public protests demanding jobs and improved public services. A new election law streamlined voting and provided for greater parliamentary representation by Iraqi minority groups and women. **Sources: Reuters, BBC, Al Jazeera**

Qatar Bolsters Military-to-Military Partnership with Turkey

UNIPATH STAFF

The Qatari Emiri Navy fortified its fleet with the ceremonial launch of a landing craft that can accommodate hundreds of troops on its broad deck.

The landing craft tank (LCT) Fuwairit was officially completed by Turkey's Anadolu Shipyard in September 2021.

Named after a coastal village in Qatar, the LCT Fuwairit holds 260 fully equipped troops on its 400-square-meter deck. The landing craft, operated by 25 Sailors, is also equipped to carry three battle tanks and other vehicles.

Qatar planned to accept delivery of the vessel — one of about six ships it is buying from Turkey — in the summer of 2022.

"We intend to complete all tests and training sessions over the next 24 months and deliver them to Qatar," Cevat Rifat Atilhan, CEO of Anadolu Shipyard, said of the multiple ship purchase.

In addition to landing craft, Qatar has ordered several ships from the Anadolu Shipyard on which to train cadets from the Qatari Naval College. The country possesses a 563-kilometer coastline in the Arabian Gulf.

The purchases are part of a joint defense agreement that Qatar concluded with Turkey in 2017. To bolster their military-to-military relationship, the two countries founded the Turkey-Qatar Combined Joint Force in 2019. It is headquartered in Doha and named for the seventh century Arab battle commander, Khalid bin Al Waleed.

The Qatar Emiri Air Force attended Anatolian Eagle, a two-week multinational exercise, in Konya in the summer of 2021. Pilots practiced maneuvering in the Qatar's newly purchased French-built Rafale jet fighters from the 1st Fighter Wing at Tamim Air Base.

Under a technical agreement signed by the militaries of the two countries, Qatar will train pilots in Turkey for five years and station up to 250 personnel and 36 aircraft in the country.

Sources: Naval News, Al Jazeera, ahvalnews.com

Jordan Approves Security Agreement with Qatar

UNIPATH STAFF

Jordan and Qatar entered into a five-year security cooperation agreement in September 2021 that focuses on exchanging intelligence and technology to fight crime.

The two countries will work to promote existing bilateral cooperation to combat all kinds of crimes: terrorism and related financing; organized crime; illicit trafficking in arms, ammunition, explosives and nuclear, radioactive, chemical and biological materials; human trafficking and illegal migration; smuggling, production and distribution of narcotics; money laundering; and counterfeiting of passports, currencies and other official documents.

From an economic perspective, the agreement also emphasized joint protection of intellectual property, technological assets, information systems, and ports and borders. The agreement also cites cooperative efforts against maritime piracy and cybercrime.

Qatari Foreign Minister Mohammed bin Abdulrahman Al-Thani, left, and Jordanian Foreign Minister Ayman Al Safadi participate in a news conference in Amman in August 2021. REUTERS

Qatar and Jordan have maintained robust diplomatic and military relations since Qatar gained independence in 1971. Jordanian experts aided Qatar's economic, educational and military sectors.

His Majesty the late King Hussein bin Talal of Jordan was the first global leader to visit Qatar and congratulated His Highness Sheikh Hamad bin Khalifa Al Thani on his assumption of power in Qatar in 1995.

His Majesty King Abdullah II of Jordan was the first Arab leader to visit Doha to congratulate His Highness Sheikh Tamim bin Hamad Al Thani on his nomination as Qatar's emir in June 2013.

Jordanian and Qatari militaries regularly participate in joint exercises. Qatari special operations forces participated in the multinational military exercise Eager Lion in Jordan in September 2019, while Jordanian forces, along with forces from seven other nations, took part in Invincible Sentry in Qatar in March 2021.

Sources: Jordan News Agency, ammonnews.net, alaraby.co.uk

Egypt and Cyprus Solidify Partnership

UNIPATH STAFF

Egypt and Cyprus confirmed their close military partnership by successfully concluding the Ptolemy 2021 military exercise in September.

The exercise included marksmanship practice, close quarters combat drill, simulated raids on terrorist hideouts and medical evacuation. The joint participation ensured that Egypt and Cyprus could test combat interoperability.

Egypt and Cyprus enjoy robust military relations. Cypriot troops — including naval and special operations forces — were major players in the two-week multinational Bright Star exercise hosted by Egypt at Mohamed Naguib Military Base in September 2021.

"Relations on a personal level and at the level of the Armed Forces of Egypt and Cyprus are excellent and fraternal," Cypriot Armed Forces Chief of Staff Lt. Gen. Democritos Zervakis said at a meeting with his Egyptian counterpart at the time.

In addition, Egypt, Cyprus and Greece hold tripartite summits to discuss partnership and collaboration in tackling issues related to the eastern Mediterranean Sea, including demarcation of shared maritime borders and exclusive economic zones.

As recently as September 2021, Egyptian and Cyprus held a presidential summit in Cairo featuring Egyptian President Abdel-Fattah el-Sisi and Cypriot President Nicos Anastasiades. Security, diplomacy, trade, tourism and agriculture were highlighted on the agenda.

"The strategic partnership we have established in the eastern Mediterranean requires constant coordination to achieve regional stability and commitment to exchange support on all issues of common interest," President el-Sisi said.

Sources: Al Ahram, defensearabia.com, egypttoday.com

BAHRAIN DRIES UP TERRORIST FINANCING

UNIPATH STAFF

Bahrain ranked best among Arabic-speaking nations with the lowest incidence of money laundering, according to the Basel Anti-Money Laundering Index 2021.

The Swiss-based organization based its ranking upon data provided by the Financial Action Task Force, Transparency International, the World Bank and the World Economic Forum.

"The kingdom achieved 4.5 points and came in the second place after Israel, among the Middle Eastern countries in the area of combating money laundering, but came in first in the Arab world," said Sheikh Salman bin Isa Al Khalifa, deputy governor of the Central Bank of Bahrain.

In July 2021, Bahrain's High Criminal Court convicted six officials from the Bahrain-based Future Bank. Each was sentenced to 10 years in prison and a $2.5 million fine for involvement in money laundering benefiting the Central Bank of Iran (CBI).

Sheikha Mai bint Muhammad Al Khalifa, director of the Financial Intelligence Department at the Ministry of Interior, said her agency seeks to enhance Bahrain's standing regionally and internationally in combating money laundering and terrorist financing.

Future Bank was accused of processing suspicious transactions for Iranian financial entities, including CBI, in violation of Bahraini laws and regulations. The value of the transfers — made in multiple currencies — amounted to more than $1 billion.

Sources: baselgovernance.org, alkhaleejonline.net.

Bahrain's financial district in Manama

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 CENTCOM.UNIPATH@MAIL.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 us at CENTCOM.UNIPATH@MAIL.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.

HTTPS://UNIPATH-MAGAZINE.COM