موفقیت قطر در
نجات پناهندگان

دفاع قوای بحری
اردن از آبراه‌ها

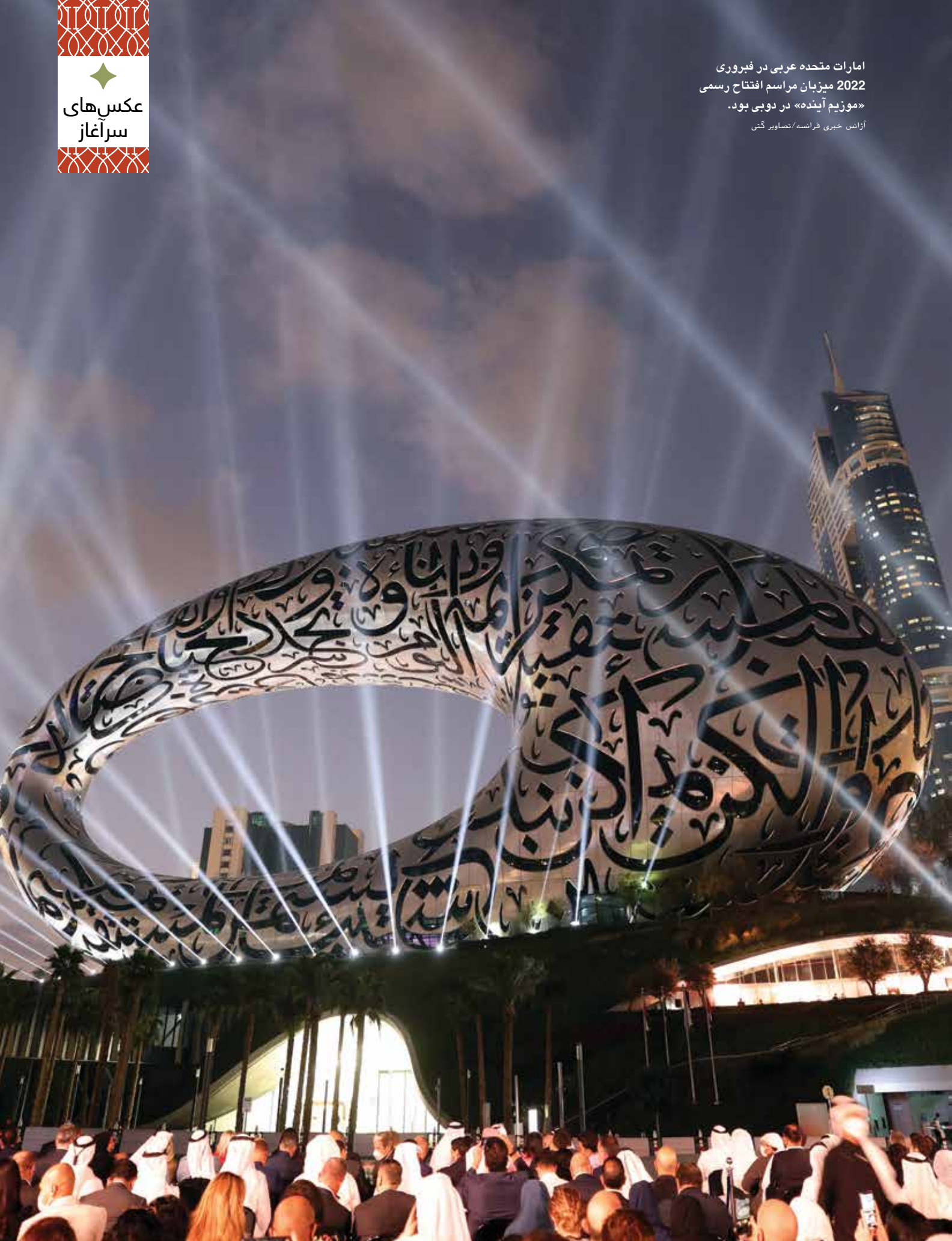
محافظت از
تمامیت ارضی یمن

UNIPATH

تأمین امنیت فضای مجازی

حضور زن قزاق در مراسم بزرگداشت نوروز یا اعتدال بهاری که در مارچ 2022 در آلماتی برگزار شد رویترز

عکس‌های
سرآغاز



امارات متحده عربی در فبروری 2022 میزبان مراسم افتتاح رسمی «موزیم آینده» در دوبی بود.

آژانس خبری فرانسه/تصاویر گتی

فهرست مندرجات

6 **دفاع گروپی: دیدگاه یکی از قوموندانان سایبری ایالات متحده**
دگر جنرال چارلز مور، معین قومندان قرارگاه سایبری ایالات متحده

8 **خشونت مجازی**
تروریستان، مجرمین و دولت‌های نابکار از فضای مجازی منحیث میدان جنگ برای بی‌ثبات ساختن جامعه استفاده می‌کنند.
ائتلاف اردوهای اسلامی برای مبارزه با تروریزم

12 **استفاده از کلمات منحیث سلاح**
اتحادیه رادیویی و تلویزیونی اسلامی که با حمایت ایران اداره می‌شود، نشر معلومات غلط برای تضعیف همبستگی اجتماعی را در دستور کار قرار داده است.
تورن جنرال متقاعد عودا شدیفات، مشاور رسانه‌ای و فرهنگی، قومندان کل، قوای مسلح اردن/اردوی عرب

14 **اعتمادسازی بحرین برای مقابله با انتشار معلومات غلط**
این کشور در میدان جلوگیری از شیوع همه‌گیری کووید-19 به جنگ معلومات ترس‌آور انترنتی رفت.
حبیب طومی، مشاور وزارت معلومات بحرین

18 **تعهد به امنیت سایبری**
محافظت از عراق در مقابل تهدیدات سایبری مستلزم تقویت امکانات عراق در حوزه تکنالوجی است.
داکتر حسین علاوی، مشاور صدراعظم عراق در امور اصلاحات بخش امنیتی

20 **قزاقستان و سپر سایبری**
پروگرام قزاقستان بالای محافظت از سیستم‌ها در مقابل هکرها و مجرمین متمرکز است.
سلطنت بردیکیوا

24 **کوشش مشترک، به رهبری قطر، برای نجات ده‌ها هزار افغان**

30 **تقویت شبکه‌های نظامی**
وزارت دفاع عراق یک گروپ امنیت سایبری برای شناسایی و مقابله با حملات سایبری ایجاد کرد.

34 **دفاع از تمامیت ارضی یمن**
دخالت ایران مانع رسیدن یمنی‌ها به توافق سیاسی برای خاتمه دادن به جنگ داخلی میباشد.
داکتر احمد عواد بن مبارک، وزیر خارجه، یمن

38 **محافظت از اموال دیجیتل پاکستان**
این کشور اولین پالیسی ملی امنیت سایبری را برای تقویت شبکه‌ها در مقابل حملات سایبری انکشاف داد.

40 **ضرورت تقویت اقدامات معلوماتی**
عصام عباس امین، اداره استخبارات و امنیت، وزارت دفاع عراق

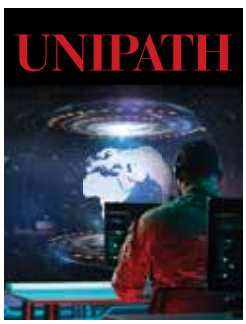
44 **آماده‌باش قوای بحری**
مصاحبه با دگروال هشام خلیل الجراح، قومندان قوای بحری سلطنتی اردن.

50 **رویکرد لبنان به امنیت سایبری**
اداره امنیت سایبری قوای مسلح لبنان خود را برای مقابله با تهدیدات آماده می‌سازد.

52 **نقش مرکز امنیت دریایی عمان**

54 **شرح حال رهبری ارشد**
دگر جنرال قیس خلف رحیمه، معین رئیس ارکان عملیات قوای مسلح عراق و قومندان قومانداني عملیاتهای مشترک عراق

58 **ماورای منطقه**



روی جلد:
اردوها، در راستای ایفای وظایف دفاعی خود، باید از جامعه در مقابل حملات سایبری و جذب قوای تروریست به کمک انترنت، محافظت کنند. تصاویر یونیپاث

UNIPATH

تأمین امنیت فضای مجازی

دوره 11، نمبر 4

قوماندان سنتکام

جنرال مایکل اریک کوریلا اردوی ایالات متحده امریکا

با ما در تماس شوید

Unipath
c/o Commander
U.S. Central Command
7115 S. Boundary Blvd.
MacDill AFB, FL 33621
USA
CENTCOM.
UNIPATH@MAIL.MIL

ISSN 2333-1844 (چاپ)
ISSN 2333-1852 (آنلاین)

پیام رهبر کلیدی

می‌خواهم از قومندانی مرکزی ایالات متحده به خاطر فراهم نمودن فرصت نوشتن این مقاله این شماره مخصوص مجله یونیپاث که به محافظت از فضای مجازی اختصاص دارد، تشکر کنم.

با پیشرفت دنیا و گسترش تکنالوژی، احتمال ایجاد اختلال در سرورهایی که تهداب‌های آنلاین را کنترول می‌کنند، افزایش می‌یابد. این شامل خدمات ترانسپورتی، برق، گاز، تصفیه‌خانه‌ها یا خدمات مالی بانکها، بورس اوراق بهادار و مراکز مالی است که در معرض حوادث ساختگی یا طبیعی قرار دارند. وقوع چنین رویدادهایی هراس‌آور است و عملاً می‌تواند دنیا را به عصر حجر بازگرداند.

ازکارافتادگی سرورهای متعلق به غول‌های تکنالوژی، سایت های شبکه‌سازی اجتماعی و پروگرام‌ها نشان‌دهنده آسیب‌پذیری دنیا و احتمال ایجاد احساس تنهایی، انزوا و پوچی در مردم دنیاست. این موضوع میزان اتکای ما به شبکه‌های اجتماعی را نشان می‌دهد. این وابستگی باعث قرار گرفتن ما در معرض تهدیدات خطرناک و ایجاد وضعیت «بودن یا نبودن» در مقابل تهدیداتی که باید برای دفع آنها آماده باشیم، می‌شود.

شاید همه‌گیری ویروس کرونا و عواقب مرگبار آن به دلیل ایجاد الزاماتی ازقبیل فاصله‌گذاری اجتماعی، گرایش به تعلیم از دور و نشر گسترده پروگرام‌های تصویری، صوتی و غیره، باعث شیوع ترس بین انسان‌ها شده است. این وضعیت تشویش‌ها درباره محافظت از فضای مجازی را افزایش داده است: امنیت سایبری در تقابل با خود طبیعت به جنگ بقا برای حفظ صحت انسان‌ها مبدل شده است.

دنیا باید برای مقابله با این سناریوها آماده باشد و آنها را جنگ جهانی قلمداد کند. نقش اردوها دیگر به مقابله با تهدیدات بالقوه محدود نمی‌شود بلکه بررسی روندها و مسیرها و تدوین پلان‌های مناسب برای پیش‌بینی تهدیدات نوظهور و مهم‌تر از همه، محافظت از فضای مجازی مربوط به تمدن بشری را نیز شامل می‌شود. این موضوع به مساله بقا تبدیل شده است: ما باید با هر وسیله‌ای که لازم باشد از فضای مجازی محافظت کنیم.

جنگ سایبری شامل جاسوسی از کشورها، سرقت اسرار تجاری و نظامی، حمله به کمپیوترهای مسئول کنترول تهداب‌های اساسی و سیستم‌های تسلیحات، نفوذ به معلومات حیاتی امنیتی و اقتصادی و هدف گرفتن سرویس‌های حیاتی یا امنیت ملی کشورهای متخاصم است.

این سبک نوظهور از جنگ میدان‌های جنگ زمینی، هوایی و دریایی را فرا گرفته است. مقابله با این حملات مستلزم مساعی مستمر همه موسسات دولتی و همکاری در قالب یک سیستم قدرتمند دفاعی و مقاوم در مقابل نفوذ، است.

دانش بشری طی دهه‌ها و قرون گذشته چندین برابر شده است. حالا، به کمک انقلاب معلوماتی، این تکثیر هر ساعت رخ می‌دهد و این پیشرفت مستمر و سریع که هر روز در جهان دیده می‌شود، باعث شکل‌گیری تهدیدات و فرصت‌های مختلفی می‌شود.

این ویژگی عصر دیجیتل گرایش بعضی دولت‌ها، سازمان‌ها و اشخاص به سوءاستفاده از تکنالوژی، استفاده مخرب از آن با نقض صریح حقوق بشر و پیمان‌ها و منشورهای بین‌المللی و سوءاستفاده از فقدان اجماع بین‌المللی را در قبال دارد. این وضعیت ایجاب می‌کند که موسسات جامعه بین‌الملل مسئولیت محافظت از دستاوردهای تکنالوژیکی و مقابله با اقدامات بدخواهانه دولت‌ها و اشخاص را به عهده بگیرند و برای ایجاد نهاد مسئول تفتیش قانون‌شکنی دولت‌ها، سازمان‌ها و/ یا اشخاص سعی کنند و چنین اشخاصی را بربنیاد قانون بین‌المللی محاکمه و مجازات کنند.

در کشور کویت، ما موضوع محافظت از فضای مجازی را جدی می‌گیریم. شورای وزیران، در جلسه مورخ 31 می 2021، با ایجاد «مرکز ملی امنیت سایبری» موافقت کرد و وزیر خارجه و وزیر امور کابینه را مامور تهیه مسوده حکم اعلان رسمی ایجاد مرکز کرد. این اقدامات با هماهنگی تعدادی از وزارتخانه‌ها و موسسات دولتی فعال در این حوزه صورت خواهد گرفت.

این مرکز مدیریت هماهنگ‌سازی و یکپارچه‌سازی مساعی موسسات دولتی برای محافظت از فضای مجازی در مقابل حملات احتمالی ناشی از آشفتگی سایبری سراسری را به عهده دارد.

همچنان، همه موسسات داخلی مکلف شده‌اند که هدفی تدبیری حفظ امنیت شبکه‌ها و هدف ستراتیژیک محافظت از فضای مجازی دولتی و فعالیت منحیث ذینفع مشترک، تحت نظارت مرکز ملی امنیت سایبری، را پیگیری کنند.

در سطح وزارت دفاع، همکاری بین اردوی کویت و قوماندانی مرکزی ایالات متحده در حوزه تکنالوژی امنیت معلومات یک نمونه از همکاری مطلوب بین‌المللی است. کورس‌های تعلیمی منظم، ورکشاپ‌ها و فعالیت‌های مشترکی برای مقابله با مخاطرات و محافظت از سیستم‌های امنیت معلومات و شبکه‌های داخلی در جریان است.

حفظ امنیت سایبری وظیفه یک کشور نیست، بلکه این وظیفه را باید ائتلافی از شرکای بین‌المللی صاحب تکنالوزی و دانش مقابله با تهدیدات روزافزون سیستم‌های کمپیوتری حیاتی مرتبط با تمدن جهانی و بشری، به عهده بگیرند.

تورن جنرال محمد اقلع العنزی، قومندان فرقهٔ نمونه اردوی کویت

دفاع گروپی:

دیدگاه یکی از قومندانان سایبری ایالات متحده

دگر جنرال چارلز مور، معین قومندان قرارگاه سایبری ایالات متحده

در نومبر 2020، بیش از 158 ملیون امریکایی در انتخابات ملی ما اشتراک نمودند. ازآنجا که اشتراک در انتخابات برای جمهوری دموکرات ما بسیار مهم است، مردم امریکا باید مطمئن شوند که پروسه‌ها و نتایج انتخابات در مقابل دخالت‌های خارجی مصئونیت دارد و اقدامات خارجی برای اعمال نفوذ در تصمیم رای‌دهندگان بی‌فایده می‌ماند. چهار سال قبل، بازیگران مخرب سایبری با اجرای عملیات در فضای مجازی قصد اعمال نفوذ در تصمیمات رای‌دهندگان را داشتند.

دگرمن جنرال چارلز مور

با هدف جلوگیری از فعالیت‌های مشابه با وقایع انتخابات ملی 2018 و 2020، نهادهای دولتی ایالات متحده گروپی چند-کارکردی و متنوع را برای شناسایی تهدیدات، تبادل معلومات و هماهنگ‌سازی اقدامات تشکیل داده‌اند. از این نهادها می‌توان به اداره امنیت سایبری و امنیت تهداب‌ها، اداره تحقیقات فدرال، اداره امنیت ملی و قرارگاه سایبری ایالات متحده (USCYBERCOM) اشاره کرد.

ضمناً، این گروپ برای پیشبرد اقدامات خود از کشورهای همکار و شرکای صنعتی کمک می‌گیرد. این یک نمونه از نوع دفاع گروپی است برای محافظت از پروسه‌های دموکرات و تمام ملت مورد ضرورت است.

برای دفاع از ملت در حوزه فضای سایبری، قرارگاه سایبری ایالات متحده استراتیژی «دفاع رو به پیش» و رویکرد عملیاتی را انتخاب نموده است. ازآنجا که حوزه فضای مجازی ماهیتاً جهانی است، بیشتر تهدیدات ملی از فضای مجازی خارجی یا همان فضای سرخ نشات می‌گیرد. مقابله با تهدیدات قرن 21 مستلزم سرعت و چالاکی -و همکاری- برای رهگیری و شناسایی دشمن در فضای سرخ، قبل از وقوع اقدامات خصمانه علیه ایالات متحده و سیستم‌های یکپارچه داده، سیستم‌های تسلیحات و شبکه‌ها، است.

به بیان ساده، به‌جای فرار از مقابل مرمی‌ها، باید با کسی که فیر می‌کند، مقابله کنیم. معلومات که در جریان عملیات‌ها جمع‌آوری می‌شود بین نهادها و همکاران و هم‌پیمانان به اشتراک گذاشته می‌شود تا امکان رسیدن به آگاهی موقعیتی مشترک از تهدیدات احتمالی، پیشبرد مساعی مشترک، و زمینه‌سازی برای عکس‌العمل یک‌پارچه و هماهنگ فراهم شود.

همانند مساعی ما در دیگر حوزه‌های جنگ، وحدت لازمه موفقیت ما در فضای مجازی، و کار گروپی بخش مهمی از این فعالیت است. از این رو، مشارکت این‌چنینی از پرزه‌جات اجزای اساسی ستراتیژی دفاع ملی ایالات متحده و رویکرد ستراتیژیک قرارگاه سایبری ایالات متحده است. ازآنجاکه فضای مجازی همه جنبه‌های جامعه مدرن را پوشش داده است، دفاع از آن را «ورزش گروپی اساسی» نامیده‌اند. ایجاد، پیشبرد و تقویت همکاری در سطح دولت برای وارد کردن هم‌پیمانان، صنایع و محافل پوهنتونی به اقدامات مستمر و گروپی ضروری است.

یکی از شگردهای قرارگاه سایبری ایالات متحده برای ایجاد مشارکت در چوکات دفاع گروپی، استفاده از عملیات شکار آینده‌نگر (HFO) است. ما،

یک امریکایی که می‌خواهد در نیویارک در انتخابات 2020 اشتراک کند. تامین امنیت انتخابات در مقابل دخالت بیگانگان بخشی از ماموریت قرارگاه سایبری ایالات متحده است.

تصاویر گتی

به دعوت یکی از کشورهای همکار، گروپ‌های جنگجویان سایبری ماهر را که در قسمت شناسایی فعالیت‌های سایبری مخرب در شبکه‌های همکار تخصص دارند، فعال کرده‌ایم. در جریان این اقدامات، گروپ‌های سایبری ما به جمع‌آوری معلومات ارزشمند و شناسایی تهدیدات بالقوه در شبکه‌ها و آماده‌سازی کشور میزبان برای بهبود کیفیت دفاع و انعطاف شبکه‌ها می‌پردازند.

در ختم هر نوبت HFO، گروپ مرتبط راپوری درباره نقاط ضعف و ستراتیژی‌های وقایه از نفوذ به شبکه‌ها در اختیار کشور میزبان قرار می‌دهد. معلومات که گروپ درباره شگردها، شیوه‌ها و پروسیجرهای (TTP) دشمن جمع‌آوری می‌کند، به همراه مستندات مربوط به فعالیت‌های بدافزار برای نفوذ به سیستم‌ها در اختیار مسئولین بین‌المللی امنیت سایبری قرار می‌گیرد. در بعضی موارد، HFO نمونه سافتویرهای مخرب را برای معرفی عمومی در اختیار قرارگاه سایبری ایالات متحده می‌گذارد. به این‌ترتیب شبکه‌های داخلی و همکار می‌توانند برای مقابله با تهدیدات آینده آماده شوند. HFO از سال 2018 در قالب اقدامات دفاعی انتخاباتی شکل گرفت و حالا در سراسر جهان اجرا می‌شود.

از روش‌های دیگر تقویت همکاری‌های مربوط به دفاع گروپی، اجرای مانورهای سنجش کارآیی فعالیت گروپی و آمادگی است. همانند بسیاری از عملیات‌های نظامی، مهم است که کشورهای هم‌پیمان و همکار پیوسته برای شناسایی نقاط قوت و ضعف یکدیگر و TTP ها تعلیم ببینند. هدف ما فعالیت بی‌وقفه در کنار یکدیگر است.

در نومبر 2021، قرارگاه سایبری ایالات متحده میزبان کلانترین مانور ترکیبی و چندملیتی خود، به نام «بیرق سایبری 1-21» بود. این مجموعه مانورها برای سنجش و تقویت مهارت‌ها و قابلیت‌های دفاعی بیش از 200 جنگاور سایبری از 23 کشور طراحی شده بود. این جنگجویان در معرض سناریوهای پیچیده فضای سایبری قرار می‌گرفتند. ما، از طریق این مانورها، خصوصیات ائتلاف -سرعت، دقت، چابکی و وحدت عمل- را که برای دفاع گروپی از ملت ضروری هستند، تقویت می‌کنیم.

دفاع کافی در فضای مجازی مستلزم همکاری نزدیک با صنایع خصوصی است. قرارگاه سایبری ایالات متحده از طریق دو پروگرام اصلی با صنایع خصوصی تعامل دارد: Under Advisement و Dreamport.

Under Advisement پروگرام تبادل معلومات آشکار، داوطلبانه و موثر بخش خصوصی است. Dreamport مرکز نوآوری بدون طبقه‌بندی است که امکان تعامل قرارگاه سایبری ایالات متحده با فعالان صنایع و محافل دانشگاهی را با هدف تبادل افکار و ارائه راهکارهای خلاقانه برای مشکلات امنیت سایبری فراهم می‌کند. هر دو پروگرام نقش مهمی در تقویت توان قرارگاه سایبری ایالات متحده در دفاع از فضای مجازی کشور دارند و گستره و مقیاس آنها روز به روز کلانتر می‌شود.

Dreamport صرفاً یکی از راه‌های بهره‌برداری قرارگاه سایبری ایالات متحده از توان مراکز پوهنتونی است. قرارگاه چندی قبل «شبکه مشارکت علمی» را به کمک 91 موسسه تاسیس کرد. این شبکه امکان همکاری در قسمت ارائه راهکارهای نوآورانه برای چالش‌های تخنیکی و دیدگاه‌های تحلیلی جدید درباره بازیگران سایبری مخرب، و حمایت از اقدامات دفاع گروپی را فراهم می‌کند. این شبکه همچنان از قابلیت تقویت روند جذب نیروی بشری، از طریق معرفی فرصت‌های کاری به محصلین در حوزه‌های مهیج امنیت سایبری نظامی و ملکی، برخوردار است.

سرانجام، رسیدن به توان دفاع از شبکه‌های وزارت دفاع ایالات متحده و تمام کشور در مقابل بازیگران سایبری مخرب مستلزم انتخاب رویکرد گروپی است. این رویکرد گروپی باید با همکاری تنگاتنگ نهادهای دولتی، هم‌پیمانان ما، صنایع و مراکز علمی همراه شود.

توانایی ما برای تبادل بی‌وقفه و سریع معلومات، تعلیم مستمر و فعالیت گروپی و انکشاف رویکردهای نوآورانه برای همه چالش‌های امنیت سایبری برای رسیدن به توانایی اجرای موفق ماموریت تامین امنیت سایبری و دفاع در قرن 21 ضروری است. ✦

خشونت مجازی

تروریستان، مجرمین و
دولت‌های نابکار از فضای مجازی
منحیث میدان جنگ برای بی‌ثبات
ساختن جامعه استفاده می‌کنند

تصاویر یونیپاث

انترنت یک شبکهٔ بین‌المللی و غیرمتمرکز است که امکان ناشناس ماندن را فراهم می‌کند و می‌توان از آن منحیث یک سامان برای فعالیت‌های غیرقانونی، بشمول سرقت اموال و ترویج افراط‌گرایی خشن، استفاده نمود. با این دورنمای تیره -سوءاستفاده افراط‌گرایان و تروریستان از انترنت- دولت‌ها با چالش مقابله با مجرمینی که در پی تضعیف مشروعیت دولت و ارتکاب اعمال خشونت‌آمیز هستند، روبرو شده‌اند.

تروریزم سایبری تهدید ملی اساسی بسیاری از دولت‌هاست. به دلیل وابستگی جهانی به تکنالوژی معلومات، این پدیده با خسارات هنگفتی همراه است. اهداف اصلی تروریستان سایبری ممکن است دولت‌ها و موسسات وابسته، بانکها، تهداب‌های ارتباطی و خدمات عامه مانند شبکه‌های آب، برق، گاز و نفت باشد. حمله به این اهداف ممکن است خسارات کلان اقتصادی، سیاسی و مادی در پی داشته باشد.

گروپ‌های تروریستی سایبری ماهرتر و هماهنگ‌تر شده‌اند. آنها می‌توانند حملات خود را با استفاده از مزیت اتصال کمپیوترها به انترنت پیش ببرند. در نتیجه، تروریزم سایبری به تهدیدی برای سازمان‌های کلان و همه مستفیدان کمپیوتر تبدیل شده است.

عملیات‌های سایبری به دلایل مختلف برای تروریستان جذابیت دارد. این عملیات‌ها، در مقایسه با شیوه‌های تروریستی سنتی، مصرف کمتری دارند و صرفاً با یک کمپیوتر شخصی و اتصال انترنت قابل اجرا هستند. در این مورد، خرید سلاح و مواد انفجاری ضروری نیست. تولید و توزیع ویروس‌های کمپیوتری از طریق خطوط تلیفون معمولی یا ارتباطات بی‌سیم یکی از رایج‌ترین شیوه‌های تروریزم الکترونیکی است. تاثیر تخریبی این شیوه بالای سیستم‌ها همتراز بمب فزیکی است.

تعریف سلاح سایبری همچنان مبهم است. این سلاح محدوده‌ای نامشخص از کودهای پروگرام‌نویسی را که کاربرد مخرب دارند، اشغال می‌کند. برای ایجاد تمایز بین سلاح و ابزار، شخص باید نیت مجرم را که ممکن است ذریعه تخریب یا تهدید در پی تحمیل صدمه باشد، در نظر بگیرد. این بخش جدایی‌ناپذیر از تعریف سلاح سایبری است.

طرز مثال، چکش یک سامان است که کاربردهای مختلفی دارد. اگر از آن برای تحمیل صدمه جسمی یا مادی استفاده شود، می‌توان آن را سلاح خطرناک قلمداد کرد. این منطق را می‌توان درباره استفاده ازنرم‌افزار که، با وجود بی‌ضرر بودن در کاربردهای خاص، ممکن است منحیث سلاح مخرب مورد استفاده قرار بگیرد، اعمال کرد.

قدرت تخریب سلاح سایبری به وابستگی مردم به شبکه هدف بستگی دارد. بنابراین، تاثیر سلاح‌های سایبری که علیه تهداب‌های اساسی مانند شبکه برق‌رسانی به کار گرفته می‌شود، شدیدتر است.

این احتمال همواره وجود دارد که سازمان‌های تروریستی از این سلاح‌ها استفاده کنند. بطورمثال، گروپی به نام Shadow Broker بعد از هک کردن سیستم اداره امنیت ملی ایالات متحده مدعی شد که سلاح‌های سایبری ملی را با هدف حراج کردن آنها دزدیده است. این رویداد نشان داد که سلاح‌های سایبری را می‌توان همانند سلاح‌های سنتی به کمک «دلالان سلاح» مجازی معامله نمود.

نرم افزارهای مخرب عبارت فراگیری برای انواع نرم‌افزارهای است که با هدف تحمیل صدمه یا سوءاستفاده از دستگاه، سرویس یا شبکه قابل پروگرام طراحی می‌شوند. مجرمین سایبری عمدتاً از این نرم افزارها برای استخراج معلومات و کسب مفاد شخصی استفاده می‌کنند. معلوماتی مانند دوسیه‌های مالی و صحی، پیام‌های ایمیل و پسوردهای شخصی در معرض سرقت قرار دارند. انواع معلومات در معرض هک، بی‌شمار است.

نوع حملات

استفاده از حمله روزِ صفر -پیدا کردن آسیب‌پذیری نرم‌افزارهای کمپیوتری که تا فعلاً برای آن وصله ترمیمی ارائه نشده است- یکی از روش‌های فریب‌آمیز دسترسی به سیستم‌ها و مختل ساختن آنهاست. هکرها می‌توانند از نقاط ضعف برای دسترسی به معلومات مهم و ایجاد و به‌کارگیری نرم‌افزارهای مخرب و نرم افزارهای جاسوسی استفاده کنند.

حملات توزیع‌شده تکذیب سرویس، دزدی معلومات و دیگر انواع نفوذ را می‌توان از طریق باتنت انجام داد. باتنت یا بات ممکن است بشمول چندین دستگاه متصل به انترنت باشد؛ هر دستگاه یک یا چند بات را اجرا می‌کند. شخص مهاجم می‌تواند ربات‌ها را با نرم‌افزار فرمان و کنترول مدیریت کند.

ویروس‌ها بدنام‌ترین و قدیمی‌ترین نوع نرم‌افزارهای مخرب هستند. ویروس پروگرامی است که به کمپیوتر یا فایلها متصل می‌شود و، با تکثیر کردن خودش، کمپیوترها یا فایلهای دیگر را آلوده می‌سازد و از قابلیت تخریب یا حذف کردن معلومات برخوردار است. کمپیوتر زمانی آلوده می‌شود که پروگرام مخرب اجرا شود. ویروس نیز زمانی بیدار می‌شود که فایل یا پیوست آلوده باز شود. ویروس‌ها برای گردش و آلوده ساختن فایلها و سیستم‌های دیگر به عمل کاربر، طرز مثال اجرای پروگرام آلوده در لست پستی، ضرورت دارند.

تروریست‌ها قربانیان خود را اغلب با نوعی خرابکاری سایبری، به نام بمب شرطی، هدف قرار می‌دهند. در این روش، سافتویر مرتبط قسمی تنظیم می‌شود که عمل مخرب مورد نظر را در صورت پوره شدن شرایط معین انجام دهد. بمب شرطی را می‌توان برای مصارف کم‌ضررتر مانند پروگرام‌های آزمایشی

شناسایی پلتفرم‌های افراط‌گرا در شبکه‌های اجتماعی

ائتلاف اردوهای اسلامی برای مبارزه با تروریزم

شبکه‌های اجتماعی آنلاین به سامان‌های غالب ارتباطی تبدیل شده‌اند: فیس بوک به تعداد ملیاردی مستفیدان خود می‌بالد، یوتیوب 2.2 ملیارد، واتساپ 2 ملیارد، مسنجر 1.3 ملیارد و اینستاگرام 1.2 ملیارد مستفید دارند. هر ماه حدود 4 ملیارد مورد ارتباط در این پلتفورم‌ها برقرار می‌شود.

کاربرد شبکه‌های اجتماعی همچنان رو به افزایش است و به روش جذب قوا برای افراط‌گرایان خشن تبدیل شده است. دولت‌های علاقمند به مقابله با تروریزم خطر شبکه‌های اجتماعی را نادیده می‌گیرند. آنها باید از تکنالوژی‌های نوظهور مانند هوش مصنوعی (AI) برای مقابله با این افراط‌گرایان ایدیولوژی که در فضای آنلاین کمین گرفته‌اند، مستفید شوند.

تروریزم و شبکه‌های اجتماعی

امبر رود، وزیر داخله سابق بریتانیا، روند مقابله با محتوای افراط‌آمیز در فضای انترنت را به رقابت تسلیحاتی بین افراط‌گرایان و مامورین مجری قانون تشبیه می‌کند. رود اظهار کرد که تا نومبر 2017، افراط‌گرایان حدود 40,000 صفحه انترنتی و پروگرام کاربردی جدید ایجاد نموده بودند. موفقیت در این رقابت نیز، مانند هر رقابت دیگری، مستلزم استفاده از تکنالوژی‌های پیشرفته است. اخیراً تکنالوژی جدیدی به نام «هوش مصنوعی مکالمه‌ای» معرفی شده است.

«هوش مصنوعی مکالمه‌ای» طرحی تحقیقی است که برای شناسایی محتوای افراطی در فضای انترنت و حذف هرچه بیشتر این محتوا اجرا شده است. البته، استفاده از روش‌های یادگیری ماشین در رسیدن به این اهداف باعث کاهش چشمگیر این نوع محتوا شده است.

غولهای دنیای تکنالوژی، به رهبری مایکروسافت، گوگل، فیس بوک، آمازون و توییتر، حمایت خود را از ابتکار بین‌المللی «فراخوان کرایست‌چرچ» که مقابله با محتوای افراطی در انترنت را دنبال می‌کند، اعلان کرده‌اند. این کمپنی‌ها تعهد مکمل خود به به‌روزرسانی مستمر ضوابط استفاده مرتبط را ابراز کرده‌اند و روش‌های مختلفی برای شناسایی محتوای افراطی و سرمایه‌گذاری در تکنالوژی‌های تفتیش به کار گرفته‌اند.

هیات اجرایی کمیته ضد تروریزم سازمان ملل با اجرای ابتکار «تکنالوژی ضد تروریزم» به تفتیش فعال بیش از 500 کانال افراطگرا در بیش از 20 پلتفورم محتوایی و پروگرام پیام‌رسان پرداخته است.

سازمان‌های تروریستی از شبکه‌های اجتماعی برای مقاصد مختلف استفاده می‌کنند. جمع‌آوری پول، تقویت هویت جمعی و یکپارچه‌سازی اقدامات بخشی از این مقاصد است. گروپ‌های این‌چنینی از این شبکه‌ها برای رسیدن به اهداف مختلف، مانند هماهنگ‌سازی، جذب قوا و ترویج ایدئولوژی، استفاده کرده‌اند. در واقع این شبکه‌ها سامان‌های تعلیم مجازی و جلب حمایت مادی و معنوی بوده‌اند.

هوش مصنوعی

شگردهای هوش مصنوعی به تکنالوژی‌های نوظهور غالب در حوزه مقابله با محتوای افراطی در انترنت تبدیل شده‌اند. به اساس گزارش فیس بوک، حدود 99% از محتوای القاعده و داعش که از فیسبوک حذف شده است، قبل از آن که به‌وسیله انسان شناسایی شود، با سیستم‌های هوش مصنوعی شناسایی شده بود.

در شرایط فعلی، هوش مصنوعی را می‌توان موثرترین سلاح مقابله با تروریزم در دنیای دیتای کلان دانست. هوش مصنوعی از قابلیت شناسایی اتومات محتوای افراطی و تروریستی، اشخاص مظنون به ارتکاب اعمال افراطی و تروریستی و جوامع مجازی افراطگرا برخوردار است. هوش مصنوعی به پیش‌بینی، وقایه و تضعیف مخاطرات تروریستی آینده کمک می‌کند.

بدون شک، استفاده از پروگرام‌های ضد تروریستی مبتنی بر هوش مصنوعی باعث تولید داده‌های دقیق برای جلوگیری از اقدامات غیرضروری در مناطق پرجمعیت و کاهش احتمال جهت‌گیری بشری در روند تصمیم‌سازی می‌شود. هوش مصنوعی باعث جلب دقیق‌تر توجه اشخاص و کاهش تعداد شهروندان مشمول تفتیش مکمل می‌شود.

قابلیت‌های هوش مصنوعی در قسمت پیش‌بینی اقدامات تروریستی ثابت شده است. سرویس‌های امنیتی و معلومات از تحلیل اتومات داده‌ها برای ارزیابی احتمال سفر هوایی و افشای ارتباط سازمان‌های تروریستی و اشخاص وابسته استفاده می‌کنند. بعضی کمپنی‌های تکنالوژی از روش‌های پیشرفته پیش‌بینی برای تفتیش و مختل ساختن فعالیت‌های تروریستی در پلتفورم‌های شبکه‌های اجتماعی استفاده می‌کنند و از هوش مصنوعی برای تشخیص موارد مشکوک انتقال وجه در بخش خدمات مالی استفاده می‌کنند.

از هوش مصنوعی برای تحلیل شبکه‌های اجتماعی، شناسایی مظنونان و روابط آنلاین آنان، طبقه‌بندی اشخاص بربنیاد مشخصات، تحلیل پیوندهای ارتباطی و شناسایی مظنونان افراطگرا در جوامع مجازی استفاده می‌شود. بربنیاد داده‌های پروگرام نرم‌افزاریSKYNET که اداره امنیت ملی ایالات متحده از آن استفاده می‌کند و شامل الگوریتم مبتنی بر هوش مصنوعی است، حدود 15,000 نفر از 55 ملیون کاربر داخلی تلیفون همراه منحیث تروریست بالقوه شناسایی شده‌اند.

فیس بوک پالیسی‌های هوش مصنوعی خود را برای مقابله با محتوای افراطی بهبود بخشیده است. این کمپنی اوسط وقت لازم برای شناسایی ویدیوهای زنده ناقض ضوابط استفاده فیس بوک را به 12 ثانیه کاهش داده است.

از دیگر شیوه‌های حذف محتوای بنیادی استفاده از تکنالوژی‌های

پروسس لسان طبیعی است که احتمالاً کارآیی پروسه مقابله با محتوای افراطی در انترنت را افزایش می‌دهد. این ادعای داکتر مجدل بن سلطان بن صفران، استاد هوش مصنوعی پوهنتون ملک سعود، است.

با این تکنالوژی‌ها می‌توان دستگاه‌ها را برای شناسایی ارتباط بشری و استخراج معلومات در گروپ‌های کلان متنی تعلیم داد. این پروسه بدون دخالت انسان صورت می‌گیرد و برای شناسایی الگوهای لسانی مختلف مورد استفاده افراطگرایان و تروریست‌ها کاربرد دارد.

چالش‌های هوش مصنوعی

با وجود پیشرفت‌های صورت‌گرفته در قسمت به‌کارگیری تکنالوژی‌های هوش مصنوعی برای مقابله با محتوای آنلاین افراطگرایی و تروریزم، این تکنالوژی‌ها تا فعلاً هم با مشکلاتی مانند تحلیل محتوای لسانی روبرو هستند. گسترش لسان‌های ترکیبی مانند فرانکو و وجود لهجه‌های محاوره‌ای و تحلیل سگنال‌ها و تصاویر غیر لسانی این مشکلات را شدت بخشیده است. این مشکلات مانع اتکای مکمل به دیتای تحلیل دیجیتل مربوط به محتوای کلان و پیچیده شده است. چنین محتوایی را نمی‌توان صرفاً با تجربیات بشری تفتیش کرد.

برای رسیدن به الگوهای استخراج مفهوم واقعی و دقیق لسان و رسیدن به مرحله‌ای فراتر از حفظ نمودن کلمات و عبارات، فعلاً راه درازی در پیش داریم. برای رسیدن به توانایی تفسیر موضوعی داده‌ها که از عوامل اساسی درک رفتار آنلاین است، باید منتظر بمانیم.

کلودیا والنر، تحلیلگر «گروپ تحقیقی تروریزم و درگیری» در موسسه مطالعات دفاعی و امنیتی Royal United Services، درباره موفقیت ستراتیژی جدید اتحادیه اروپا در قسمت حذف محتوای تروریستی ابراز تردید نموده است.

والنر این استراتیژی را، به دلایل مختلف، چندان کاربردی نمی‌داند. از این دلایل می‌توان به ابهام درباره تعریف حقوقی محتوای افراطی یا تروریستی اشاره نمود. دولت‌ها پیشنهاد تغییر دادن تعاریف افراطگرایی خشن و تروریزم را مطرح ساخته اند ولی فهرست‌های طبقه‌بندی ملی اغلب فقط بخش کوچکی از گروپ‌های فعال افراطگرا یا تروریست را پوشش می‌دهد.

شناسایی محتوای افراطی مشمول پیچیدگی‌های قانونی است. گاهی نمی‌توان کلمه افراطگرایی را به‌دقت تعریف کرد. بعضی محتواهای مربوط به گروپ‌ها و اشخاص افراطگرا شامل هیچ اشاره یا کنایه حاوی تنفر یا خشونت نیست، ولی حالات خشم یا نارضایتی را با شوخی و طعنه منتقل می‌کند.

متاسفانه، تفتیش محتوای افراطی در انترنت باعث شده است که افراطگرایان و تروریست‌ها به پلتفرم‌های کلان مهاجرت کنند و در میان ملیون‌ها سایت در این پلتفرم‌ها مخفی شوند. به این ترتیب، نهادهای مجری قانون نمی‌توانند فعالیت آنان را به‌آسانی زیر نظر بگیرند.

به دلیل محدودیت منابع این پلتفرم‌ها برای حذف موثر محتوای تروریستی، سایتهای کوچک شبکه‌سازی اجتماعی حالا قطبی‌تر شده‌اند و مورد استفاده القاعده، داعش و دیگر گروپ‌ها قرار گرفته‌اند.

رایگان که بعد از مدت معینی بطور اتومات غیرفعال می‌شوند، به کار گرفت. تروریست‌ها با اهمیت بمب شرطی آشنا هستند. تهداب‌های بیشتر کشورهای دنیا به شبکه‌های کمپیوتری بستگی دارد و مجموعه مشخصی از حملات با بمب شرطی می‌تواند بسیاری از سیستم‌های سراسری بانکداری و ترانسپورت را مختل سازد.

هدف قرار دادن زیربناها

تهداب‌های بحرانی از خدمات اساسی موردضرورت جامعه، مانند ترانسپورت، تولید مواد غذایی، انرژی و خدمات صحی، پشتیبانی می‌کند. بروز اختلال شدید در این سرویس‌ها ممکن است اشخاص بسیاری را دچار آسیب‌پذیری کند. وابستگی این خدمات به زنجیره‌های تامین تدارکات الکترونیکی باعث تشدید آثار زیان‌بار حملات سایبری می‌شود چون این خدمات را می‌توان ستون فقرات اقتصاد ملی، بخصوص امنیت، معالجه، انرژی، آب، ترانسپورت، خدمات حمل و نقل، ارتباطات، بانکداری و خدمات مالی در نظر گرفت.

تهداب‌های بحرانی ممکن است در مقابل تروریزم سایبری آسیب‌پذیر باشد. دسترسی‌پذیری و وابستگی متقابل داده‌ها، در کنار استفاده از سیستم‌های کنترول صنعتی، تهداب‌های ارتباطات عمومی و هوش مصنوعی، توجه به امنیت سایبری در سطح ملی را ضروری ساخته است. ضمناً، افزایش سیستم‌های الکترونیکی-فزیکی، مانند موترهای بدون دریور، آسیب‌پذیری‌های جدیدی ایجاد نموده است.

انکشاف سریع و وابستگی متقابل تکنالوژی‌ها نیز باعث ایجاد تشویش‌هایی شده است. این تشویش‌ها عمدتاً از پیدایش «انترنت اشیا» که مسیر حملات جدید را برای مجرمین سایبری و تروریست‌ها فراهم نموده است، ناشی می‌شود.

در 8 اپریل 2020، «اداره امنیت سایبری و امنیت تهداب‌ها» و «مرکز ملی امنیت سایبری» در بریتانیا درباره وقوع حوادث امنیتی که تهداب‌های اساسی خدمات صحی و نهادهای دواویی را نشانه گرفته بود، هشدار داد. از قربانیان این حوادث می‌توان به کمپنی‌ها، موسسات تحقیقات طبی و پوهنتون‌ها اشاره نمود. بخشی از حملات نیز با پیدایش پاندیمی کووید-19 همزمان شده بود.

در فبروری 2021، در ایالات متحده، هکرها به یکی از تصفیه‌خانه‌های شهر کوچکی در فلوریدا نفوذ کردند. هدف آنها افزایش میزان مواد کیمیاوی احتمالاً خطرناک در منبع آب بود. خوشبختانه، این حمله قبل از ایجاد نتایج خطرناک خنثی شد.

همان ماه، وزارت امنیت داخلی ایالات متحده از حمله نرم‌افزارهای باجگیری به تهداب‌های اساسی یک مرکز فشرده‌سازی گاز طبیعی خبر داد. شخص مهاجم از روش فیشینگ نیزه‌ای استفاده کرده بود. این حمله هدفمند برای قانع ساختن قربانی به ارائه معلومات حساس و رسیدن به شبکه‌های موسسه طراحی شده است که در این مورد به رخصتی دو-روزه آن مرکز منجر شد.

با پیچیده‌تر شدن حملات مجازی، نهادهای مسئول دفاع از امنیت ملی، مانند قوای مسلح، نباید سلاح خود را به زمین بگذارند. البته چنین نیست که همه حملات مخرب به حاکمیت ملی با سلاح‌های سنتی صورت بگیرد. ✦

استفاده از کلمات منحیث سلاح

اتحادیه رادیویی و تلویزیونی اسلامی که با حمایت ایران اداره می‌شود، نشر **معلومات غلط** برای تضعیف همبستگی اجتماعی را در دستور کار قرار داده است

تورن جنرال متقاعد عودا شدیفات، مشاور رسانه‌ای و فرهنگی، قومندان کل، قوای مسلح اردن/اردوی عرب

اخبار گوناگون به همراه تحلیل، راپور، ارتباط و گفتگو در همه جای دنیا جریان دارد. بربنیاد باورها، نظرات و اهداف رسانه یا مهمانان، پروگرام‌ها می‌توانند موضع تهمت‌آمیز، دفاعی یا خنثی درباره مسائل روز اتخاذ کنند.

در بسیاری از رسانه‌ها، تغییر خصوصیات، احساسات و حالات دیده می‌شود. صبر به پایان رسیده است و صداها، حتی تا سطح فریاد زدن و دشنام دادن، بالا شده است و این وضعیت بیننده را آزار می‌دهد. در بیشتر موارد، استخراج معلومات واقعی و موثر از این ترکیب دیدگاه‌ها سخت می‌شود. این صحنه هر بار که بیننده سعی در رهگیری اخبار از یک درگاه به درگاه دیگر، معمولاً از طریق کانال‌های ستلایت، می‌کند، تکرار می‌شود.

ما کاملاً می‌دانیم که رسانه‌ها، با درگاه‌ها و محتوای منظم، از ضروریات زندگی امروزی هستند و این نقش را نمی‌توان از کلیت زندگی انسان‌ها حذف نمود. با توسعه سریع تکنالوژی معلومات و الزامات مرتبط، محتوای رسانه‌ها در اختیار تک‌تک ساکنان این دهکده جهانی قرار می‌گیرد.

البته این نکته درخور تامل است که اردوی کانال‌های ستلایت با تامین مالی اتحادیه رادیویی و تلویزیونی اسلامی اقدام به پخش پروگرام‌های نفرت‌پراکن فرقه‌ای، پنهان نمودن زشتی گروپ‌های مسلح و «مقدس» خواندن گروپ‌های کوچک وابسته نموده است.

این اتحادیه شامل 210 کمپنی رسانه‌ای در 35 کشور است که بیشتر آنها در شرق میانه فعال هستند. مراکز تحقیقی و سروی، گروپ‌های جنگ روانی و سایت های خبری نیز عضو این اتحادیه هستند. این موسسات بخش مشخصی از جامعه را برای تلقین معلومات غلط به ذهن مردم هدف قرار داده اند. در چنین وضعیتی، احساس ظلم و محرومیت در اشخاص شکل می‌گیرد و این احساس زمینه‌ساز شورش آنها علیه دولت خودشان می‌شود.

به نظر من، این همان پرخاشگری و اعلان جنگ علیه آرامش مدنی جوامع عرب است. ایران از این سامان‌های رسانه‌ای منحیث اهرم فشار علیه کشورهای منطقه و دنیا استفاده می‌کند و کشورها را در معرض آفت جنگ و ویرانی قرار می‌دهد. اعمال تحریم‌های بین‌المللی علیه این نهاد ضروری است چون این نهاد، همانند سپاه پاسداران انقلاب اسلامی در ایران و موسسات امنیتی، زمینه‌ساز خشونت و تروریزم شده است.

شما اغلب موضوع خاصی را در عناوین اصلی اخبار، گفتگوهای خبری و پروگرام‌های مشابه می‌بینید. امروزه، دنبال‌کنندگان شبکه‌های خبری در منطقه و بعضی شبکه‌های دیگر نقاط دنیا، حتماً با نام ایران و رژیم، اهداف، آرمان‌ها، نفوذ، سلاح‌ها و تاثیر آن بالای جوامع مختلف و نیز اخبار اقدامات غلط ایران و دخالت‌های آن در امور داخلی و خارجی کشورهای دیگر در اخبار و راپورها روبرو می‌شود.

ایران حتی با همه امکانات در آینده آن جوامع - آینده اطفال، آرمان‌ها، و پروگرام‌های خاص- دخالت می‌کند. طرز مثال، در سطح مشکلات جهانی، پروگرام هسته‌ای ایران باعث تشویش همه شده است و موضوعی برجسته محسوب می‌شود. اخبار مربوط به این موضوع صبح و شب در مقابل دیدگان مردم قرار دارد. این وضعیت باعث شده است که بعضی کشورهای منطقه بودیجه‌های کلانی، تا 1.5$ ملیارد، برای مقابله با تهدید ایران اختصاص دهند.

مالزیا همه روابط خود با ایران را قطع کرده است و در اقدامی ناگهانی همه همکاری‌های خود با ایران را متوقف ساخته است. دخالت ایران در لبنان باعث ایجاد مشکلات جدی شده است. همچنان، دخالت‌های مشابه در یمن عواقب ناگواری داشته است. این مشکل هم‌اکنون افغانستان را نیز درگیر نموده است. وضعیت در عراق و سوریه نیز نامطلوب یا بدتر است. کشورهای همسایه خلیج‌فارس و دیگر نقاط منطقه نیز از دخالت‌های ایران که با جذب سرداران، سودجویان اوضاع بحرانی و ترویج فرقه‌گرایی شکل‌های مختلفی به خود می‌گیرد، در امان نیستند.

ما در مقابل این تهدید معنوی -با استفاده از سلاح، شبه‌نظامیان، چریک‌های عکس العمل سریع، جنگ رسانه‌ای، دلالان مواد مخدر، آیدیالوجی افراطی و آسان‌گیری در مقابل هر چیزی که در خدمت ایدئولوژی کشورهای دچار تعصب مذهبی و ملی باشد- نباید خاموش بمانیم. ما باید از ثبات و امنیت سرزمین‌های خود که در تیررس تروریزم مورد حمایت ایران قرار دارند، محافظت کنیم.

دولت ایالات متحده صفحه‌های انترنتی اتحادیه رادیویی و تلویزیونی اسلامی را که ایران از آنها برای ترویج افراطگرایی خشن استفاده می‌کند، مسدود ساخته است. رویترز

لازم نیست ما علیه ایران اعلان جنگ کنیم تا آرمان‌های انکشافی آن به حساب کشورهای منطقه و سرمایه‌گذاری در گروپ‌های تروریستی متوقف شود. من نیز، مانند دیگران، جنگ را محصول کوتاهی در یافتن راهکار سیاسی برای مشکلات می‌دانم. من خواستار استفاده از قدرت نرم هستم و امیدوار هستم که مجبور به دفاع از خودمان نشویم. این یگانه راه مهار ساختن خواسته‌های نابخردانه ایران است. این قدرت نرم فشار اقتصادی و دیپلوماتیک را شامل می‌شود.

ما باید به ایجاد و حفظ روابط منطقوی و بین‌المللی بپردازیم. این روابط مانعی در مقابل ناقضان قوانین بین‌المللی که خود را در پشت نیروهای نیابتی و جنگوجیان کرایی پنهان می‌کنند، ایجاد خواهد کرد. ایران به مساعی برای رسیدن به سلاح هسته‌ای ادامه می‌دهد و حتی قبل از رسیدن به این سلاح نیز خطری برای منطقه به شمار می‌رود. اگر کشوری با این رفتار غیرمنطقی به سلاح کشتار جمعی دست پیدا کند، چه خواهد شد؟

ما باید به ایجاد فشار علیه ایران ادامه بدهیم و آن را از حمایت، پرورش و تعلیم گروپ‌های تروریستی بازداریم. ✦

اعتمادسازی بحرین برای مقابله با انتشار معلومات غلط

این کشور در میدان جلوگیری از شیوع همه‌گیری کووید-19 به جنگ معلومات ترس‌آور انترنتی رفت

حبیب طومی، مشاور وزارت معلومات بحرین

در شرایط همه‌گیری، همانند دوران جنگ، واقعیت ظاهراً نخستین قربانی خواهد بود.

با این که دنیا از قرون قبل درگیر امراض پادیمیک و مسری بوده است، هیچ‌گاه در میانه سیل معلومات غلط، معلومات تحریف‌شده و نظریه‌های توطئه مربوط به کووید-19 مجبور به مقابله با این بحران‌ها نبوده است.

گسترش ابزارهای ارتباطی با ادغام پیام‌های تصویری، صوتی، ویدیویی و مکتوب -و انتشار راپورهای شبه‌واقعی که به‌آسانی در سطح کشورها تولید و توزیع می‌شود- باعث تغییر دورنما، متحول شدن انتظارات و ایجاد آشفتگی در جوامع شده است.

سازمان صحی جهان کلمه «پاندیمی معلومات» (Infodemic) را برای اشاره به نشر گسترده معلومات گمراه‌کننده و سردرگم‌کننده درباره کووید-19 که مساعی مربوط به مقابله با ویروس را خنثی می‌کند و معالجه و وقایه را سخت می‌سازد، وضع نمود.

تصاویر بودیبات

ترکیب امراض ترسناک و معلومات غلط از زمان وقوع نخستین فجایع وجود داشته است و اشخاص طی قرنها این حوادث را به جادو، چشم بد، اهریمن و خشم خدا نسبت می‌داده‌اند.

درحالی‌که مریضی قربانی می‌گیرد، معلومات غلط مقصران احتمالی را هدف قرار می‌دهد و زمینه اعدام، انزوا و اخراج آنها را فراهم می‌کند.

اتهامات جعل‌شده بر مبنای دلایل سیاسی، اقتصادی یا اجتماعی گروپ‌هایی مانند یهودیان، مسیحیان، مسلمانان، زنان، افریقایی‌ها، آسیایی‌ها، اقلیت‌ها، جذامیان، فقرا، آدم‌های ایلاگرد و بیگانگان را هدف قرار می‌دهد. فریبکارانی که این داستان‌ها، ادعاها و شایعات را می‌پذیرند، ظاهراً هیچ‌گاه ضرورت به معلومات غلط پیدا نمی‌کنند.

حتی با سپری شدن دوره‌های تاریخی، اهداف نشر معلومات غلط و دروغ تغییر نمی‌کند. صرفاً روایت‌ها بربنیاد خصوصیات آخرین دوره پاندیمی به‌روز می‌شود.

جان د. لی در آخرین کتاب خود، «پاندیمی شایعات»، در سال 2014 نوشت که: «روایت‌ها از یک دوره شیوع به دوره بعدی بازیافت می‌شود و تغییری که رخ می‌دهد به مضمون مربوط نمی‌شود، بلکه به جزییات لازم برای مرتبط ساختن روایت‌ها به شرایط جاری مربوط می‌شود.»

بعضی از تصاویر دستکاری‌شده و روایت‌های غلط را بدخواهانی که خواستار بحران، ترس و سترس هستند، نشر کرده‌اند. بخشی از تصاویر نیز با حس تحریف‌شده شوخی و اندیشه ناهنجار سرگرمی تولید شده‌اند.

تکنالوژی باعث ساده و موثر شدن ترکیب واقعیت و داستان‌های جعلی شده است. پروگرام‌های کاربردی امکان ایجاد دنیای خیالی را که جایگزین دنیای واقعی و واقعیات نادیده‌گرفته‌شده می‌شود، فراهم نموده است. رشد نمایی تکنالوژی، که ظاهراً قرار است دنیا را به جای بهتری تبدیل کند، مورد سوءاستفاده قرار گرفته است.

در نخستین روزهای 2020، که دنیا در حال آگاه شدن از پاندیمی کووید-19 بود، مردم در معرض پیام‌های فراوان از طرف شبکه‌های داخلی -خویشاوندان، دوستان، همکاران، همسایگان- و معلومات خارجی از طرف داکتران، کارشناسان صحی، اشخاص مشهور، مسئولین و شخصیت‌های سیاسی قرار می‌گرفتند.

رهبران بیشتر کشورها متوجه شدند که یکی از پرزه‌جات مهم استراتیژی مقابله با این مرض لجام‌گسیخته مهار کردن سیل معلومات غلطی بود که می‌توانست احتمال کنترول مرض تا زمان تولید واکسین را از بین ببرد.

بحرین، یک جزیره کوچک (765 کیلومتر مربع) و یکی از متراکم‌ترین کشورهای دنیا (حدود 2,052 نفر در هر کیلومتر مربع) جزو کشورهایی بود که احتمال پاندیمی در آن بالا بود. با این حال، «پاندیمی» ذریعه انترنت و شبکه‌های اجتماعی می‌توانست فاجعه‌بار باشد.

بربنیاد دیتای DataReportal، در جنوری 2020، میزان نفوذ انترنت در بحرین 99% و میزان نفوذ شبکه‌های اجتماعی 84% بود. در آن زمان، این کشور 1.65 ملیون کاربر انترنت و 1.4 ملیون کاربر شبکه‌های اجتماعی داشت.

کارگروپ ملی چند-وزارتخانه‌ای در اوایل فبروری 2020 برای رسیدگی به موضوع شیوع و گسترش کووید-19 تشکیل شد و بشمول یک پرزه رسانه‌ای کلان بود.

درحالی‌که مسئولین در حال مقابله با پاندیمی بودند، دولت خود را مکلف

مردم در صف دریافت واکسین کووید-19 در مرکز خرید Sitra منامه. با وجود اقدام موثر بحرین برای وقایه از نشر وایرس، بدخواهان به نشر معلومات دروغ درباره پاندیمی در سطح کشور می‌پردازند. رویترز

به مقابله با معلومات غلط و معلومات دروغ که بر بنیاد مزیت اعتیاد محلی به پلتفورم‌های دیجیتل برای تخریب مساعی دولتی نشر می‌شد، کرده بود.

این کارگروپ از مردم می‌خواست که از منابع معلوماتی معتبر استفاده کنند و در دام ادعاهای غلط و گمراه‌کننده اشخاص شهرت‌طلب، نظریه‌پردازان توطئه و لاف‌زن‌ها نیفتند.

این کارگروپ، با هدف تسهیل ارتباط، یک خط رهنما به هفت لسان دایر کرد. بیش از نیمی از جمعیت 1.7 ملیونی بحرین اصالتاً از 140 کشور هستند.

بحرین دارای دو روزنامه عربی، دو روزنامه انگلیسی، یک روزنامه به لسان مالایالام (هند) و یک روزنامه به لسان تاگالوگ (فیلیپین) است. هفته‌نامه‌ها و ماهنامه‌ها به لسان‌های مختلف نشر و پروگرام‌های رادیویی و تلویزیونی به لسان‌های گوناگون پخش می‌شوند.

همه آنها سنگینی شرایط را درک کردند و خود را مکلف به چاپ و نشر اخبار منابع معتبر نمودند. از منابع معتبر می‌توان به مسئولین رسمی، بیانیه‌های کارشناسان و مامورین پولیس، و اطلاعیه‌های وزارت‌خانه‌ها اشاره نمود.

رسانه‌ها ادعاهای مشکوک را نمی‌پذیرفتند و راپور دهندگان را اغلب برای گفتگو با داکتران -عمدتاً مشاورین امراض عفونی و داخلی و کارشناسان مایکروبیولوژی- که قادر به ارائه توضیحات علمی برای تشریح وضعیت بودند، اعزام می‌کردند. این رویکرد تاثیر بسزایی در تکذیب معلومات غلط داشت.

شخصیت‌های مذهبی در مواعظ و سخنرانی‌های خود دروغ‌پراکنی را معادل نقض آموزه‌ها و ارزش‌های مذهبی عنوان می‌کردند.

مقامات امنیتی و قضایی نیز منظماً به مردم هشدار می‌دادند که نشر معلومات دروغ معادل اتهام اخلال در نظم عمومی است و با پیگیری حقوقی، شامل حبس و جریمه سنگین، همراه خواهد شد.

این کارگروپ منظماً جلسات رسانه‌ای را برای ارائه راپور، صدور هشدار و معلومات‌رسانی برای تقویت حس مسئولیت‌پذیری و یادآوری عواقب مخرب نشر شایعه و ادعا برگزار می‌کرد.

بالا بودن نرخ باسوادی (97.5% در 2018) و اجرای کمپاین «آگاه باش» در اعتمادسازی بین مردم و دولت و موسسات خصوصی تاثیر بسزایی داشت و به جلوگیری از نشر نظریه‌های توطئه که معمولاً در شرق میانه دیده می‌شود، کمک کرد.

مقاومت عمومی مردم بحرین در مقابل معلومات غلط و معلومات دروغ نتیجه ترکیبی اقدام عاجل کارگروپ، هشدارهای سختگیرانه علیه متخلفین و ارتباط آزاد با کارشناسان صحی و خبرنگاران متعهد بود.

بیشتر پیام‌های حاوی معلومات غلط و معلومات دروغ ذریعه واتساپ که پرکاربردترین پروگرام ارتباطی در بحرین است، بین مردم این کشور مبادله می‌شد.

این پیام‌ها عمدتاً ارتباطی با مسائل سیاسی یا مذهبی یا فرقوی که متاسفانه، به دلیل دشمنی بین فرقه‌ها و کشورها، بر شرق میانه حاکم است، نداشت.

ناراحت‌کننده‌ترین پیام 26 فبروری، دو روز بعد از تشخیص نخستین مصاب شدن در یک شهروند بحرینی که از سفر زیارتی از ایران بازگشته بود، منتشر شد. پیام‌های واتساپ حاوی انتقاد از اتباع بحرینی که به ایران سفر می‌کردند بود. این اتباع به انتقال مرض و قرار دادن بحرین در معرض خطر متهم می‌شدند. به راپور پولیس، 30 حساب اقدام به نشر پیام‌های دارای محتوای فرقوی می‌کردند.

البته، مداخله سریع جلالت مآب شاهزاده سلمان بن حمد آل خلیفه به خنثی شدن تنش ناشی از ترس کمک کرد. او خواستار حفظ وحدت ملی شد و تاکید کرد که «انتقال کووید-19 ارتباطی با نژاد، قومیت، مذهب یا طبقه اجتماعی ندارد.»

بعضی مساعی برای نشر معلومات دروغ با هدف فریب دادن مستفیدان یا تاثیرگذاری بالای رفتار آنان صورت می‌گرفت. طرز مثال:

- در رسانه‌های اجتماعی اعلان می‌شد که نخستین موارد کووید-19 در Dragon City یا «شهر اژدها» از مراکز خرید کلان دارای معماری چینی دیده شده است و این که پولیس به فروشگاه‌ها و مراکز عرضه لوازم جانبی، تزیینات خانه و غذا حمله کرده است.

جلالت مآب شاهزاده سلمان بن حمد آل خلیفه، صدراعظم بحرین، در حال دریافت واکسین یادآور کووید. وزارت معلومات بحرین

بحرین برای هماهنگ‌سازی اقدامات مقابله با بحران کووید-19 از شخصیت‌های معروف کمک گرفت. رویترز

بحرینی‌ها از مسافرین سعودی که بعد از باز شدن سرحدات به روی اشخاص پیچکاری شده علیه کووید-19 وارد این کشور می‌شوند، استقبال می‌کنند. رویترز

- در یک مورد دیگر، رسانه‌های اجتماعی این ادعا را نشر کرده بودند که بعضی اشخاص مصاب به کووید-19 از مراکز قرنطین فرار کرده‌اند و در سراسر کشور پراکنده هستند. پولیس به‌سرعت هر دو شایعه را تکذیب کرد.
- پولیس یک مستفید را که ادعا کرده بود که کووید-19 دروغ کلانی برای جمع‌آوری پول از مردم است، بازداشت کرد.
- یک خواننده معروف بعد از استفاده از واتساپ برای هشدار دادن به مردم درباره تماس با پیکهای رساندن پیتزا و غذا به خانه ها، دچار مشکل حقوقی شد چون این کارگران را خطرناک و دارای آلودگی معرفی کرده بود.
- موسسه بین‌المللی حقوق بشر با صدور راپوری که بعد از بازدید میدانی منتشر شد، شایعه مصاب شدن چند تن از زندانیان به کووید-19 را تکذیب کرد.
- بعضی معلومات دروغ که در کشور نشر می‌شد به راپورهای «معتبر» یا «سرّی» درباره منشاء ویروس و راه‌های تداوی مریضی مربوط می‌شد.

امروز، دو سال بعد از شروع پاندیمی، بحرین برنبیاد شاخص Nikkei بهبود کووید-19 در دنیا در ماه نومبر در رتبه اول قرار گرفت. این پادشاهی به مساعی جدی برای مقابله با پاندیمی و بازگشت به زندگی عادی ادامه داده است.

این شاخص، که نخستین بار در جولای 2021 منتشر شد، آمار بهبود کووید در 121 کشور و منطقه را بربنیاد نُه عامل و سه کتگوری ارزیابی می‌کند: مدیریت آلودگی، تزریق واکسین و جابجایی.

مدیریت آلودگی بشمول موارد تاییدشده کووید-19 در مقابل حداکثر تعداد موارد، سرانه موارد تاییدشده و تعداد تست در هر مورد است.

عامل تزریق واکسین تعداد مجموع سرانه دوزهای واکسین، تعداد سرانه دوزهای جدید واکسین، و سهم اشخاص کاملاً-پیچکاری شده را پوشش می‌دهد.

عامل جابجایی به تحرک اجتماعی، شاخص قاطعیت آکسفورد و فعالیت‌های پروازی مربوط می‌شود.

هرچه رتبه، در محدوده 0 الی 90، بالاتر باشد، کشور به نقطه بهبود نزدیک‌تر است که در این زمینه کاهش میزان آلودگی، سطح بالای پیچکاری و اقدامات آسان‌گیرانه‌تر برای فاصله‌گذاری اجتماعی مد نظر قرار می‌گیرد.

بحرین نمره 73% را اخذ نمود و بعد از آن، کویت 72% و امارات متحده عربی 70.5% را کسب کردند.

در نومبر 2021، اداره نظارت و قانون‌گذاری صحت بحرین اعلان کرد که مصرف عاجلی واکسین فایزر-بایونتک را برای اطفال 5 الی 11 ساله تایید نموده است. این تصمیم بعد از ارزیابی داده‌های فایزر-بایونتک از طرف کمیته کارآزمایی‌های کلنیکی اداره ملی نظارت و قانون‌گذاری صحت و کمیته پیچکاری وزارت صحت گرفته شد. ✦

تعهد به امنیت سایبری

محافظت از عراق در مقابل تهدیدات سایبری مستلزم تقویت امکانات عراق در حوزه تکنالوجی است

داکتر حسین علاوی، مشاور صدراعظم عراق در امور اصلاحات بخش امنیتی

تصاویر یونیپاث

امنیت سایبری از اولویت‌های ستراتژیک دولت عراق است. عراق دست به ایجاد گروپ واکنش به حوادث سایبری (CERT)، فعال‌سازی پالیسی امنیت سایبری و تهیه مسوده قانون جرایم الکترونیکی زده است. قانون مذکور زمینه‌ساز بحثهای گسترده‌ای در پارلمان عراق شد.

وظیفه اصلی گروپ واکنش به حوادث سایبری مقابله با حملات سایبری در همه وزارتخانه‌ها، همکاری با نهادهای امنیتی و استخباراتی برای تفتیش هکرها و گروپ‌های تروریستی و تعقیب گروپ‌های جرایم سازمان‌یافته سایبری است. این اقدامات احتیاطی برای جوامع امروزی، مانند عراق، که برای انتقال پول و اجرای وظایف دولتی وابستگی روزافزونی به انترنت دارد، ضروری است.

حملات سایبری از تهدیدات رو به گسترش دنیا محسوب می‌شود. این حملات باعث ایجاد این تشویش بین‌المللی شده است که گروپ‌های تروریستی از تکنالوژی‌های پیشرفته برای اجرای حملات سایبری علیه تاسیسات حیاتی استفاده می‌کنند. با توجه به این موضوع، عراق دومین جلسه «انکشاف و ایجاد امکانات امنیتی در فضای مجازی» را در سپتمبر 2021 در بغداد برگزار کرد.

برگزاری این جلسه نقطه عطفی در فعالیت گروپ واکنش به حوادث سایبری عراق محسوب می‌شود. در این جلسه مسائل مهمی مانند جرم الکترونیکی، امکانات سایبری برای جلوگیری از وقوع جنگ 5G، تاثیر امنیت سایبری و تکنالوجی‌های مدرن بالای امنیت ملی، و محافظت از اطفال در انترنت بررسی شد. از موضوعات دیگر می‌توان به تاثیر امنیت سایبری بالای اشخاص در دنیای سرشار از معلومات دروغ، امنیت دیجیتل برای محصلین و پول‌شویی و تعاملات مالی اونلاین اشاره نمود.

در حاشیه این جلسه، گروپ واکنش به حوادث سایبری عراق نمایشگاهی تخنیکی را برگزار کرد و مانور امنیتی برگزار شد. در این مانور، این گروپ به‌سرعت برای دفع یک تهدید سایبری وارد عمل می‌شد.

اثیر الجابر، رئیس گروپ واکنش به حوادث سایبری عراق، بالای اهمیت این جلسه در دورانی که کمپنی‌ها و نهادهای دولتی اتومات‌سازی الکترونیک را به دلیل پاندیمی کووید-19 پذیرفته‌اند، تاکید کرد.

الجابر اظهار کرد: «طی جلسات این نشست، ما یک قدم دیگر در مسیر موفقیت در قسمت ارائه خدمات در فضای مجازی برداشتیم.»

تبادل دانش تخنیکی با کشورهای دوست در جریان مقابله با حملات سایبری یا ترمیم شبکه‌ها بعد از نفوذ به سیستم امنیتی ستون فقرات امنیت سایبری محسوب می‌شود. تجربه کشورهای دوست عراق در حوزه تکنالوژی مزیتی برای عراق محسوب می‌شود. این کشور سعی می‌کند تا امکانات امنیتی خود را در فضای مجازی انکشاف دهد و تقویت نماید.

از طرف دیگر، عراق علاقمند به تبادل معلومات موجود درباره شیوه‌های تروریستان برای سوءاستفاده از تکنالوژی سایبری در مسیر ارتباطات، رمزگذاری و پلان‌گذاری حملات است. ازآنجاکه گروپ‌های تروریستی و باندهای جرایم سازمان‌یافته به تبادل مفکوره و تکنالوژی می‌پردازند، اعضای جامعه بین‌المللی باید برای دفع نقشه‌های بدخواهانه مهاجمان همکاری کنند.

مبنای امنیت سایبری ایجاد یک بخش تکنالوژی پیشرفته و مستفید از ابتکار دفع حملات سایبری پیچیده است. عراق باید پیوسته به اصلاح پالیسی‌های ملی امنیت سایبری و تقویت امکانات خود بپردازد. دولت عراق در پی جذب اشخاص فعال در حوزه امنیت و خدمات مدنی است تا از این طریق امکانات عراق در قسمت امنیت سایبری و همکاری با بخش دولتی، بخش خصوصی و کمپنی‌های بین‌المللی تقویت شود.

عراق می‌خواهد که به ترویج فرهنگ یکپارچه مقابله با تهدیدات سایبری، کاهش تعداد موارد هک و سرقت معلومات، جلوگیری از نشر معلومات دروغ و تهدیدکننده آرامش مدنی، و کاهش تعداد جرایم سایبری که اشخاص بی‌وجدان علیه مستفیدان انترنت مرتکب می‌شوند، بپردازد.

همکاری دولتی-خصوصی در حوزه امنیت سایبری یک ضرورت استراتیژیک است. وابستگی بخشهایی مانند صحت، تعلیم و انرجی به ارتباطات سایبری برای ایفای وظایف مرتبط روزبه‌روز بیشتر می‌شود. به همین دلیل، دولت عراق و گروپ گروپ واکنش به حوادث سایبری در پی ایجاد راهکارهای جدید در قسمت تکنالوجی معلومات هستند.

عراق می‌خواهد که به ترویج فرهنگ یکپارچه مقابله با تهدیدات سایبری، کاهش تعداد موارد هک و سرقت معلومات، جلوگیری از نشر معلومات دروغ و تهدیدکننده آرامش مدنی، و کاهش تعداد جرایم سایبری که اشخاص بی‌وجدان علیه کاربران انترنت مرتکب می‌شوند، بپردازد.

وزارت‌خانه‌های دولتی از مشوق‌های مالی برای تشویق کارآفرینان بخش تکنالوژی معلوماتی و امنیت سایبری کار می‌گیرند. عراق باید بالای توانمندسازی زنان برای مشارکت هرچه بیشتر در این بخش مهم نیز متمرکز شود. آنها قوه محرک جامعه ما به طرف آبادانی هستند؛ جامعه‌ای که حالا با مشکلات زیادی روبروست. توانمندسازی زنان از پرزه‌جات اساسی پروگرام و فلسفه کار دولت عراق است. نقش زنان در کشورهای انکشاف یافته در حوزه تخنیکی برجسته است و زنان فعال در مراکز حساس در رسانه‌های اجتماعی، صنعت سافتویر و مارکتینگ الکترونیکی از سامان‌های تکنالوجی پیشرفته بهره گرفته‌اند.

امروزه ما باید از رشد چشمگیر در حوزه‌های کسب‌وکار، تجارت الکترونیکی و سرمایه‌گذاری در تکنالوژی معلومات در تمامی بخشهای عراق حمایت کنیم. این اقدام باید با تدوین قوانین سودمند، وضع پالیسی‌های عمومی و رسیدن به توانایی تامین الزامات امنیت سایبری صورت بگیرد. ما باید از پلان‌های دولت عراق در قسمت ایجاد همکاری بین عراق و جامعه بین‌المللی تشبثات، ذریعه تامین ماحول مناسب برای رشد شرکتهای تکنالوژی معلوماتی، با هدف خدمت‌رسانی به جامعه و نوسازی امکانات آن، حمایت کنیم.

خوشبختانه، موفقیت دولت عراق در حمایت از کمیسیون عالی مستقل انتخابات به خاطر برگزاری انتخابات آزاد و منصفانه و توانایی کمیسیون برای مقابله با حملات سایبری در جریان انتخابات پارلمانی در 10 اکتوبر 2021، پیام مهمی درباره بهبود امکانات عراق در حوزه مقابله با حملات سیابری و تقویت امنیت سایبری به همراه داشت. ✦

قزاقستان و سپر سایبری

پروگرام قزاقستان بالای محافظت از سیستم‌ها در مقابل هکرها و مجرمین متمرکز است

سلطنت بردیکیوا

تصاویر یونیپاث

تبدیل شدن قزاقستان به یک کشور پیشرفته در حوزه دیجیتل تمرکز بالای امنیت سایبری را ایجاب می‌کند. اینجا نمایی از پایتخت آستانه، مرکز نوآوری تکنالوژیک، دیده می‌شود. آسوشیتد پرس

بیش از 85% جمعیت قزاقستان از انترنت استفاده می‌کنند که این آمار در بین کشورهای آسیای میانه بی‌نظیر است. بخشهای عمده اقتصادی کشور و دولت کاملاً دیجیتلی شده‌اند. در سال 2018، دولت قزاقستان دست به اجرای پروگرام «قزاقستان دیجیتل» زد. این پروگرام برای تشویق نهادهای دولتی و شرکتها برای جابجایی از مرحله خشت و ملاط به مرحله دسترسی آنلاین و تسهیل دسترسی موثر مشتریان طراحی شده است.

با وجود پیدایش تحولات چشمگیر در اقتصاد دیجیتل قزاقستان، ضرورت به امنیت سایبری افزایش یافته است؛ بخصوص در دوران شیوع پاندیمی کووید-19 که بسیاری از مردم را مجبور به استفاده از سامان‌های کار و تحصیل از راه دور کرد.

این وضعیت مسئولین قزاقستان را به فکر اجرای اقدامات جدی برای مقابله با تهدیدات سایبری انداخت. با وجود چالش‌های فراوان در حوزه جرایم سایبری، که محدوده، شدت و پیچیدگی آنها رو به افزایش است، نتایج مساعی قزاقستان برای مقابله با جرایم و تهدیدات سایبری در سالهای اخیر چشمگیر بوده است.

با استفاده از پیشرفت‌های حوزه امنیت سایبری، قزاقستان در قسمت پایبندی به امنیت سایبری بربنیاد «شاخص جهانی امنیت سایبری 2020» که اتحادیه بین‌المللی مخابرات منتشر می‌کند، رتبه 31 را در بین 182 کشور کسب نموده است. این اتحادیه را سازمان ملل برای رسیدگی به امور تکنالوژی‌های ارتباطات و معلومات تشکیل داده است.

پنج رکن اصلی این شاخص عبارت‌اند از حقوقی، تخنیکی، سازمانی، انکشاف ظرفیت و اقدامات همکارانه. رتبه 2020 پیشرفت مهمی در مقایسه با جایگاه قبلی 83 قزاقستان در شاخص جهانی امنیت سایبری 2017 محسوب می‌شود.

نصب سپر سایبری

سیاست امنیت سایبری قزاقستان از پروگرام «سپر سایبری» که رئیس‌جمهور وقت، نورسلطان نظربایف، در سال 2013 آغاز کرد، نشات می‌گیرد. او تاکید کرد که انکشاف ستراتیژی امنیت سایبری جزو علایق امنیتی ملی قزاقستان بود چون مجرمین سایبری از توانایی ایجاد اختلال در تهداب‌های مانند نیروگاه و خط ریل برخوردار اند.

نظربایف در سال 2017 اظهار کرد: «در دنیای امروز، جنگ صرفاً با طیاره و تانک صورت نمی‌گیرد.»

آن سال، قزاقستان سیاست‌های دولتی در قسمت جلوگیری، تضعیف و مقابله با حملات سایبری و جنگ ترکیبی و بهبود پروسه‌های حقوقی برای ایفای موثر این وظایف را انکشاف کرد. مقامات قزاقستان با رایزنی با کارشناسان بین‌المللی با بهترین شیوه‌های تامین امنیت سایبری آشنا شدند. مرحله نخست پروگرام «سپر سایبری» از 2017 الی 2018 اجرا شد و مرحله دوم فاصله زمانی 2019 الی 2022 را پوشش می‌دهد. تا فعلاً، این پروگرام 28 ملیارد تنگه قزاقستان (حدود 66$ ملیون) مصرف داشته است.

وزارت توسعه دیجیتل، نوآوری و هوافضای این کشور مسئول دولتی اصلی اجرای پروگرام عملی «سپر سایبری» محسوب می‌شود و کمپنی سهامی سرویس تخنیکی دولتی که زیرمجموعه وزارت سرمایه‌گذاری و انکشاف قزاقستان است، در این زمینه با این وزارتخانه همکاری می‌کند.

«سپر سایبری» روش‌های اجرای پالیسی‌های دولتی در قسمت محافظت از منابع معلومات الکترونیکی، سیستم‌های معلوماتی و شبکه‌های مخابراتی و تضمین استفاده مصئون از تکنالوژی‌های معلوماتی و ارتباطات را مشخص می‌کند. این مفهوم به یکپارچه‌سازی رویکردهای موقت قبلی در حوزه

پذیرش تکنالوژی دیجیتل بین مردم قزاقستان دولت را به فکر تمرکز بیشتر بالای امنیت سایبری انداخته است. آژانس خبری فرانسه/تصاویر گتی

امنیت سایبری کمک کرده است. «سپر سایبری» همچنان از انکشاف میکانیزم های عکس‌العمل سریع برای وقایه از حوادث امنیت معلومات، شامل شرایط عاجلی، حمایت می‌کند.

قزاقستان در معرض حملات مجرمین

در بهار 2021، ویب‌سایت Comparitech (مستقر در بریتانیا) که در عرصه اخبار مربوط به تکنالوجی و مصرف‌کنندگان فعال است، یک راپور درباره پرخطرترین کشورهای دنیا از نظر امنیت سایبری نشر کرد. در این راپور، کشورهای آسیای میانه، بشمول قزاقستان، تقریباً در ردیف‌های آخر قرار داشتند.

قزاقستان یکی از جذاب‌ترین کشورها برای سارقان رمزارز است. این اشخاص از کمپیوترهای آسیب‌پذیر برای تولید ارز دیجیتل، یا رمزارز، استفاده می‌کنند. این پروسه را استخراج رمزارز یا رمزارز-کاوی (کریپتو ماینینگ) می‌نامند. سارقان رمزارز، بدون کسب اجازه از مالکان کمپیوترها، از پرداخت مصارف هنگفت برق لازم برای کاوش رمزارز خودداری می‌کنند. قزاقستان، به دلیل پایین بودن مصرف برق و وجود کمپیوترهای غیر مصئون، در مقایسه با دیگر کشورهای دنیا، کشور جذابی برای متقاضیان رمزارز-کاوی محسوب می‌شود.

یکی از مهم‌ترین دلایل ناامنی کمپیوترهای قزاقستان این است که تقریباً 74% از نرم‌افزارهای نصب‌شده در کمپیوترهای قزاقستان بدون جواز است یا از منابع غیرمجاز دانلود شده است. این ادعا در جلسه 2019 کارگروپ نرم‌افزارهای کمپیوتری قزاقستان مطرح شده است.

نرم‌افزارهای بدون مجوز ممکن است حاوی نرم‌افزارهای مخرب افشاکننده دیتای مستفید باشد. همچنان، دانلود کردن به‌روزرسانی‌های امنیتی خاص برای وقایه از حملات سایبری برای این نرم‌افزارها سخت است. در نتیجه، کمپیوترهای دارای نرم‌افزارهای غیرمجاز به‌شدت در معرض نفوذ، رمزارز-کاوی، دزدی معلومات محرمانه، فریب‌کاری و دیگر انواع جرایم سایبری قرار دارد.

در بیانیه 2017 روسلان آبدیکالیکوف، رئیس کمیته امنیت معلومات وزارت سابق دفاع و صنایع هوافضا، آمده است: «تعداد حملات سایبری به سیستم‌های الکترونیکی ادارات دولتی [قزاقستان] هر سال دو برابر می‌شود.»

گروپ ملی عکس العمل عاجلی کمپیوتری قزاقستان، معروف به KZ-CERT، در نیمه نخست 2021 تعداد 11,432 فقره جرم سایبری و تهدید امنیت را ثبت کرد که این رقم در مقایسه با سال 2020 افزایش 15 فیصدی را نشان می‌دهد. به راپور KZ-CERT، بات‌نت‌ها، اسبهای تروا و ویروس‌های کمپیوتری بخشی از سافتویرهای مخربی هستند که مجرمین سایبری برای حمله به کمپیوترهای قزاقستان استفاده می‌کنند.

حملات سایبری به ماډیول‌های مدیریت محتوا WordPress (سافتویر ایجاد ویب‌سایت و تولید محتوا که در انترنت در دسترس است)، که در قزاقستان پرکاربرد است، باعث سرقت معلومات محرمانه و حساس بسیاری از مستفیدان ویب‌سایت‌ها و نشر غیرمجاز پیام‌های تروریستی و تبلیغاتی افراط‌گراها در بعضی از ویب‌سایت‌ها شده است.

مجرمین سایبری مکرراً شرکتها، نهادهای دولتی و اتباع قزاقستان را برای کسب مفاد مورد حمله قرار می‌دهند. در آگوست 2021، هیچ بانکی در قزاقستان از امکانات لازم برای محافظت از منابع انترنتی، بشمول امکانات حفظ امنیت داده، انتقال داده، رمزگذاری ترافیک و تنظیمات امنیتی، در مقابل حملات سایبری برخوردار نبود.

خنثی ساختن حملات سایبری

به گفته آندره‌ای کوریلین، مدیرکل Citibank در قزاقستان، ضعف دفاع سایبری در بانک های قزاقستان بسیار تشویش‌آور است؛ بخصوص با توجه به این که بانکهای بین‌المللی مهم مکرراً در معرض حملات سایبری هستند.

با وجود این، از زمان استقرار «سپر سایبری» در 2017، دولت قزاقستان روند تفتیش و عکس العمل فعال برای حفظ امنیت فضای مجازی کشور را تقویت کرده و تعداد حملات سایبری را کاهش چشمگیری داده است. تا سال 2019، وزارتخانه توسعه دیجیتل، نوآوری و هوافضا از دانش کافی درباره منابع و زمان‌بندی حملات سایبری علیه قزاقستان برخوردار بود. این وزارتخانه به کاهش تعداد سایت‌های در معرض نفوذ و کاهش میزان آلودگی نرم‌افزارها در این کشور کمک کرده است.

به کمک «سپر سایبری»، بیش از 300 بخش تهداب‌های اساسی، بشمول بانکها، نهادهای دولتی، کمپنی‌ها و کارخانجات سیستم‌های امنیتی خود را تقویت کرده‌اند. سرویس تخنیکی دولتی قزاقستان امکانات لازم برای جلوگیری و دفع روزانه تقریباً 1 ملیون حمله سایبری را فراهم نموده است.

در سال 2018، کمیته امنیت ملی قزاقستان دست به تاسیس «مرکز هماهنگی امنیت معلومات» (NISCC) زد. این مرکز برای محافظت از منابع معلوماتی نهادهای دولتی و معلومات مهم تهداب قزاقستان در مقابل حملات سایبری شکل گرفت. در سال 2020، NISCC انتی‌ویروس و امکانات لازم برای محافظت از سیستم‌های معلوماتی در مقابل حوادث و تهدیدات سایبری را در اختیار 17 نهاد دولتی قرار داد.

ساکنان قزاقستان، مانند این مرد در مرکز رای‌گیری در سال 2019، روزبه روز بیشتر با تکنالوژی تلیفون هوشمند آشنا می‌شوند و به همین دلیل تشویش‌های مربوط به امنیت سایبری افزایش یافته است. آژانس خبری فرانسه/تصاویر گتی

مقامات قزاقستان دریافته‌اند که عموم مردم عمدتاً با مخاطرات ابتدایی امنیت سایبری، مانند خطرهای دانلود ناخواسته نرم‌افزارهای مخرب که ممکن است زمینه‌ساز فیشینگ و فریب‌کاری آنلاین شود، ناآشنا هستند.

یکی از پرزه‌جات مهم «سپر سایبری» تربیت کارشناسان امنیت سایبری و معلومات‌رسانی به مردم درباره امنیت معلومات است. به دلیل کمبود کارشناسان حوزه تکنالوژی معلومات در قزاقستان، مقامات این کشور اقدام به اعطای بورس تحصیلی به محصلین رشته‌های مرتبط با فضای سایبری کرده‌اند. وزارت توسعه دیجیتل، نوآوری و هوافضا مسئولیت اجرای کمپاین‌های معلومات رسانی و تعلیم به مردم در قسمت مسائل امنیت سایبری را به عهده گرفته است.

در قالب پروگرام عملی «سپر سایبری»، دولت قزاقستان برای نخستین بار در تاریخ این کشور اقدام به معرفی بیمه اختیاری سایبری کرد. اشخاص حقوقی می‌توانند خسارات مادی ناشی از حملات سایبری یا درز اطلاعات را از طریق این بیمه جبران کنند.

اهمیت تعلیم

دولت می‌داند که گذار سریع کشور به عرصه اقتصاد و حکمرانی دیجیتل مستلزم مشارکت و تعلیم گسترده مردم درباره امنیت سایبری و کاهش حملات سایبری و خسارات مرتبط است. مقامات قزاقستان دریافته‌اند که عموم مردم عمدتاً با مخاطرات ابتدایی امنیت سایبری، مانند خطرهای دانلود ناخواسته نرم‌افزارهای مخرب که ممکن است زمینه‌ساز فیشینگ و فریب‌کاری آنلاین شود، ناآشنا هستند.

ضمناً، بسیاری از کمپنی‌های کوچک و متوسط کشور از دانش ابتدایی محافظت از معلومات و تکنالوژی‌های ارتباطی بی‌بهره هستند.

بنابراین، دولت اکنون تقویت روند اطلاع‌رسانی عمومی و برگزاری کمپاین‌های تعلیمی برای ارائه سامان‌های محافظت از کمپیوترها و تکنالوژی‌های ارتباطی را در دستور کار قرار داده است. بربنیاد نتایج سروی اخیر، این مساعی برای ارتقای سطح آگاهی عمومی درباره تهدیدات امنیت سایبری موثر بوده است و طبق آمار هم‌اکنون 78% مردم از دانش مرتبط مستفید هستند.

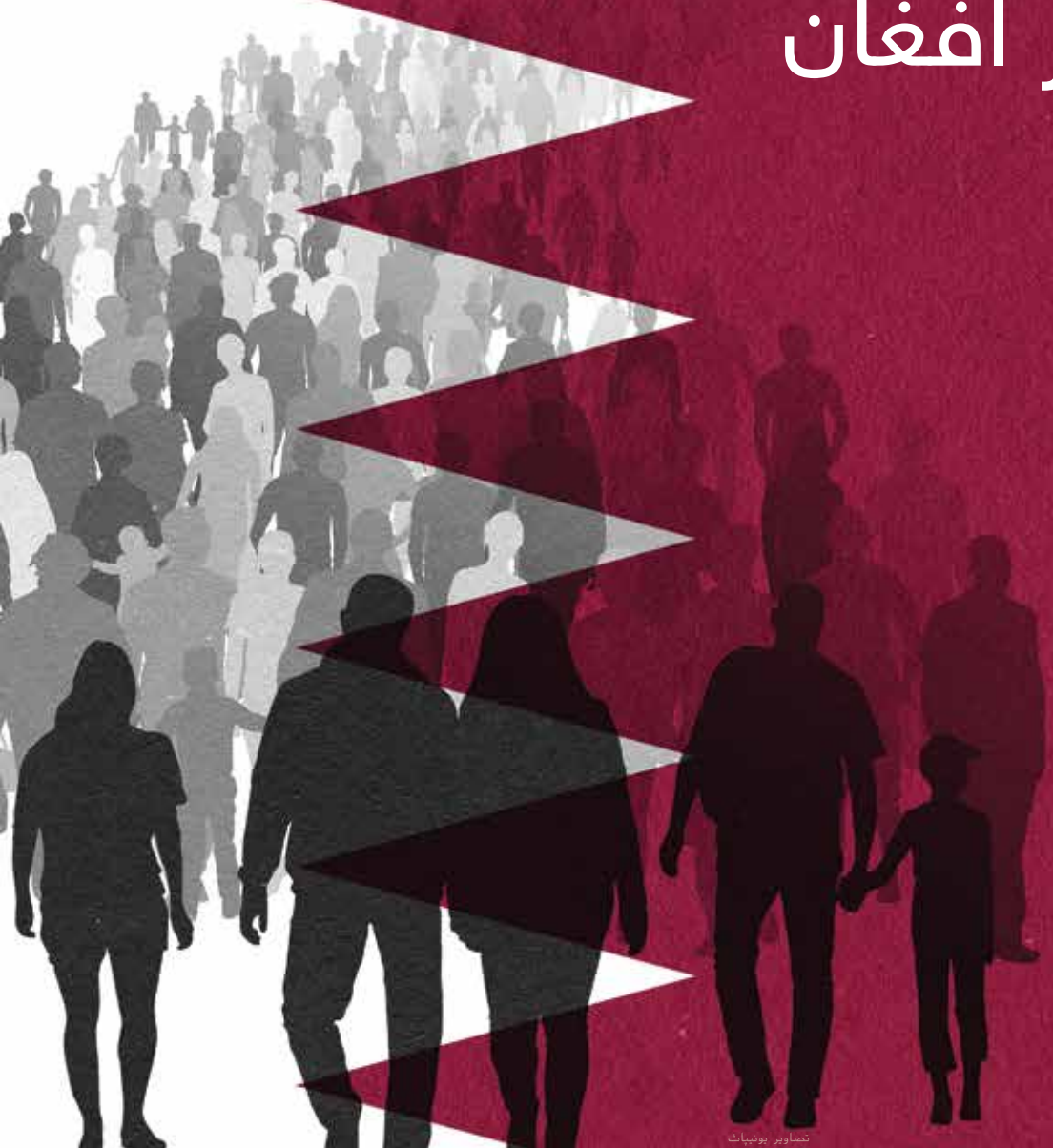
قزاقستان در قسمت سرمایه‌گذاری در حوزه آشناسازی کارمندان دولت با قوانین امنیت سایبری، معلومات و تکنالوژی و دولت الکترونیک نیز فعال بوده است. از 5 جنوری 2021، «اکادمی حکمرانی عمومی»، تحت نظر رئیس‌جمهور قزاقستان، برگزاری کورس‌های آنلاین تعلیم کارمندان دولت در قسمت دیجیتل‌سازی نهادهای دولتی را آغاز نموده است. در سال 2019، وزارت توسعه دیجیتل، نوآوری و هوافضا دوره تعلیم اونلاین رایگانی را در قسمت امنیت سایبری برای مقامات دولتی در بیش از 20 اداره دولتی و 17 نهاد دولتی محلی برگزار کرد.

در ابتدای دوره پاندیمی جهانی در 2020، بسیاری از کارمندان دولت در قزاقستان به کار کردن از راه دور روی آوردند. در سال 2020، اکادمی حکمرانی عمومی، پروگرام انکشاف سازمان ملل در قزاقستان، مرکز خدمات مدنی آستانه و سازمان امور خدمات مدنی قزاقستان پروگرام‌های تعلیمی گسترده‌ای را با هدف تقویت مهارت‌های دیجیتل و ارتباطی کارمندان دولت برای کارمندان دولت برگزار کردند.

رئیس‌جمهور، قاسم-جومارت توقایف، در سخنرانی خود خطاب به مردم در 1 سپتمبر 2021 اظهار کرد: «همه پروگرام‌های حوزه معلومات و تکنالوژی در بخش دولتی منحصراً مبتنی بر پلتفورم جدید و تحت نظارت تخنیکی دولت قزاقستان اجرا خواهد شد. به این ترتیب از دوباره‌کاری، تحمیل مصرف و کاغذبازی جلوگیری می‌شود و امکان ارائه کامل خدمات دولتی به شهروندان، ذریعه تلیفون هوشمند، فراهم می‌گردد.»

روند رو به رشد دیجیتل‌سازی خدمات دولتی ادامه خواهد یافت و سرمایه‌گذاری در قسمت تعلیم کارمندان دولت در حوزه امنیت سایبری الزامی خواهد شد. دیدگاه رئیس‌جمهور، توقایف، در حوزه دیجیتل در مورد ضرورت ارائه خدمات دولتی به طرز الکترونیکی و اتکای بخش خصوصی به تجارت الکترونیکی را نمی‌توان از تعهد او به بهبود مستمر سطح امنیت سایبری این کشور جدا دانست. ✦

کوشش مشترک، به رهبری **قطر**، برای نجات ده‌ها هزار افغان



تصاویر پوښپاڼ

مجله یونیپاث قوماندانی مرکزی ایالات متحده با برید جنرال عبدالعزیز صالح السلیطی، رئیس اداره همکاری نظامی بین‌المللی قوای مسلح قطر، که شاهد عملیات انتقال اتباع افغانستان و نقش ارزشمند و بشردوستانه رهبران قطر، بربنیاد دستورهای عالی‌جناب شیخ تمیم بن حمد آل ثانی، امیر قطر، بوده است، مصاحبه کرده است. قطر به‌سرعت از طریق عملیات انتقال و اسکان ده‌ها هزار افغان و اتباع کشورهای دیگر که در وضعیت امنیتی فوق‌العاده پیچیده آگست 2021 مجبور به خروج از افغانستان بودند، وارد عمل شد.

برید جنرال عبدالعزیز صالح السلیطی

یونیپاث: منحیث یکی از مسئولین برجسته عملیات انتقال، که یکی از کلانترین عملیات لوجستیکی سالهای اخیر به حساب می‌رود، لطفاً درباره مقدمات این عملیات و شرایط و امکانات عملیات توضیح بدهید.

برید جنرال السلیطی: بعد از این که قوای ائتلاف مکلف به خروج از افغانستان شدند، وضعیت این کشور بی‌ثبات شد. کمپاین انتقال طِبق تشویش‌های بشردوستانه و نیز نقش ملی، منطقوی و بین‌المللی رهبران سیاسی و نظامی قطر که جزو جامعه جهانی هستند، شکل گرفت. این عملیات با هم‌پیمان استراتژیک ما، ایالات متحده، نیز هماهنگ شد. مسئولین قطری، به نمایندگی از رهبر دوراندیش خود، عالی‌جناب شیخ تمیم بن حمد آل ثانی، امیر قطر، دستورهای امیر درباره ارائه پشتیبانی و حمایت همه‌جانبه را اجرا نمودند. این اقدام تاثیر مثبت و سریعی بالای روند اجرای کلانترین و سریع‌ترین عملیات انتقال قرن اخیر گذاشت.

یونیپاث: فرمان شروع عملیات انتقال چی‌قسم به شما رسید؟

برید جنرال السلیطی: ما درخواست قوماندانی مرکزی ایالات متحده را از طریق وزارت امور خارجه قطر که ورود گروپی از مردم افغانستان را به ما اطلاع می‌داد، دریافت نمودیم. ما، با هماهنگی این وزارت‌خانه، وارد عمل شدیم. در نخست، از ما درخواست شد که اتباع قطری ساکن افغانستان را که تعداد آنها به 8,000 تن می‌رسد، درجریان یک سال از افغانستان خارج کنیم. بر این بنیاد، کمپ‌های العدید و السیلیه آماده شدند و میکانیزم‌های فعالیت و ترانسپورت قسمی طراحی شد که یک بارکد و یک جواز سفر از افغانستان برای همه پروازهای ورودی صادر شود. ما اقدامات احتیاطی مربوط به وقایه از کووید-19 را قبل از هر پرواز در نظر گرفتیم. این اقدامات بسیار منظم بود ولی بعد از این که مردم، قبل از بالا شدن طیاره، به‌شکل نامنظم به آن سوار شدند، دستور تغییر کرد.

یونیپاث: چی‌قسم با قوماندانی مرکزی در قسمت جواب‌گویی به این درخواست‌ها هماهنگ شدید؟

برید جنرال السلیطی: ما از وزیر امور دفاعی دستور مستقیمی مبنی بر پشتیبانی کامل از ایالات متحده دریافت نمودیم. این عملیات محدود به قوای مسلح نبود. این عملیات حاصل کوشش مشترک وزارت امور خارجه قطر، وزارت امور خارجه ایالات متحده، قوای مسلح قطر، صندوق توسعه قطر و وزارت صحت قطر بود. شفاخانه الوکره، یکی از مجهزترین و کلانترین شفاخانه‌های قطر آماده پذیرش و تداوی مریضان پناهنده شد.

یونیپاث: کلانترین چالش عملیات انتقال چه بود؟

برید جنرال السلیطی: انتقال مریضان به شفاخانه‌های دیگر واقعاً سخت بود. بعضی مریضان بدون سند یا کارت هویتی بودند یا به امکانات خاصی ضرورت داشتند. سرعت وقوع رویدادها این مشکلات را تشدید می‌کرد ولی شیخ تمیم بن حمد آل ثانی، امیر قطر، شخصاً دستور داد که شفاخانه الوکره کاملاً آماده خدمت‌رسانی به پناه‌جویان مریض شود.

پناهندگان افغان در العدید قطر از امکانات اسکان برخوردار شدند. رویترز

یونیپاث: مسیرهای مختلفی برای عملیات انتقال در نظر گرفته شد. می‌توانید در این باره توضیح بدهید؟

برید جنرال السلیطی: ما چهار مسیر برای عملیات انتقال در نظر گرفته بودیم. نخستین مسیر مخصوص مسئولین دیپلماتیک بود که به‌آسانی برقرار شد چون دیپلمات‌ها قرار بود با اعضای فامیل خود به قطر منتقل شوند. بعضی از آنها در قطر ماندند و بعضی دیگر عازم نقاط دیگر شدند. مسیر دوم مخصوص خبرنگاران، محصلین و اتباع کشورهای دیگر بود که درخواست انتقال خود را تسلیم وزارت امور خارجه کرده بودند. این گروپ از پناهندگان در کمپ‌هایی که آماده شده بود، اسکان یافتند. مسیر سوم مخصوص کشورهایی ازقبیل هند و بنگلادش بود که خواستار انتقال اتباع خود از طریق میدان‌هوایی‌های قطر بودند.

مسیر چهارم را طیاره C-17 قوماندانی مرکزی پوشش می‌داد. این مسیر به دلیل زیاد بودن متقاضیان سفر و شدت گرفتن تهدیدات در میدان‌هوایی کابل خطرناک شده بود. آنچه مشکل را تشدید می‌کرد این بود که اشخاص باقی‌مانده در اطراف میدان‌هوایی دچار مشکلات شدید و مختلف صحی شده بودند. ما شاهد بودیم که عساکر ایالات متحده به اطفال کمک می‌کنند که از بالای حصارها عبور کنند. به دلیل ازدحام، موضوع مرگ و زندگی این اطفال در میان بود. پذیرایی از این اشخاص در مرکز مراقبت از اطفال بی‌سرپرست قطر و سازمان‌دهی آنان بربنیاد سن، یک کار فوق‌العاده بود. پروسس معلومات پاسپورت نیز از مشکلات دیگر ما بود. این اشخاص در حالی وارد قطر می‌شدند که قطر قرار بود توقفگاه بین‌راهی آنها باشد و پذیرش آنها در این کشور سخت بود. ما در آستانه برگزاری «جام عرب» که تمرینی برای برگزاری جام جهانی محسوب می‌شود، بودیم. در عین حال، تحولات و سرعت وقوع رویدادها، بخصوص خودداری یا تعلل بعضی کشورها در پذیرش این اشخاص، ما را غافلگیر ساخت. برای جلوگیری از ایجاد ازدحام، بخش ترانسپورت قوای هوایی امیرنشین قطر چندین فروند طیاره C-17 از العدید به پایگاه‌های نظامی تحت پوشش ایالات متحده و هم‌پیمانان آن اعزام کرد.

یونیپاث: ازکدام طریق توانستید این عملیات را با قوماندانی مرکزی هماهنگ کنید؟

برید جنرال السلیطی: توافق اولیه با قوماندانی مرکزی انتقال 8,000 نفر طی 12 ماه بود. هجوم 16,000 پناهنده در همان هفته نخست ما را غافلگیر ساخت. لوی درستیز و وزیر دفاع به ما دستور دادند که برای ایجاد کمپ‌های موقت با امکانات کامل و مجهز به دستگاه‌های تهویه اقدام نماییم. ما در حالی مصروف آماده‌سازی این کمپ‌ها شدیم که برای این کار صرفاً سه روز فرصت داشتیم. در این سه روز، تعداد پناهندگان از 30,000 به 40,000 و بعداً 50,000 تن رسید. مشکل اصلی ما این بود که ورود این تعداد نفر با روزهای گرم آگست همزمان شده بود و ما باید امکانات سرمایشی مناسبی را فراهم می‌کردیم. از طرف دیگر، همه گروپ‌ها باید در یک نقطه متمرکز می‌شدند تا تامین مناسب

این نقش هم‌پیمانان در قسمت همکاری و مقاومت در شرایط بحرانی، بخصوص بحران‌های بشری، است. **ما به دستاوردهای خود افتخار می‌کنیم.**

~ برید جنرال عبدالعزیز صالح السلیطی

پناهندگان افغان، بعد از این که با کوشش‌های مشترک قطر و ایالات متحده نجات یافتند، در پایگاه هوایی قطر مستقر شدند. رویترز

قطر به پناهندگان افغان خدمات صحی ارائه می‌کند.

ریاست هدایت اخلاقی

قطر در پروسه انتقال شهروندان افغانستان و اتباع خارجی مشارکت می‌کند.

ریاست هدایت اخلاقی

و منظم امکانات ضروری میسر شود. ما حتی در اجرای امور عادی نیز با مشکل روبرو شده بودیم. بطورمثال، ازدحام باعث وقوع مشکلات صحی و اجرایی شده بود که در این زمینه وزارت شهرنشینی وارد عمل شد. ما همه اقدامات لازم را انجام دادیم و به فعالیت خود شدت بخشیدیم. در مورد غذا، بسته‌های غذایی آماده در دسترس پناهندگان قرار گرفت. همچنان یک مرکز عملیات در ترمینال میدان‌هوایی العدید تشکیل شد. این مرکز را گرتا هولتز، کاردار سابق ایالات متحده که مسئولیت عملیات انتقال و اسکان را به عهده گرفته بود، اداره می‌کرد. از طرف قطر نیز اعضای وزارت امور خارجه؛ اداره همکاری نظامی بین‌المللی، تدارکات و خدمات صحی قوای مسلح؛ و وزارت کشور، گمرک، وزارت صحت، خدمات امبولانس و خیریه قطر وارد عمل شده بودند. در بخش پشتی نیز مرکزی ویژه قوای مسلح ایجاد شد. این مرکز را محمد حمد النعیمی، رئیس عملیات، اداره می‌کرد. گروپی از وزارت صحت، کار پشتیبانی از این مرکز را آغاز کرد. به دلیل تقاضای بالا و فرصت محدود انتقال، این موضوع که طیاره‌ها فقط پناهندگان را منتقل می‌کردند و عملیات انتقال طبق پلان پیش نمی‌رفت، ما را غافلگیر ساخته بود. طیاره‌ها بطورمنظم مردم را از کابل به قطر منتقل می‌کردند و به تعداد پناهندگان می‌افزودند. حتی یک بار در فاصله صبح الی چاشت در هر 90 دقیقه 900 پناهنده وارد قطر می‌شدند. این تعداد به 4,000 نفر در روز رسید و ما باید امکانات ترانسپورت را فراهم می‌کردیم. ظرفیت میدان هوایی قسمی نبود که بتواند بیش از 10,000 نفر را طی پنج یا شش ساعت پذیرش کند و جابجا کردن این جمعیت سخت بود. گاهی الی 40 فروند طیاره C-17، ضمن طیاره‌های ورودی از دیگر کشورها، بالای باند دیده می‌شد. رسیدگی به این مشکلات نیازمند روحیه جمعی و هماهنگی فوق‌العاده بود. خوشبختانه من شخصاً به همراه دگر جنرال گریگوری گیلوت، قومندان قوای هوایی قوماندانی مرکزی ایالات متحده، و برید جنرال جرالد دونهو، قومندان لوای هوایی اعزامی 379، شاهد این کوشش‌ها بود. ما در میدان هوایی با هم ملاقات کردیم و برای برای مقابله با چالش‌ها و غلبه بر موانع با هم کار نمودیم. عساکر آمریکایی مستقر در العدید از هیچ کوششی دریغ نکردند. برای هر 3,000 نفر، یک دگروال اردوی ایالات متحده با همه ماموران خود شبانه‌روزی و بی‌وقفه در کنار اعضای قوای مسلح قطر و مامورین وزارت امور خارجه کوشش می‌کردند. همه این کوشش‌ها با موفقیت همراه شد. به یاد دارم که یک روز سفیر هولتز اعلان کرد که باید پروازهای خارجی متوقف شود و پروازها به طیاره‌های ورودی از کابل محدود شود. او می‌گفت که بعد از چند ساعت این تعداد چند برابر خواهد شد و ظرفیت امکاناتی محدود خواهد شد. او می‌گفت که ما با چالش‌های بسیاری روبرو خواهیم شد و چاره‌ای جز پذیرش یا عدم پذیرش طیاره‌های ورودی از کابل نخواهیم داشت. این نظر قومندان اعلی بود و ما لوی درستیز را از موضوع مطلع ساختیم. لوی درستیز با وزیر و سپس قومندان اعلی کشور تماس گرفت. تصمیم بر آن شد که عقب‌نشینی نکنیم و از هم‌پیمان استراتژیک خود، ایالات متحده، در قسمت پذیرش پناهندگان و تامین پناهگاه پشتیبانی کنیم. بعد از این تصمیم‌گیری، پیش‌بینی شد که احتمالاً باید پذیرای 30,000 نفر باشیم. قبلاً 16,000 پناهنده وارد شده بودند و به این ترتیب تعداد پناهندگان به 46,000 می‌رسید. این تعداد فراتر از ظرفیت کمپ‌ها بود. من با سفیر عیسی المنایی، مدیر اداره امور ایالات متحده در وزارت امور خارجه، تماس گرفتم. تصمیم گرفته شد که قطر طیاره‌های بیشتری برای انتقال پناهندگان اختصاص دهد.

من از سفیر عیسی خواستم که درخواستی را تسلیم وزارت امور خارجه کند. همچنان با رئیس ستاد قوای مسلح قطر، دگر جنرال غانم بن شاهین، تماس گرفتم و راپوری به ایشان ارائه کردم که عمدتاً به وضعیت پناهندگان در پنج تا هفت روز گذشته مربوط می‌شد. آنان قبل از ورود از سرپناه و غذا محروم شده بودند و گرمای هوا باعث فرسودگی و خسنگی شدید بیشتر آنان شده بود. من خواستار استفاده از یک فروند طیاره C-17 شدم. البته در این راستا محدودیت داشتیم و تعدادی از این طیاره‌ها مصروف اجرای ماموریت‌های دیگری بودند. لوی درستیز این درخواست را به داکتر خالد بن محمد العطیه، وزیر دفاع، ارجاع داد و به این‌ترتیب درخواست به عالی‌جناب امیر رسید. به دستور امیر 10 فروند طیارهٔ مسافربری قطری به انتقال پناهندگان اختصاص یافت که این دستور یک اقدام مهمی برای جلوگیری از ایجاد ازدحام بود. بعد از انتقال پناهندگان با 10 طیاره اول، خواستار 10 فروند طیاره دیگر شدیم که این طیاره‌ها در اختیار ما قرار گرفت. ضمناً، شفاخانه الوکره همه کارمندان و تجهیزات خود را بسیج نمود که این اقدام 35 ملیون دالر مصرف به قوای مسلح تحمیل کرد.

این نقش هم‌پیمانان در قسمت همکاری و مقاومت در شرایط بحرانی،

قطر در جریان توقف اضطراری پناه‌جویان افغان در العدید، برای آنان امکانات حمام سیار و روشویی فراهم ساخت. رویترز

بخصوص بحران‌های بشری، است. ما به دستاوردهای خود افتخار می‌کنیم. ما از دیرباز هم‌پیمان ایالات متحده بوده‌ایم. در دهه 90 میلادی، قوای امریکایی در کمپ‌هایی در مرز قطر مستقر بودند. این کمپ‌ها بعداً به پایگاه هوایی العدید تبدیل شد. این پایگاه به مرکز کسب آمادگی برای پشتیبانی از هم‌پیمان ما، ایالات متحده، مبدل شد و این کارکرد همچنان برقرار است. العدید یک نمونه بارز است. العدید از پایگاه‌های مشترک قوای قطری و امریکایی است. در سالهای اخیر، استفاده قوای مسلح قطر از تسلیحات امریکایی افزایش یافته است. همکاری بین این دو کشور باعث تقویت دانش تخصصی قوا و تقویت حضور قوای امریکایی در پایگاه‌های ما شده است. این وضعیت شرایط ثبات منطقه را بهبود بخشیده است. ما قدردان کوشش قوای امریکایی هستیم.

پروسه گسترش و پیشرفت پایگاه هوایی العدید در مراحل اولیه است. ما قصد داریم این محدوده را طی چند مرحله برای قوای قطری و امریکایی گسترش دهیم (طرح توسعه پایگاه هوایی العدید).

یونیپاث: اگر توضیحات تکمیلی دارید، لطفاً ارائه کنید؟

برید جنرال السلیطی: میخواهم روحیه جمعی و فضای مثبت حاکم بر عملیات انتقال را تحسین کنم. از همه کسانی که در اجرای این ماموریت بشردوستانه سخت با ما همکاری نمودند، تشکر می‌کنم. رسیدن به این موفقیت بدون حمایت عالی‌جناب شیخ تمیم بن حمد آل ثانی، امیر قطر، و پیگیری‌های محترم آقای داکتر خالد بن محمد العطیه، معاون صدراعظم و وزیر امور دفاعی، امکان‌پذیر نمی‌شد. شخص لوی درستیز، دگر جنرال غانم بن شاهین الغانم، با پشتیبانی و مداخله مستقیم دگر جنرال سالم بن حمد النبیط، از قوای هوایی امیرنشین قطر (رئیس فعلی ستاد کل قوای مسلح قطر) بر این ماموریت نظارت کردند. همچنان از قوای اصلی، یعنی پولیس نظامی، تدارکات، اداره عملیات و پایگاه هوایی العدید تشکر می‌کنم. از برید جنرال یوسف شاهین العتیق، قومندان پایگاه، و نیز اداره معلومات و اداره همکاری نظامی بین‌المللی، قدردانی ویژه می‌کنم.

در مورد نهادهای غیرنظامی، نمی‌توان نقش مهم وزارت امور خارجه را نادیده گرفت. از این جایگاه از لولو الخطیر، معاون وزیر امور خارجه؛ عیسی محمد المنایی، مدیر اداره امور ایالات متحده در وزارت امور خارجه؛ و همه کارمندان وزارت امور خارجه صمیمانه تشکر می‌کنم. همچنان بطور ویژه قدردان جناب سرلشگر عبدا... المال، وزیر داخله و همه کارمندان این وزارتخانه هستم. از اداره گمرک، وزارت صحت، وزارت شهرنشینی و همه اشخاصی که در موفقیت این ماموریت بشردوستانه نقش داشتند، صمیمانه تشکر می‌کنم. بدون مشیت الهی و حمایت این اشخاص و نهادها، این وضعیت به بحران انسانی تبدیل می‌شد. از شما بسیار تشکر! خداوند رهبر، مردم و دولت قطر را حفظ کند. ✦

تصاویر یونیپاث

تقویت شبکه‌های نظامی

وزارت دفاع عراق یک گروپ امنیت سایبری برای شناسایی و مقابله با حملات سایبری ایجاد کرد

کارکنان یونیپاث

با انکشاف سریع انترنت و تلیفون‌های همراه، تکنالوجی به یکی از ضرورت‌های زندگی روزمره مردم مبدل شده است. این تکنالوژی‌ها همه بخشهای جامعه، ازجمله تعلیم، صحت، انجینری، امنیت و اقتصاد را متحول ساخته است. البته، سوءاستفاده مجرمین سازمان‌یافته و تروریست‌ها از این تکنالوژی‌های باعث شده است که کشورها گروپ‌های امنیت سایبری را برای محافظت از شبکه‌های خود در مقابل حملات سایبری تشکیل دهند. مجله یونیپاث با تورن جنرال ستاد رعد شاکر الکنانی، مدیر اداره ارتباطات نظامی وزارت دفاع عراق درباره وظایف و دستاوردهای گروپ امنیت سایبری وزارتخانه گفتگو نموده است.

یونیپاث: اداره شما چه اقداماتی برای محافظت از عراق در مقابل حملات سایبری انجام داده است؟

تورن جنرال رعد: ماموریت اصلی اداره ارتباطات نظامی در حوزه امنیت سایبری محافظت از سیستم‌ها و شبکه وزارت دفاع عراق و انکشاف پالیسی‌های خاص در قسمت روش استفاده از دستگاه‌ها و شبکه‌های متعلق به وزارتخانه و جزوتام‌های آن است. پس، این اداره با هدف تضمین به‌کارگیری پروسیجرهای جلوگیری از حملات سایبری، محدودیت‌ها و رهنمودهای خاصی درباره امنیت معلومات وضع نموده است. ما، برای تضمین محافظت از شبکه‌های سرّی و محرمانه در مقابل دسترسی همگانی و جداسازی آنها از شبکه‌های عمومی مانند انترنت، با اداره طراحی و مدیریت شبکه همکاری می‌کنیم. البته پروسیجرهای دیگری نیز با همکاری ادارات تخنیکی مرتبط اجرا می‌شود. اصطلاح شبکه بسته درباره شبکه‌های حاوی ایمیل‌ها، صفحه‌های انترنتی و قراردادهای نظامی کاربرد دارد. ما یک شبکه عمومی آنلاین نیز داریم که مستقل از شبکه بسته عمل می‌کند. این شبکه از طریق ویب‌سایت رسمی وزارتخانه مدیریت می‌شود و برای خدمت‌رسانی به مردم طراحی شده است.

ما جلسات اطلاع‌رسانی درباره مخاطرات تروریزم سایبری و ضرورت مراعات رهنمودهای وزارتخانه را برای کاربران شبکه برگزار می‌کنیم تا این شبکه را در مقابل نفوذ امن کنیم. ضمناً، ممنوعیت استفاده از USB شخصی در دستگاه‌های وزارتخانه یا ممنوعیت استفاده از لوح فشرده برای دیدن فلم یا بازی اونلاین مورد تاکید قرار گرفته است و دانلود پروگرام‌های خارجی در دستگاه‌ها شدیداً منع است.

همکاری در این حوزه از ضروریات حفظ امنیت شبکه ملی و ایجاد روابط سازنده با دیگر نهادهای تخصصی امنیتی است. این همکاری باعث تبادل معلومات و اجرای شیوه‌های مطلوب در مقابل تهدیدات و حملات می‌شود.

یونیپاث: این وزارتخانه برای تقویت امنیت سایبری چگونه با نهادهای امنیتی دیگر همکاری می‌کند؟

تورن جنرال رعد: ما با دیگر نهادهای امنیتی در حوزه امنیت سایبری از طریق کمیته‌هایی مانند «کمیته عالی ارتباطات و امنیت معلومات» و کمیته مسئول انکشاف ستراتیژی ملی امنیت سایبری همکاری مستقیم داریم. مباحثی نیز درباره قانون جرایم سایبری و همکاری با گروپ ملی عکس‌العمل عاجلی حوادث کمپیوتری مطرح شده است. همکاری در این حوزه از ضروریات حفظ امنیت شبکه ملی و ایجاد روابط سازنده با دیگر نهادهای تخصصی امنیتی است. این همکاری باعث تبادل اطلاعات و اجرای شیوه‌های مطلوب در مقابل تهدیدات و حملات می‌شود. این ضمن همکاری ما با دوستان‌مان در قوای ائتلاف،

از طریق قرارگاه مشترک عملیات، است. تبادل اطلاعات امنیت سایبری و اطلاعات به‌دست‌آمده از دستگاه‌های موجود در مخفیگاه‌های تروریست‌ها و پروگرام‌های هک و نفوذ در ویب‌سایت‌ها ما را قادر به مقابله با حملات تروریستی علیه ویب‌سایت‌های داخلی می‌کند.

صاحب‌منصبان متخصص در حوزه امنیت معلومات باید در همه ساختارها مستقر شوند و از تعلیمات گروپ امنیت سایبری مستفید گردند. این صاحب‌منصبان باید عساکر را درباره ضرورت مراعات رهنمودهای امنیتی تعلیم دهند.

یونیپاث: نقش شما در محافظت از مراکز رای‌گیری در مقابل حملات اونلاین چیست؟

تورن جنرال رعد: منحیث وزارتخانه دفاعی، ما موظف به محافظت از مراکز رای‌گیری در مقابل حملات تروریستی یا شورش‌های رایج هستیم، و اداره ارتباطات نظامی وظیفه‌ای برای محافظت از این مراکز در مقابل حملات سایبری ندارد. البته، قسمی که ذکر شد، ما با دیگر نهادهای تخصصی امنیتی در حوزه امنیت سایبری برای محافظت از شبکه ملی در مقابل حملات خارجی همکاری می‌کنیم و تا فعلاً کدام راپور درباره نفوذ یا فعالیت غیرعادی دریافت نکرده‌ایم.

یونیپاث: آیا وظیفه شما به محافظت از تاسیسات وزارت دفاع محدود می‌شود یا دیگر مراکز دولتی و خصوصی را نیز شامل می‌شود؟

تورن جنرال رعد: وظیفه اداره ارتباطات نظامی به محافظت از تاسیسات وزارت دفاع محدود می‌شود که این وظیفه را با همکاری ادارات تخنیکی مرتبط انجام می‌دهیم. البته، امنیت سایبری شبکه‌های وزارتخانه را نمی‌توان مساله‌ای مستقل از دیگر شبکه‌های دولتی دانست. بنابراین، طرز مثال ما باید مطمئن شویم که دستگاه‌های وزارتخانه در مقابل نفوذ امن هستند یا این که شبکه ما به ابزاری برای حمله به دیگر صفحه‌های انترنتی مهم دولتی تبدیل نمی‌شود. رسیدن به این هدف مستلزم تعلیم کارمندان در قسمت مخاطرات تهدیدات سایبری و روش حفظ امنیت شبکه است. همزمان با حفظ هشیاری برای محافظت از شبکه در مقابل تهدیدات خارجی، باید ورودی‌ها و خروجی‌های آنلاین شبکه وزارتخانه و دیتای خروجی از دیگر شبکه‌های دولتی را تفتیش کنیم. ما از پروگرام‌های تشخیص نرم‌افزار مخرب و شناسایی ویروس، که منظماً اپدیت می‌شوند، استفاده می‌کنیم.

یونیپاث: چگونه مانع استفاده از دستگاه‌های فاقد امکانات رمزگذاری می‌شوید؟

تورن جنرال رعد: چندی قبل اداره امنیت سایبری وزارت دفاع برای حفظ همگامی با روند پیشرفت‌های سریع جهانی در حوزه تکنالوژی تشکیل شد. به دلیل این که عراق قبل از سال 2003 در جهان منزوی بود، طی دو دهه گذشته امکان همگام شدن با تحولات تکنالوژی برای ما فراهم نشد. تلیفون‌های همراه به ابزار ترجیحی ارتباط تبدیل شده‌اند. امکان ملزم ساختن همه جزوتام‌های نظامی به مراعات ممنوعیت استفاده از تلیفون همراه برای ارتباطات نظامی یا انتقال معلومات مربوط به عملیات نظامی از میدان جنگ، وجود نداشت. بعضی عساکر ما از رویدادهای میدان جنگ عکس و فلم تهیه می‌کردند و بعضی قومندانان در وقت جنگ از تلیفون همراه استفاده می‌کردند. در این راستا اقدامات لازم صورت گرفته است. طرزالعمل‌ها و رهنمودهای خاصی برای جلوگیری از مصرف دستگاه‌ها و سامان‌های ارتباطی غیر مصئون و رمزگذاری‌نشده وجود دارد. جواز مصرف منحصراً برای دستگاه‌های رمزگذاری‌شده، مصئون و مورد تایید اداره ارتباطات نظامی صادر شده است. البته، این تخلفات حتی در پیشرفته‌ترین اردوها نیز رخ می‌دهد. بنابراین، صاحب‌منصبان متخصص در حوزه امنیت معلومات باید در همه ساختارها مستقر شوند و از تعلیمات گروپ امنیت سایبری مستفید گردند. این صاحب‌منصبان باید عساکر را درباره ضرورت مراعات رهنمودهای امنیتی تعلیم دهند.

یونیپاث: شما در سپتمبر *2021* در جلسه گروپ عکس‌العمل عاجلی امنیت سایبری اشتراک کردید. در این نشست چه پیشنهاداتی مطرح شد؟

تورن جنرال رعد: نتایج این جلسه اهمیت فوق‌العاده‌ای داشت و مباحث بالای تهدیدات واقعی جاری متمرکز بود. من از اشتراک در این جلسه راضی بودم و ضمن دیدار با برادران‌مان در دیگر سرویس‌های امنیتی، با آخرین شگردهای آنان آشنا شدم و از تجربیات آنان در این حوزه استفاده گرفتم. از توصیه‌های جلسه امنیت سایبری می‌توان به اینها اشاره نمود:

1. اجرای طرحی برای ارائه پروگرام انکشاف امنیت سایبری در همه موسسات دولتی.
2. تصویب پروگرام تعلیمی پوهنتونی و حرفوی و مطالعات تخصصی عالی در حوزه امنیت سایبری در وزارت تحصیلات عالی و تحقیقات علمی.
3. جذب اشخاص شایسته از طریق تشکیل انجمن خبرگان، اشخاص آماتور و متخصصین در حوزه امنیت سایبری. برای رسیدن به این هدف، «صندوق انکشاف ابتکار اجتماعی» با حمایت سازمان‌های مردم‌نهاد و بخش خصوصی ایجاد شد.

4. «گروپ عکس‌العمل عاجلی کمپیوتری عراق» (IQCERT)، وزارت تحصیلات عالی و تحقیقات علمی، کمپنی‌های خصوصی و سازمان‌های عمومی با تعلیم و تقویت گروپ‌های گروپ واکنش به حوادث سایبری محلی موافقت کردند. گروپ عکس‌العمل عاجلی کمپیوتری عراق مقرراتی را برای کمپنی‌های حوزه امنیت سایبری و پروگرامی ستراتیژیک را برای ارتقای جایگاه شاخص جهانی امنیت سایبری عراق انکشاف کرد.

یونیپاث: وزارتخانه برای انتخاب و آماده‌سازی گروپ امنیت سایبری کدام پروسه را سپری می‌کند؟

تورن جنرال رعد: اعضای گروپ از بین کارمندان اداره تخنیکی تخصصی وابسته به وزارت دفاع عراق انتخاب می‌شوند. اعضای گروپ باید ماموربن و انجینران وزیده و ماهر حوزه امنیت سایبری باشند و داوطلبان باید پروسه بازرسی امنیتی را طی کرده باشند.

یونیپاث: قوانین پیگرد مجرمین سایبری در عراق چقدر سختگیرانه است؟

تورن جنرال رعد: تا اواخر 2021، عراق هنوز قانونی در قسمت جرایم سایبری نداشت ولی مسوده این قانون قرار است در شورای نمایندگان تصویب شود و بعداً برای تایید در اختیار دولت قرار بگیرد. ما امیدوار هستیم که تصویب این قانون زمینه تعقیب و مجازات مرتکبین جرایم سایبری را فراهم کند و مانع از این شود که گروپ‌های جرایم سایبری سازمان‌یافته از شبکه ملی عراق منحیث یک سامان برای حمله به دیگر سیستم‌های دولتی، با هدف اخاذی یا خرابکاری، استفاده کنند.

حفظ امنیت سایبری وظیفه‌ای همگانی است و حتی نفوذ در کمپیوترهای دوردست می‌تواند تاثیر مستقیمی بالای شبکه‌های کشورهای دیگر بگذارد.

یونیپاث: در قسمت بهبود تکنالوژی‌های سایبری، چقدر با کشورهای دوست همکاری می‌کنید؟

تورن جنرال رعد: حفظ امنیت سایبری وظیفه‌ای همگانی است و حتی نفوذ در کمپیوترهای دوردست می‌تواند تاثیر مستقیمی بالای شبکه‌های کشورهای دیگر بگذارد. هدف از دوردست، دوردستی جغرافیایی، و نه الکترونیکی، است. عصر دیجیتل باعث اتصال همه مردم دنیا به یکدیگر شده است و مکان دوردستی باقی نگذاشته است. با وجود مزایای بی‌شمار عصر دیجیتل، مخاطرات کلانی ما را تهدید می‌کند. بنابراین، ما باید برای مقابله با اشخاصی که از تکنالوژی معلوماتی برای اهداف مجرمانه، محلی یا فرا ملی، استفاده می‌کنند، هشیار باشیم. انترنت، ایمیل و صفحات شبکه‌های مجازی دنیا را به دهکده تبدیل نموده است و در عین حال زمینه انتشار سریع سافتویرهای مخرب و ویروس‌ها را فراهم کرده است. بنابراین، همکاری و تبادل معلومات بین‌المللی بین کشورهای دوست ضروری به نظر می‌رسد. همکاری با کشورهای دوست از طریق برگزاری دوره‌های تخصصی امنیت سایبری و اجرای مانورها و نمایشگاه‌هایی مانند نمایشگاه جنگجوی سایبری که دفتر همکاری دفاعی سفارت ایالات متحده در 2020 برگزار کرد، صورت می‌گیرد. این کورس‌ها و مانورها منافع بسیاری برای اشتراک‌کنندگان دارد.

ما برای حفظ سطح کارآمدی خود، مشتاق جذب اشخاص دارای مهارت‌های برجسته از میان فارغ‌التحصیلان پوهنتونی عراق و کارمندان وزارت دفاع عراق هستیم.

یونیپاث: اداره سگنال و ارتباطات وزارت دفاع چگونه خود را با تحولات سریع تکنالوژی همگام می‌سازد؟

تورن جنرال رعد: ما گروپی از کارشناسان مسلکی در حوزه تحقیقات و تفتیش تحولات تکنالوجی را گرد هم آورده‌ایم و در پی اشتراک در جلسات و ورکشاپ‌های مسلکی امنیت سایبری هستیم. در قسمت تقویت مهارت‌های کارمندان، ما با مراکز تحقیق و انکشاف وزارتخانه و پوهنتون‌های تخنیکی همکاری می‌کنیم. ضمناً، ما قصد داریم تعدادی از کارمندان خود را به کورس‌های تخصصی ناتو یا کشورهای هم‌پیمان اعزام کنیم. ما برای حفظ سطح کارآمدی خود، مشتاق جذب اشخاص دارای مهارت‌های برجسته از میان فارغ‌التحصیلان دانشگاهی عراق و کارمندان وزارت دفاع عراق هستیم.

یونیپاث: آیا داعش تا فعلاً حملات سایبری علیه صفحه‌های انترنتی وزارت دفاع ترتیب داده است؟

تورن جنرال رعد: خیر، داعش تا فعلاً به صفحه‌های انترنتی وزارت دفاع حمله سایبری نکرده است. شاید دلیل این خودداری این باشد که شبکه وزارتخانه از نظر تخنیکی کاملاً تقویت شده است و گروپی از کارشناسان مجرب امنیت معلومات از آن پشتیبانی می‌کنند. همچنان، این شبکه را می‌توان شبکه بسته‌ای برای تحرکات و قوا دانست. ✦

عسکر وفادار به دولت مشروع یمن در حال بررسی میدان جنگ در ولایت مأرب. با وجود مساعی بین‌المللی برای ایجاد آتش‌بس، حوثی‌ها تا فعلاً هم جنگ را متوقف نکرده‌اند.

آژانس خبری فرانسه/تصاویر گتی

دفاع از تمامیت ارضی یمن

دخالت ایران مانع رسیدن یمنی‌ها به توافق سیاسی برای خاتمه دادن به جنگ داخلی میباشد

داکتر احمد عواد بن مبارک، وزیر خارجه، یمن

جنگ یمن سال هفتم خود را پشت سر گذاشت. شبه‌نظامیان حوثی این جنگ را بعد از کودتا علیه دولت قانونی یمن به مردم این کشور تحمیل نمودند. این جنگ به دلیل مساعی شبه‌نظامیان حوثی برای کسب قدرت، و نیز سعی برای تغییر ماهیت جامعه یمن، منحرف ساختن پروگرام‌های آینده کشور و منطقه از طریق جذب گسترده اطفال و آشناسازی جوانان با اعمال خشونت، درگیری و نفرت‌پراکنی بین مردم کشور، عواقب خطرناکی داشته است. ضمناً، حوثی‌ها در پی گسترش جهل در جامعه هستند تا بتوانند به‌راحتی به مردم مسلط شوند. آنها برای تضعیف یمن و سوءاستفاده از آنها برای اشتراک در جنگ سعی می‌کنند. همه این شرایط زمینه را برای تبدیل شدن یمن به یکی از ارکان ستراتیژی توسعه‌گرایی ایران در منطقه آماده نموده است.

نقشه ایران فعلاً آشکار شده است. شبه‌نظامیان تحت حمایت ایران شبه‌جزیره عربستان را محاصره کرده‌اند. وجود امکانات نظامی باکیفیت باعث گسترده شدن خطر شده است. شکی نیست که شکست نقشه ایران در یمن باعث تضمین شکست نقشه ایران در تمام منطقه می‌شود. موفقیت ایران در یمن درگیری را وارد مرحله جدیدی می‌کند و چرخه دیگری از خشونت و آشوب را پدید می‌آورد. من سعی می‌کنم که شرایط امروز و چشم‌انداز صلح در یمن را تشریح کنم.

در این مرحله از جنگ، ولایت مأرب در کانون توجه علاقمندان مندان به مسائل یمن قرار گرفته است. از نومبر 2020، شبه‌نظامیان حوثی حملات مستمری علیه مأرب ترتیب داده‌اند. این حملات ناشی از دشمنی‌هایی است که زیان آنها از توهم قدرت شبه‌نظامیان در تصرف

حضور اطفال یمنی در صنف درس در کمپ بیجاشدگان در حدیده. اینان قربانیان جنگی هستند که حوثی‌ها به نفع ایران در یمن به راه انداخته اند. جنگ باعث شده است که 2 ملیون طفل در سن مکتب از دسترسی به خدمات تعلیمی عادی محروم شوند.

آژانس خبری فرانسه/تصاویر گتی

این ولایت و توهم کلانتر کنترول یمن با توسل به خشونت، تروریزم و قوای نظامی کمتر نیست.

ولایت مأرب، با جایگاه تاریخی خاص، اهمیت ملی و ستراتیژیک یافته است. این واقعیت ممکن است فراموش شده باشد که مردم مأرب که نفوس آن از 350,000 نفر تجاوز نمی‌کند، حوثی‌ها را در سال 2015 با امکانات جنگی که در مقایسه با امکانات امروز ناچیز بود، شکست دادند. امکانات این ولایت امروز بسیار بیشتر است. این ولایت با جمعیتی بالغ بر 4 میلیون نفر که در میان آنها 2 میلیون نفر بیجاشده داخلی هستند، به پناهگاه یمنی‌ها با تعلقات مختلف اجتماعی و سیاسی تبدیل شده است. این جمعیت حامی اردوی است که از گرایش ملی و اراده قاطع و محکمی برای خنثی ساختن نقشه حوثی‌ها برخوردار است.

با وجود این، باید توجه داشت که بعضی ذینفعان با مطرح نمودن سناریو پس-مأرب دچار اشتباه محاسباتی شده‌اند. اگر ما به سناریو غیرواقع‌بینانه بپردازیم، بدون شک خواهیم گفت که تسلط حوثی‌ها بر مأرب به اندازه نابود شدن سد مشهور آن زیان‌بار خواهد بود. امروز، مأرب دیوار نفوذناپذیر یمن است. این ولایت به یکی از اولویت‌های ستراتیژیک رژیم ایران تبدیل شده است. سقوط مأرب نه تنها زمینه‌ساز فاجعه بشری خواهد شد، بلکه پروسه سیاسی رسیدن به صلح در یمن را نیز مختل خواهد کرد. این اتفاق نقطه خاتمه بازگشت امنیت و ثبات خواهد بود. آشفتگی شیوع خواهد یافت و در پی آن خشونت، کشمکش‌های داخلی و امواج مهاجرت شکل خواهد گرفت. این اتفاق می‌تواند زمینه‌ساز دوره ماندگار بی‌ثباتی شود و شرایط را برای گسترش جنگ از یمن به دیگر نقاط منطقه فراهم کند.

چشم‌انداز و رویکرد ما در دولت یمن به شرح ذیل است: جایگزینی برای صلح در یمن وجود ندارد. صلح حقیقی، فراگیر و پایدار باید با رفع ریشه‌های سیاسی جنگ که سعی شبه‌نظامیان حوثی برای تحمیل حضور خود و تسلط اجباری بر یمن نماد آن است، شکل بگیرد.

با وجود مداخله مخرب ایران در یمن، با وجود حمایت نظامی ایران از شبه‌نظامیان حوثی و تامین مالی ماشین جنگی این گروپ، معرفی جنگ یمن منحیث جنگ نیابتی منطقوی سوءتفاهمی است که باید برطرف شود. رسیدن به توافق صلح در یمن بدون اقدام یمنی‌ها برای حل مشکلات داخلی طبق نتایج «نشست مذاکرات جامع ملی» و توزیع عادلانه قدرت و ثروت امکان‌پذیر نخواهد بود.

البته، در عین حال، ابعاد جغرافیایی-ستراتیژیک دخالت ایران در یمن و علاقه ایران به نزدیک‌تر شدن به دریای سرخ و دریای عربستان نباید نادیده گرفته شود. این رویکرد می‌تواند ارزش افزوده استراتیژیک نظامی برای ایران ایجاد کند و رقابت منطقوی و بین‌المللی را تشدید نماید.

سرمایه‌گذاری ایران در جنبش حوثی از مدت‌ها قبل آغاز شده بود و در ابتدای هزاره دوم به اوج رسید. اقدام قوای بحری ایالات متحده در توقیف کشتی‌های ایرانی «جهان 1» و «جهان 2» که قصد داشتند به حوثی‌ها سلاح و موشک برسانند، گواه این مدعاست. این اتفاق چند سال قبل از شروع جنبش حوثی رخ داده بود. به این ترتیب می‌توانیم این ادعا را که جنگ فعلی دلیل اصلی مداخله ایران در یمن است، تقویت کنیم.

از دیگر سوءبرداشت‌های مهم می‌توان به این نکته اشاره نمود که حوثی‌ها

کشتی جنگی ایالات متحده قایقی را که محموله کود کیمیاوی را برای ساخت مواد انفجاری به یمن حمل می‌کرد، توقیف کرد.

آسوشیتد پرس

هر بار که دست به پیشروی نظامی می‌زنند، پیشنهاد صلح را رد می‌کنند. در واقع، آنها پیشنهاد صلح را، صرف‌نظر از این که در حال پیشروی یا عقب‌نشینی باشند، بربنیاد اصلی ستراتیژیک رد می‌کنند و از صلح منحیث ترفندی در چوکات ستراتیژی نظامی خود استفاده می‌کنند. در این زمینه شواهد فراوانی در دست داریم. شفاف‌ترین دلیل شاید «قرارداد استکهلم» باشد که شبه‌نظامیان حوثی آن را در دسمبر 2018 بدون اجرای هیچ‌یک از مواد آن قبول کردند.

درک این موضوع به به ما یاری میرساند تا رویکرد مناسب برای دستیابی به صلح با گروهی را درک کنیم که محاسبات اش بر مبنای حقایق نبوده، بلکه بر مبنی یک تفکر خداسالاری مبتنی بر توهم ادعای حاکمیت الهی برای حکومت است. این وحشتناک‌ترین مانع رسیدن به توافق صلح در همه دوره‌ها، از جنوا تا کویت و حتی استکهلم بوده است. اگر این واقعیت صریح را در ذهن داشته باشیم، می‌توانیم مدعی شویم که مهم‌ترین امتحان برای شبه‌نظامیان حوثی -امتحانی که پیوسته آن را رد می‌کنند- پذیرش آتش‌بس جامع، به‌عنوان مهم‌ترین اقدام بشردوستانه، است. دیگر مسائل مهم انسانی را می‌توان قبل از شروع مذاکرات بررسی و برای آنها راهکار سیاسی جامع پیدا نمود.

ما به این باور هستیم که همبستگی و وحدت همه قدرت‌های سیاسی میانه‌رو مخالف حضور ایران در یمن اولین شرط رسیدن به توافق سیاسی است. «قرارداد ریاض»، به همراه پیوست امنیتی و نظامی آن، را می‌توان مکمل و اجرا نمود. این اسناد رکن اصلی رسیدن به صلح، امنیت و ثبات هستند.

حمایت منطقوی و بین‌المللی از دولت یمن در رویارویی با مشکلات اقتصادی و تقویت همکاری‌های سیاسی، اقتصادی و بشری باعث می‌شود که این دولت از توانایی ایجاد یمن میانه‌رو و برخوردار از ارزش‌ها و اصول بشری مشترک با دیگر کشورهای دنیا، مستفید شود. ما اهمیت مساعی مستمر کشورهای منطقه و دنیا برای تحمیل فشار به ایران، با هدف جلوگیری از فعالیت‌های مخرب ایران در یمن، و رساندن شرق میانه به امنیت، صلح و ثبات پایدار را درک می‌کنیم.

رسیدن به صلح در کشور ما برای سرکوب شبه‌نظامیان و رفع مشکلات و مسائلی که در جامعه یمن ایجاد کرده‌اند، کافی است. به همین دلیل، ما باید در اقدامات مربوط به ایجاد صلح مبتنی بر اصول ملی، ابتکار شورای همکاری خلیج‌فارس و میکانیزم اجرایی آن، نتایج «جلسه مذاکرات جامع ملی» و قطعنامه 2216 شورای امنیت سازمان ملل، برای رسیدن به صلح جامع، واقعی و پایدار و بازگرداندن امنیت و ثبات به یمن، منعطف باشیم.

در خاتمه، به خطر زیست‌محیطی فاجعه‌باری که همه از آن مطلع هستند ولی عملاً سعی موثری برای جلوگیری از وقوع آن انجام نمی‌دهند، اشاره می‌کنم: نشت بیش از 1 ملیون بیلر نفتی که هفت سال درنفتکش Safer نگهداری می‌شد، فاجعه‌ای واقعی است که ماحول زیست دریایی یمن و منطقه، بخصوص دریای سرخ و مناطق اطراف، را نابود خواهد ساخت. این نفتکش همچنان گروگان حوثی‌هاست. آنها به گروپ سازمان ملل اجازه نمی‌دهند که برای بازرسی از نفتکش وارد عمل شود. ✦

این نسخه نسبتاً مختصری از سخنرانی صورت‌گرفته در هفدهمین جلسه امنیت منطقوی در بحرین است که در چوکات مذاکرات منامه در نومبر 2021 برگزار شد.

محافظت
از اموال دیجیتل
پاکستان

تصاویر یونسپاث

این کشور اولین پالیسی ملی امنیت سایبری را برای تقویت شبکه‌ها در مقابل حملات سایبری انکشاف داد

کارکنان یونیپاث

کابینه

فدرال پاکستان، با هدف محافظت از شبکه‌های کمپیوتری در مقابل حملات سایبری، نخستین «پالیسی ملی امنیت سایبری» این کشور را در جولای 2021 تصویب کرد. وزارت تکنالوژی معلومات و ارتباطات پاکستان این پالیسی را با هدف محافظت از اموال دیجیتل کشور در مقابل مجرمین سایبری و رقبای جیوپلتیک احتمالی انکشاف کرده است.

پاکستان این پالیسی را به چندین کتگوری همپوشان -حقوقی، تخنیکی و سازمانی- تقسیم کرده است تا آنچه را که وزیر معلومات کشور نقص در محافظت از دستگاه‌های متصل به انترنت قلمداد می‌کند، پوشش دهد. بیش از 65 ملیون تن از مردم پاکستان از سرویس انترنت مستفید هستند و این کشور، مانند بسیاری از کشورها، خدمات تجاری و دولتی خود را در بستر انترنت عرضه می‌کند.

پاکستان این پالیسی را در چوکات گروپ‌های عکس‌العمل عاجلی کمپیوتری دولتی تطبیق می‌کند.

سید امین‌الحق، وزیر تکنالوژی معلوماتی و ارتباطات پاکستان، اظهار کرد: «وزارت معلومات و همه موسسات مرتبط دولتی و خصوصی از حمایت و رهنمایی لازم برای تضمین مراعات الزامات امنیت سایبری در بخش دیتا، خدمات، محصولات و سیستمی ICT [تکنالوژی معلوماتی و ارتباطات] مستفید خواهند شد.»

از رهنمودهای مهم پالیسی جدید امنیت سایبری پاکستان می‌توان به این موارد اشاره نمود:

- ایجاد کمیته پالیسی حکمرانی سایبری برای نظارت بالای استراتیژی امنیت سایبری کشور.
- اجرای پروگرام «دفاع فعال» برای جلوگیری از فیشینگ ایمیلی، نفوذ به شبکه‌های دولتی و نشر نرم‌افزار مخرب.
- محافظت و ارتقای سطح انعطاف ساختار ملی معلومات حیاتی و سیستم‌های معلومات‌رسانی دولتی.
- ترویج مشارکت‌های عمومی-دولتی برای مستفید شدن از مزیت نوآوری‌های کارآفرینانه به نفع مردم پاکستان.
- هدایت و تمویل پروگرام‌های تحقیق و انکشاف در بخش امنیت سایبری، مانند بهبود کیفیت تعلیم پرسونل.
- ترویج فرهنگ ملی امنیت سایبری با هدف تشویق کاربران کمپیوترها و تلیفون‌های هوشمند به یادگیری اصول محافظت از معلومات مهم.
- زمینه‌سازی برای همکاری بین‌المللی و هماهنگی در راستای ارتقای رتبه پاکستان در قسمت شاخص‌های بین‌المللی امنیت سایبری.
- ایجاد میکانیزم مقابله با جرایم سایبری با بهبود قوانین و مقررات.
- اعتمادسازی در حوزه تعاملات دیجیتل با بهبود میکانیزم‌های صدور سرتفکیت و راستی‌آزمایی.
- جهانگیر مدثر، خبرنگار حوزه تکنالوژی پاکستان، که با مجله نظامی «هلال» پاکستان همکاری می‌کند، تاکید کرد که محافظت از کمپیوترها و تلیفون‌های همراه در مقابل حملات سایبری مستلزم ارتقای سطح آگاهی عموم مردم است.

مدثر نوشت: «امنیت سایبری موضوعی در حد فشار دادن یک دکمه برای فعال‌سازی پروتوکل‌های خاص نیست. امنیت سایبری یک موضوع فرهنگی است که باید به بخشی از سبک زندگی ما، اعم از شهروندان، کارمندان دولت و قوای امنیتی، تبدیل شود.

«برای ارتقای سطح فعلی و آینده امنیت سایبری، پالیسی جامع امنیت سایبری باید وارد کتاب قانون ما شود و مورد پذیرش همه ذینفعان قرار بگیرد.» ✦

منابع: وزارت تکنالوژی معلوماتی و ارتباطات پاکستان، هلال، فجر، نقد اوراسیا

فروشندگان پاکستانی در حال دانلود کردن فایل از کمپیوتر برای نصب در تلیفون‌های همراه در فیصل‌آباد. استفاده روزافزون مردم این کشور از تکنالوژی معلوماتی ضرورت اقدام دولت برای تقویت پالیسی‌های سایبری را آشکار ساخته است. آژانس خبری فرانسه/تصاویر گتی

تصاویر یونیپاث

ضرورت تقویت اقدامات معلوماتی

عصام عباس امین، اداره استخبارات و امنیت، وزارت دفاع عراق

جامعه استخبارات تحت فشار انتظارات غیرواقع‌بینانه درباره وقایع از وقایع غیرمنتظره، بخصوص تهدیدات مربوط به استقلال یا امنیت داخلی، قرار گرفته است. از عوامل پدیدآورنده این انتظارات می‌توان به حمله دو فروند طیاره بی‌سرنشین به خانه صدراعظم عراق در 7 نومبر 2021 اشاره نمود.

شکست استخبارات اساساً باعث ایجاد ابهام در شایستگی سرویس‌های معلوماتی و شیوه‌های فعالیت آنها در مقابله با تهدیدات امنیتی می‌شود.

موضوع رویکردهای استخباراتی پیوسته در معرض نقد بوده است. شکست‌های ستراتیژیک حتی در سابقه سرویس‌های استخباراتی معروف، مانند ایالات متحده، دیده می‌شود. از نمونه‌های بارز می‌توان به حمله پرل هاربر در 1941، تهاجم کوریای شمالی به خاک کوریای جنوبی در 1950، دخالت شوروی در امور داخلی چکسلواکی در 1968 و حملات 11 سپتمبر 2001 اشاره کرد. گاهی نهادها در ارائه هشدارهای بهنگام ناکام می‌مانند که حادثه 11 سپتمبر مثال آشکاری در این راستا است. همچنان، صدور هشدارهای فراوان ولی غلط از طرف نهادهای امنیتی عواقب ناگواری ایجاد می‌کند که ادعای رسیدن عراق به سلاح‌های کشتار جمعی نمونه بارز آن است.

در هر دو مورد، شکست، آشکار و انتقادها کوبنده بود. باور شایع این است که معلومات‌رسانی در هر نوبت باید به‌درستی صورت بگیرد. رسیدن همیشگی به این هدف در دنیای واقعی قابل ممکن نیست و رویدادهای غیرمنتظره زمینه‌ساز شکست‌های گسترده می‌شود.

اگر موضوع به نگرش کشورهای همسایه، مانند ایران، یا تخمین خسارت عراق بر اثر حمله احتمالی به مکان‌های خاص مطرح باشد، سرویس‌های استخباراتی می‌توانند نقش خود را به شکل نسبتاً مناسبی ایفا کنند. این نوع معلومات‌رسانی به سوالات باز جواب می‌دهد و توانایی درک این موضوع بیشتر به فرضیات صحیح و کمتر به معلومات معتبر بستگی دارد.

ولی اگر سوال این باشد که داعش چی وقت و کدام نقطه را هدف قرار خواهد داد، چی باید کرد؟ در این مورد مساله متفاوت است چون ارائه جواب صحیح به نفوذ داخل حلقه داخلی این سازمان ضرورت دارد که موضوع توانایی ما در قسمت پیشرفت در روش‌های کسب معلومات را مطرح می‌کند.

ضمناً، بهبود کار استخباراتی، بخصوص در حوزه روش‌های تحلیلی و وقایع از وقایع غیرمنتظره، سخت است. با وجود پیشرفت در عرصه روش‌ها و ابزارهای کسب معلومات، تحول چندانی در میزان اعتبار تحلیل و ارزیابی معلومات صورت نگرفته است. حتی دسترسی به معلومات بسیار معتبر و قابل اعتماد، مشکل عدم‌قطعیت و تردید را برطرف نمی‌سازد.

موضوع مهم این است که معلومات نمی‌تواند همواره عنصر غافلگیری را از بین ببرد. اقدامات استخباراتی باعث می‌شود که تصمیم‌سازان از واقعیات باخبر شوند و تصمیمات خود را با اطمینان معقول بگیرند. این دستاورد کمی نیست و چنین نیست که همواره واقع شود.

در سطح استراتیژیک، سرویس‌های استخباراتی مسئول ارزیابی‌های معلوماتی ملی هستند. نتایج این ارزیابی‌ها پالیسی‌ها و استراتیژی‌های امنیت ملی، روش‌های مدیریت ریسک امنیتی، بودیجه‌های امنیتی و ترکیب قوای مسلح را شکل می‌دهد. قومندانان درستیزوال عراق برای پلان‌گذاری‌های خود به این ارزیابی‌ها متکی هستند.


우리민족
조선인민군

ارزیابی‌های استخباراتی در سطح محلی برای هدایت اقدامات رهبران سیاسی ضروری است.

ما باید بالای تفاوت بین ارزیابی‌های استخباراتی در سطح ملی، در ارتباط با تهدیدات خارجی، و ارزیابی‌های مربوط به ماحول داخلی تاکید کنیم. تاکید بیش از حد عراق بر ارزیابی‌های داخلی، در مقایسه با اقدامات خارجی، نقطه‌ضعفی است که باید برطرف شود.

مشکل دیگر این است که تحلیل‌گران استخباراتی فعلی به زنجیره فرمان، دقیقاً در بالای هرم، وابسته هستند. به این‌ترتیب، اصل عینیت و بی‌طرفی دچار خدشه حتمی می‌شود. ادارات استخباراتی بهتر است در پروسه ارزیابی استخبارات در حوزه‌های تصمیم‌سازی راهبردی مستقل عمل کنند.

ارزیابی‌های استخباراتی در سطح محلی برای هدایت اقدامات رهبران سیاسی ضروری است. این ارزیابی‌ها باید حرفوی، کاربردی و عملی باشد. طرز مثال، کار ارزیابی هشدار استراتیژیک جنگ، که یک موضوع سیاسی-نظامی است، باید مشترکاً به اداره کل استخبارات و امنیت و وزارت خارجه سپرده شود و در هر بخش بربنیاد وظایف مرتبط مدیریت شود.

البته، این دو نهاد دولتی از هماهنگی کافی برای تهیه مشترک مسوده هشدار برخوردار نیستند. چنین اقداماتی مستلزم هماهنگی و همکاری گسترده و استفاده از لسان اداری مشترک است.

با ظهور نهادهای جدید، گوناگونی ساحات و عوامل دینامیک و تقریباً غیرقابل‌پیش‌بینی، ارزیابی استخباراتی را به کار پیچیده و سختی مبدل ساخته است. ضمناً، پروسه های مستمر اجتماعی و فرهنگی -بشمول ورود تکنالوژی‌های جدید مانند شبکه‌های اجتماعی- که جامعه معلوماتی تا فعلاً با آنها عادت نکرده است، این پیچیدگی را افزایش داده است. نهادهای استخباراتی اغلب دانش مسلکی لازم برای رسیدگی به این پدیده‌ها که گاهی عوامل اصلی مشکلات، چالش‌ها و مخاطرات متعدد هستند، را ندارند.

در شرایط جاری، به دلیل سرعت بالای تحولات، جامعه استخباراتی قادر به پیش‌بینی دقیق رویدادهای آینده نیست. دشمن می‌تواند در فضای سایبری به‌سرعت وارد عمل شود. زمان مورد ضرورت پرتاب طیاره‌های بی‌سرنشین و موشک‌ها بسیار کاهش یافته است. به این‌ترتیب، فاصله زمانی بین مفکوره تا اجرا برای دشمن کاهش یافته است. برای اثبات این ادعا می‌توان به حمله 7 نومبر 2021 اشاره نمود. این حمله هم شخص صدراعظم و هم سرویس‌های استخباراتی را غافلگیر ساخت. ✦

با تاسف باید درگذشت نویسنده عصام عباس امین را به اطلاع تان برسانیم. درگذشت او ضایعه‌ای بزرگی برای خوانندگان یونیپاث و اداره امنیت و استخبارات وزارت دفاع عراق است.

ارزیابی معلوماتی بشمول عناصر ذیل است:

1. **تهدیدات.** امکانات و اهداف بازیگران مختلف را توصیف می‌کند و بین آنها ارتباط برقرار می‌کند، پروسه‌ها و روندهای سطح سازمانی و پالیسی‌های منطقوی و جهانی را تحلیل می‌کند.
2. **پروسه‌ها.** احتمال وقوع پروسه‌ها و روندهای مستمر را توصیف می‌کند، سناریوها را ارائه می‌کند و عکس‌العمل‌های احتمالی بازیگران به رویدادهای خاص را تحلیل می‌کند. طرز مثال، اگر قوای ما اقدام مشخصی انجام دهند، عکس‌العمل بازیگران (داخلی و خارجی) چه خواهد بود؟
3. **توصیه‌ها.** توصیه‌ها درباره مخاطرات و فرصت‌ها ارائه می‌کند.

چهار نمونه از شکست‌های معلوماتی که منشاء تحولات جهانی شد: (صفحه روبرو) حمله کوریای شمالی به خاک کوریای جنوبی در 1950، (بالا، راست به چپ) حمله به پرل هاربر در 1941، تهاجم شوروی به چکسلواکیا در 1968 و حمله 11 سپتمبر به ایالات متحده.

آژانس خبری فرانسه/تصاویر گتی

آماده‌باش

قوای بحری

قوای مسلح اردن

مصاحبه با دگَروال هشام خلیل الجراح، قومندان قوای بحری سلطنتی اردن

کارکنان یونیپاث

یونیپاث: وظایف قوای بحری سلطنتی اردن را تشریح کنید.

دگَروال الجراح: قوای بحری سلطنتی یکی از سه شاخه قوای مسلح اردن (زمینی، هوایی و بحری) و مکمل سیستم دفاع ملی محسوب می‌شود. این قوا در واقع نقشی دوگانه دارد: نقش نظامی قوای بحری و نقش سازمانی و امنیتی گارد ساحلی. این قوا را می‌توان قوای اصلی فعال در دریا و مسئول اصلی حفظ امنیت دریایی اردن توصیف نمود؛ ماموریتی که با وظایف متعددی همراه است. گزمه برای محافظت و دفاع از سرحدات دریایی اردن و جلوگیری از نفوذ و قاچاق، تفتیش‌های دریایی به کمک گروپ‌های تفتیش ورزیده و ماهر با تجهیزات پیشرفته، شناسایی و دفع فعالیت‌های مجرمانه در آبراه‌های منطقه، تطبیق قوانین مصوب و تفتیش تاسیسات نظامی و ملکی و اهداف مهم در عقبه از طریق «مرکز عملیات دریایی»، و اجرای عملیات جستجو و نجات در آبهای منطقوی و جلوگیری از ایجاد آلودگی دریایی از وظایف این قوا به شمار می‌رود.

یونیپاث: چالش‌های امنیتی پیش روی قوای بحری اردن در دریای سرخ چیست؟

دگَروال الجراح: چالش‌های امنیتی پیش روی قوای بحری اردن در دریای سرخ در چوکات حفظ امنیت دریایی اردن شکلهای مختلفی دارد. از این چالش‌ها می‌توان به عوامل دارای ماهیت غیرسنتی، مانند تروریزم، که شکلهای مختلفی مانند حمله به کشتی‌ها و بنادر و دزدی دریایی دارد و امنیت خطوط کشتی‌رانی را تهدید می‌کند اشاره نمود. اخیراً نیز بحران ویروس کرونا بالای فعالیت‌های ترانسپورت دریایی سایه انداخته است. بعضی از این چالش‌ها، مانند نفوذ و عبور از سرحدات دریایی و انواع قاچاق، جنبه امنیتی سنتی دارند، ولی بعضی دیگر، مانند حوادث و حوادث دریایی، آتش‌سوزی کشتی و بندر، آلودگی دریایی و اعتصاب موارد خاص محسوب می‌شوند. با وجود این چالش‌ها، همه نهادهای مرتبط با امنیت دریایی باید سطح هماهنگی، کارآیی و آمادگی خود را ارتقا دهند.

یونیپاث: کشورهای همکار چی‌قسم می‌توانند به انکشاف قوای بحری اردن کمک کنند؟ به کدام نوع کشتی‌ها و تجهیزاتی ضرورت دارید؟

دگَروال الجراح: بدون شک، همکاری بین‌المللی و منطقوی نقش مهمی در تقویت توانایی‌های دریایی اردن در حوزه تعلیم و در رسیدن به دانش تخصصی از طریق برگزاری دوره‌ها و مانورهای مختلف داشته است. این اقدامات همچنان ضروریات قوای بحری اردن از نظر بهره‌برداری از کشتی‌های دارای توانایی حرکت خارج از آبهای منطقوی و برخوردار از تجهیزات تخصصی سطح بالا را که می‌تواند به ایجاد توانایی واکنش سریع و کاهش زمان عکس‌العمل عاجل منجر شود، برآورده ساخته است. قابل یادآوری است که انکشاف قابلیت‌های کَندَک دریایی 77 باعث تقویت توانایی‌های این کَندَک در اجرای وظایف مرتبط شده است. همچنان، همکاری بسیار نزدیک بین قوای بحری اردن، قوای بحری ایالات متحده و تفنگداران دریایی ایالات متحده در این حوزه اهمیت بسزایی دارد.

یونیپاث: آیا بین کشورهای اطراف خلیج عقبه همکاری امنیتی وجود دارد؟

دگَروال الجراح: قطعاً اجرای وظیفه حفظ امنیت دریایی اردن مستلزم حفظ سطح بالای هماهنگی و همکاری با کشورهای اطراف خلیج عقبه است. این یگانه بندر دریایی اردن برای خطوط کشتی‌رانی بین‌المللی است و البته بین این کشورها همکاری امنیتی از طریق مامورین رابط و جلسات امنیتی دوره‌ای برقرار است. اجرای مانورهای دریایی با حضور این کشورها نمادی از این همکاری و هماهنگی است.

یونیپاث: اهمیت مانورهای دریایی مشترک منطقوی و بین‌المللی چیست؟

دگَروال الجراح: اجرای مانورهای دریایی دوجانبه یا چندجانبه نقش مهمی در رسیدن به سطح بالای هماهنگی و همکاری بین قوای بحری دارد. این مانورها تاثیر مثبتی بالای موثریت و توانایی قوای اشتراک‌کننده می‌گذارد. ضمناً، اشتراک در مانور باعث رسیدن همه طرف‌ها به دانش تخصصی و زمینه‌ساز تبادل مهارت و یکپارچه‌سازی عالی مفاهیم و پروسیجرهای مورداستفاده قوای بحری، در سطح منطقوی و جهانی، می‌شود.

یونیپاث: به‌عنوان بخشی از قوای بحری ترکیبی، اردن از تجربیات 34 کشور دیگر ائتلاف چه استفاده‌ای نموده است؟

دگَروال الجراح: از اوایل تاسیس «قوای بحری ترکیبی» در سال 2009، قوای بحری سلطنتی اردن یکی از اعضای فعال آن بوده است. این مشارکت بیانگر نقش فعال و تصویر بارز قوای بحری اردن بوده است، و بدون شک در انکشاف

جایگاه‌های دریایی اردن از طریق تبادل دانش تخصصی با کشورهای ائتلاف، شناسایی شیوه‌های فعالیت قوای بحری کشورهای دیگر و کسب معلومات درباره تجربیات کشورهای دیگر در حوزه مدیریت عملیات دریایی نقش داشته است. این مشارکت تاثیر مثبتی بالای استندردهای خدمت صاحب‌منصبان، خورد ضابطان و پرسونل مرتبط داشته است و قوای بحری اردن را از امکانات عالی تعلیم، دانش و مهارتهای عالیتر، و زمینه ایجاد روابط دوستانه و رسیدن به اهداف آگاهی اجتماعی و فرهنگی به کمک اشتراک‌کنندگان کشورهای دیگر مستفید ساخته است.

یونیپاث: قوای بحری سلطنتی اردن در کدام مانورها اشتراک نموده است و چرا این مشارکت برای شما مهم است؟

دگَروال الجراح: قوای بحری اردن در سه سطح در مانورهای مختلف اشتراک می‌کند: محلی و ملی، منطقوی و بین‌المللی. در سطح محلی، قوای بحری مانورهایی را با هدف تقویت یکپارچگی و همکاری بین جزوتام‌ها در محدوده قومندانی قوای بحری برگزار می‌کند. بعضی مانورها و سناریوهای متنوع در سطح ملی و با مشارکت سرویس‌های نظامی و امنیتی و بعضی نهادهای ملکی مرتبط با حوزه دریا اجرا می‌شود. هدف از اجرای این مانورها رسیدن به سطح مطلوب همکاری و هماهنگی بین این گروپ‌ها و تقویت امکانات مقابله با حوادث دریایی است. در سطح منطقوی، قوای بحری اردن مرتباً و همراه با کشورهای اطراف خلیج عقبه در مانورهای دریایی اشتراک می‌کند. مانورهایی مانند «شیر در کمین» و «مدافع عظیم» در پادشاهی اردن هاشمی، «ستاره درخشان» در مصر، و «موج سرخ» و «صخره امن» در عربستان سعودی برگزار شده است. در سطح بین‌المللی، قوای بحری اردن، به‌عنوان عضو فعال یا ناظر، حضور مستمری در مانورهای بین‌المللی دریایی متعددی داشته است. بدون شک، حضور دائمی و مستمر ازین قبیل باعث آشنایی پرسونل قوای بحری اردن با جدیدترین ترفندهای مدیریت عملیات دریایی و تبادل دانش تخصصی و کسب تجربه در کنار اشتراک‌کنندگان دیگر می‌شود.

یونیپاث: تفنگداران دریایی ایالات متحده چه نقشی در تقویت قوای شما داشته است؟

دگَروال الجراح: قوای بحری اردن، از طریق کَندَک دریایی 77، رابطه خاصی با تفنگداران دریایی ایالات متحده دارد. این رابطه در پروگرام هماهنگ مشترکی که در جریان سالها اجرا شده و در ارتقای سطح آمادگی و تعلیم کَندَک در حوزه عملیات آفندی و پدافندی، عملیات امنیت داخلی و تعلیم SWAT قوای بحری و گروپ‌های بازرسی کشتی نقش داشته است، نمایان شده است. باید اشاره کرد که کَندَک دریایی 77 از طریق این همکاری با تفنگداران دریایی ایالات متحده، از تجهیزات مختلف و دستگاه‌های پیچیده‌ای که در حوزه پیاده‌نظام (تفنگداران) دریایی کاربرد دارد، مستفید شده است. اهمیت این رابطه از طریق فعالیت‌های مستمر مشترک و هماهنگی چند-سطحی نیز آشکار شده است. ما، در قومندانی قوای بحری اردن، خواستار حفظ و تقویت این رابطه برای تامین منافع مشترک هر دو طرف هستیم.

یونیپاث: در قسمت حفظ امنیت آبهای سرزمینی اردن، قوای بحری اردن چه تعاملی با دیگر قوای مسلح و موسسات امنیتی دارد؟

دگَروال الجراح: حفظ امنیت دریایی اردن مسئولیت مشترک نهادهای نظامی و امنیتی مختلف و ادارات و موسسات دولتی مرتبط با فعالیت‌های دریایی است. بنابراین، قوای بحری اردن اهمیت همکاری و هماهنگی با نهادهای

تفنگداران دریایی اردن در خلیج عقبه به تعلیم و اجرای عملیات می‌پردازند. قوای مسلح اردن

قوای مسلح اردن

دگروال هشام خلیل الجراح، قومندان قوای بحری سلطنتی اردن، راست، و دریابان برد کوپر، قومندان قرارگاه مرکزی قوای بحری ایالات متحده، در حال امتحان عملکرد شناور سطحی اتومات Saildrone Explorer در بحرین، نومبر 2021

خورد ضابط بحری صنف دوم مارک توماس محمود/ قوای بحری ایالات متحده

دیگر در مسیر رسیدن به هدف مطلوب را که همان پاسبانی از آبهای سرزمینی اردن است، درک می‌کند. این هماهنگی و همکاری با تبادل معلومات با مرکز عملیات دریایی مجسم می‌شود. این مرکز به پیشرفته‌ترین سیستم‌های نظارتی و شبکه‌های ارتباطی پیچیده مجهز است و پروگرام‌های عکس‌العمل به حوادث دریایی و حفظ امنیت عقبه را پیوسته اپدیت می‌کند. ارتباط مستمری نیز با صاحب‌منصبان امنیتی و نهادهای تخصصی برقرار شده است و مانورهای دریایی مشترک در سطح محلی و ملی با انواع سناریوهای احتمالی با هدف تقویت یکپارچگی میان-نهادی برگزار می‌شود و در رسیدن به سطح عالی هماهنگی نقش دارد.

یونیپاث: درباره آماده‌سازی و تعلیم قوای بحری و پرسونل دریایی اردن توضیح بدهید.

دگَروال الجراح: اعضای قوای بحری اردن، بشمول صاحب‌منصبان، خوردضابطان و پرسونل، طبق الزامات اساسی نظامی عساکر، مشمول پروگرام فشرده تقویتی و تعلیم قرار می‌گیرند. این پروگرام شامل تعلیم مقدماتی، تعلیم سلاح، فیر، آب‌بازی و تعلیم امنیتی و اطلاع‌رسانی است. تعلیم تخصصی دریایی و تخنیکی و تعلیمات مخصوص تفنگداران، نظر به رسته‌های مختلف، نیز در دستور کار قرار دارد. ضمناً، این اعضا در کورس‌های تعلیمی که در موسسات دریایی و امنیتی اردن و موسسات ملکی فعال در حوزه علوم دریایی برگزار می‌شود، اشتراک می‌کنند.

یونیپاث: آیا دوره‌های تعلیمی صاحب‌منصبان و خوردضابطان خارج از خاک پادشاهی برگزار می‌شود؟

دگَروال الجراح: صاحب‌منصبان و خوردضابطان بحری اردن در تعدادی از کورس‌های خارجی که در موسسات تعلیم دریایی کشورهای هم‌پیمان و دوست برگزار می‌شود، اشتراک می‌کنند. از اینها می‌توان به کورس‌های اساسی و پیشرفته مخصوص رسته‌های دریایی (قوای بحری، انجینر دریایی، غواص، پیاده‌نظام دریایی) و نیز دوره‌های مختلف لسان و دوره‌های تعلیمی صاحب‌منصبان ستاد و مدیران ارشد با کاربرد تعلیمی مشخص، که برای تقویت کارآیی و توانایی این رده‌ها و مجهز ساختن آنها به مهارت‌ها و تخصص‌ها و تبادل تجربه با دیگران طراحی شده است، اشتراک می‌کنند.

یونیپاث: آیا ماموریت‌های محافظت از اکوسیستم دریایی برای قوای بحری اردن تعریف می‌شود؟

دگَروال الجراح: یکی از مهم‌ترین وظایف قوای بحری اردن محافظت از اکوسیستم دریایی است. اردن سازمانی تخصصی برای محافظت از ماحول زیست دریایی تشکیل داده است و هماهنگی و همکاری مستمری برای تضمین اجرای پیشنهادات مربوط به محافظت از اکوسیستم دریایی و نظارت بالای ماهیگیری در جریان است. باید متوجه بود که قوای بحری اردن بر صنعت ماهیگیری نظارت می‌کند و از اجرای شیوه‌های غلط ماهیگیری جلوگیری می‌کند. ✦

رویکرد لبنان به امنیت سایبری

اداره امنیت سایبری قوای مسلح لبنان خود را برای مقابله با تهدیدات آماده می‌سازد

یونیپاث با برید جنرال علی قنسو، سخنگوی ارشد قوای مسلح لبنان مصاحبه کرده است. او توضیح داد که چی‌قسم اردوی لبنان با مخاطرات تهدیدکننده شبکه‌های کمپیوتری که ممکن است بالای امنیت ملی تاثیر بگذارد، مقابله می‌کند.

یونیپاث: امنیت سایبری به بخش جدایی‌ناپذیر امنیت ملی کشورها تبدیل شده است. تهدیدات سایبری پیش روی لبنان کدام است؟

برید جنرال قنسو: لبنان از طرف بازیگران متعدد آماج تهدیدات سایبری قرار گرفته است. اینها در پی نفوذ به سیستم‌های آنلاین، جاسوسی از ارتباطات و دزدی معلومات هستند. بعضی سازمان‌های تروریستی برای ترویج ایدئولوژی افراطی بین جوانان و جذب قوای جوان اقدام به هک کردن حساب‌های دیگران می‌کنند. بعضی اشخاص و گروپ‌های فعال در لبنان و دیگر نقاط دنیا در پی حمله الکترونیکی به دولت‌ها و موسسات دولتی هستند.

در این عرصه، لبنان 24 ساعته در معرض حملات سایبری، بشمول محروم‌سازی از سرویس توزیع‌شده و حمله به بخش بانکی (با نرم‌افزارهای مخرب مانند Gauss و Flame)، بخش مخابراتی و کمپنی‌های ملکی قرار دارد.

فقدان سیستم‌های محافظت سایبری و منابع بشری ورزیده و برخوردار از توانایی مقابله با این حملات، ظرفیت لبنان برای مقابله با این حملات را کاهش داده است. بر این اساس، عملیات و عکس‌العمل‌های امنیت سایبری به اقدامات کنشگرا و تضمین مقابله هرچه بیشتر با این حملات محدود شده است.

یونیپاث: نقش اداره امنیت سایبری قوای مسلح لبنان چیست؟

برید جنرال قنسو: بیشتر بخشهای قوای مسلح پیگیر تاسیس ادارات امنیت سایبری برای محافظت از منابع سیستم‌ها و شبکه‌های مختلف خود هستند. از این منابع می‌توان به معلومات حساس امنیتی و نظامی مرتبط با تسلیحات، تجهیزات، اجرای ماموریت، استقرار جزوتام‌ها و مشخصات شخصی و حرفوی مرتبط با پرسونل نظامی و ملکی اشاره نمود. اینترانت، انترنت و ارتباطات بی‌سیم نیز جزو این منابع هستند.

در مورد قوای مسلح لبنان، اداره امنیت سایبری نقش بسیار مهمی در قسمت مقابله با اقدامات مختل‌کننده یا پروسه‌های نفوذ به سیستم‌های استخباراتی نظامی و امنیتی دارد. این تهدید امنیتی جدی محسوب می‌شود که فعالیت‌های اردوی لبنان، جزوتام‌ها آن و جان کارمندان آن را در معرض خطر قرار می‌دهد.

یونیپاث: این نوع حملات چه تاثیری بالای اردوی لبنان می‌گذارد؟

برید جنرال قنسو: قوای مسلح لبنان از سیستم‌های مختلف شبکه سایبری، بشمول صفحه‌های انترنتی رسمی دولتی، سرویس‌های ایمیل و پروگرام‌های تلیفون هوشمند، استفاده می‌کنند. این قوا امکان دسترسی به انترنت را برای عساکر و جزوتام‌ها خود فراهم می‌کنند.

در همه این سیستم‌ها حوزه‌هایی وجود دارد که ممکن است مورد استفاده دشمنان ملت یا دیگر بازیگرانی که در پی صدمه رسانیدن به اردو هستند، قرار بگیرد. طرز مثال، حمله موفقیت‌آمیز ممکن است زمینه‌ساز ایجاد اختلال در شبکه ارتباطات داخلی مرتبط کننده جزوتام‌ها با قومندانی شود. ویب‌سایت‌های اردو یا هریک از حساب‌های رسمی در شبکه‌های اجتماعی ممکن است هک شود. این امکان وجود دارد که معلومات حساس از شبکه داخلی که محیط تبادل فایل است، دزدیده شود.

این مسائل ممکن است عواقب ناگواری برای اردو، جزوتام‌ها و کارمندان آن داشته باشد، بخصوص اگر گروپ‌های تروریستی که پرسونل و مراکز نظامی را پیوسته آماج حمله قرار می‌دهند، بتوانند از این امکانات استفاده کنند.

یونیپاث: همکاری بین‌المللی در محافظت از شبکه‌های کمپیوتری لبنان چه اهمیتی دارد؟

برید جنرال قنسو: همکاری بین‌المللی برای محافظت از شبکه‌های معلومات لبنان حیاتی است. این همکاری در دو سطح صورت می‌گیرد: نخست، ارائه نرم‌افزار پیشرفته لازم برای تقویت شبکه‌ها در مقابل حملات سایبری است و دوم، تعلیم دادن نیروی بشری برای مقابله با این حملات و ارائه عکس‌العمل سریع و مناسب برای جلوگیری از حمله یا محدود ساختن میزان خسارات آن است.

یونیپاث: کارمندان شما چی‌قسم مهارت‌های خود را متناسب با پیشرفت حوزه‌های امنیت سایبری تقویت می‌کنند؟

برید جنرال قنسو: پرسونل ما در کورس‌های تعلیمی مختلف، جلسات سخنرانی و جلسات مختلف در لبنان و خارج از آن اشتراک می‌کنند. دنیای سایبری با سرعت بالا در حال پیشرفت است و روزانه هزاران نرم‌افزار مخرب امنیت سایبری تولید می‌شود. ضمناً، هزاران گروپ و شخص مجری حملات سایبری در سراسر دنیا پیوسته در حال ابداع روش‌های جدید هستند. دشمنان ما نیز در پی تقویت امکانات آنلاین با هدف نفوذ به سیستم‌های معلومات ما هستند.

بنا به این دلایل، پرسونل ما باید با آخرین تحولات عرصه امنیت سایبری همگام شوند تا بتوانند برای مقابله با چالش‌های جدید آماده شوند. از طرف دیگر، مکمل کردن اقدامات دفاع سایبری به تجهیزات و نرم‌افزارهای پیچیده‌ای ضرورت دارد که ما قصد داریم در کنار دولت‌ها و بازیگران دوست از آنها استفاده کنیم. ✦

نقش
مرکز امنیت دریایی عمان

از چپ، برید جنرال علی بن سیف المقبلی، مدیر کل گارد ساحلی پولیس سلطنتی عمان؛ عبدالمنیر، معاون امیرالبحر قوای بحری پاکستان، قومندان وقت کارگروپ مشترک 151؛ و کاشف فرحان، ناخدای وابسته دفاعی پاکستان از دفتر گارد ساحلی پولیس سلطنتی عمان در مسقط بازدید کردند.

معاون امیرالبحر عبدالمنیر، چپ و برید جنرال عبدالمقبل، در حال تبادل هدیه

مرکز امنیت دریایی، متشکل از اردوی عمان، نهادهای امنیتی و ملکی، وظیفه حفظ امنیت و ثبات آبهای سرزمینی را به عهده دارد.

این مرکز، واقع در گارنیزون المرتفع، مسئولیت دریافت راپور از این نهادها و هماهنگی با نهادهای مرتبط را به عهده دارد. سیستم‌ها و تجهیزات تخصصی آن شبانه‌روزی برای دفاع از آبهای عمان به کار گرفته می‌شود.

بخشی از وظایف این مرکز به شرح ذیل است:

1. یکپارچه‌سازی اقدامات نهادهای امنیتی دریایی.
2. تامین امکانات و وسایل لازم در حوزه تجهیزات، دستگاه‌ها، طیاره شناسایی، کشتی و قایق.
3. تدوین پروسیجرها و پروگرام‌های لازم برای مقابله با فعالیت‌های غیرقانونی و جرایم سازمان‌یافته در بنادر، تاسیسات و نواحی ساحلی.
4. تقویت پروسیجرها و اقدامات برای محافظت از ذخایر ماهی، منابع طبیعی و حیات آبی.
5. مقابله با حوادث زیست‌محیطی و انسانی با امکانات و اموال در اختیار سلطان‌نشین.
6. اشتراک در روند پلان‌گذاری مدیریت بحران و حوادث طبیعی و آماده‌سازی سناریوهای ریسک دریایی.
7. تعلیم شهروندان، ساکنان و دریانوردان در قسمت اهمیت امنیت و همکاری برای محافظت از ذخایر دریایی طبیعی سلطان‌نشین.
8. رهگیری و تفتیش تحرکات کشتی‌ها در/اطراف آبهای سرزمینی عمان.
9. تقویت همکاری با ملت‌های هم‌پیمان و دوست و با سازمان‌های منطقوی و بین‌المللی فعال در حوزه امنیت دریایی.

این مرکز مسئول تفتیش موارد نقض قانون در محدوده آبهای عمان است. بشمول ذیل:

1. دزدی دریایی
2. مهاجرت یا نفوذ غیرقانونی
3. ماهیگیری غیرقانونی و صید بیش‌ازحد
4. آلودگی دریایی
5. انسداد مسیرهای کشتی‌رانی بین‌المللی
6. تروریزم دریایی
7. دستکاری و/یا خرابکاری در تاسیسات نفتی دریایی
8. جرایم سازمان‌یافته، تجارت غیرقانونی و قاچاق ✦

معاون امیرالبحر عبدالمنیر، وسط، و همکارانش از مرکز امنیت دریایی عمان بازدید می‌کنند.

مدیریت چابک

دگر جنرال قیس خلف رحیمه با تهدیدات سنتی و مدرن

کارکنان یونیپاث | عکس از وزارت دفاع عراق

ظاهر و خصوصیات متمایز او بیانگر ریشه‌های سومری اوست. او با مهربانی، تواضع و ادب، کلمات را برای ارتباط با مهمان به‌دقت انتخاب می‌کند و روحیه مهمان‌نوازی جنوبی را به نمایش می‌گذارد. تواضع و ادب او مانع کسب تجربه در قسمت علوم نظامی نشده است. حضور در جنگ های مختلف، منحیث عسکر، او را به جایگاه فداکاری سرسختانه و ایمان به پیروزی رسانده است.

او دگر جنرال قیس خلف رحیمه، معین رئیس ارکان قوای مسلح عراق، و قومندان قوماندانی عملیاتهای مشترک عراق است. این نام و سابقه معانی بسیاری برای رهبران سیاسی و امنیتی دارد. او با مسلکی‌گرایی و درستکاری وظیفهٔ سخت دفاع از کشور را به‌خوبی انجام داده است.

او متولد 1962 در میسان است و از همان دوران طفولیت شیوه معاشرت با اشخاص فرهیخته را آموخته است. او در 1984 از کالج نظامی اول فارغ‌التحصیل شد و بعد از جنگ اول خلیج فارس موفق به کسب سند ماستری شد. همچنان بعد از آزادسازی موصل سند دوکتورا گرفت و تحصیلات خود را با تجربیات جنگی مکمل کرد.

جنرال می‌گوید: «وقتی در 1984 وارد کالج نظامی شدم، جنگ ایران و عراق به نقطه اوج رسیده بود. آن کالج نیز جبهه جنگی بود که محصلین را از دانش تخصصی استادان مستفید می ساخت. این استادان از خط مقدم بازگشته بودند و تجربیات و درسهای جنگ را با محصلین در میان می‌گذاشتند. ما از قومندانان میدانی که وظیفه تدریس را به عهده داشتند، درسهای بسیاری آموختیم. بعد از فارغ‌التحصیل شدن، از چنان تجربه میدانی و علمی مستفید شده بودیم که گویی واقعاً در جنگ اشتراک نموده بودیم.»

با وجود فعالیت در بخشهای عملیاتی، دگر جنرال قیس مطالعات ستراتژیک خود را ادامه داد و در سال 2010 وارد کالج ملی دفاعی شد.

«از این که از طرف وزارت دفاع برای ادامه تحصیل [ستراتیژی امنیت ملی] و کسب سند ماستری انتخاب شده بودم، خوشحال بودم. این رشته منحصربه‌فرد بود و استادان آن در قسمت علوم سیاسی و نظامی تخصص داشتند. این تجربه برای من بی‌نظیر بود چون قبلاً در میدان تل‌عفر تجربه کسب کرده بودم و می‌توانستم

پروگرام‌های موجود برای بازگرداندن امنیت به آن شهر را در کنار پروگرام‌های درسی تحلیل کنم. این شرایط باعث شد که انگیزه ادامه تحصیل در مقطع دوکتورا با گرایش «جنگهای نوین و تحول در مفاهیم قدرت» در سال 2019 در من ایجاد شود. با وجود تشویشهای مربوط به فعالیت منحیث قومندان عملیات میان-فرات، مشکلات امنیتی کشور و ایجاد وقفه چندباره در روند تهیه مونوگراف، اراده من برای سپری نمودن این مقطع سست نشد. این نکته مهم بود که تخصص من با همه چالش‌های پیش روی عراق، بخصوص نسل پنجم و ششم جنگ، مرتبط بود.»

دگر جنرال قیس در مرحله جنگ سنتی متوقف نشد. او با یادگیری علوم نظامی معاصر ذریعه تحقیقات ستراتیژیک، شناخت اهمیت جنگ سایبری و آشنایی با مخاطرات گروپ‌های تروریستی و افراط‌گرا در کانال‌های مجازی، وارد مسیر جدیدی شد.

جنرال اظهار کرد: «بعد از پیدایش فاجعه داعش و تسلط این گروپ بر بخش وسیعی از مناطق عراق، جنگ روانی با شایعه‌پراکنی در شبکه‌های مجازی با هدف تضعیف هرچه بیشتر وضعیت امنیتی آغاز شد.

در آن زمان، پاسخ‌های نهادهای رسانه‌ای رسمی و غیررسمی دولت مطابق چالش‌ها نبود. گروپ‌های تروریستی به اجرای عملیات‌های گسترده و مبتنی بر وحشت‌آفرینی در قلب مردم از طریق سر بریدن، انفجار دادن بازارها، اسیر کردن زنان و انتشار این تصاویر در شبکه‌های اجتماعی برای پیام‌رسانی به دیگران، می‌پرداختند.»

«هدف آنها تضعیف روحیه مخالفین و وادار ساختن شهروندان و قوای امنیتی به مصالحه و تسلیم بود. ما شروع به تخریب شبکه‌های سایبری آنها که از بیرون از عراق و مناطق تحت تصرف آنها کنترول می‌شد، کردیم.»

جنرال و همکارانش همراه با قوای ائتلاف بین‌المللی اقدام به شناسایی و تخریب شبکه‌های جنگ سایبری داعش کردند. گروپ‌های جنگ الکترونیک عراق نیز با گروپ‌های ائتلاف برای شناسایی اشخاصی که با نوشتن توییت و وبلاگ از داعش حمایت می‌کردند، همکاری کردند و این حساب‌ها را مسدود نمودند.

جنرال اظهار کرد: «بعداً بر مساله جلب اعتماد قوا و تقویت روحیه متمرکز شدیم و موفق به بازیابی آمادگی روانی-نظامی

تانک M1A1 فرقهٔ 9 زرهی در بیرون از موصل موضع دفاعی گرفته است. 2017

پرسونل جزوتام‌ها شدیم. بعداً، قهرمانان ما به مقاومت در میدان جنگ پرداختند و حتی در جنگ های شدید هیچ‌گاه از حوزه وظایف خود خارج نشدند. برای آنها به‌تدریج آشکار شد که تصویری که داعش با تبلیغات آنلاین ایجاد نموده بود، دروغی بیش نبود. داعش تروریست‌ها را رزمندگانی فوق‌العاده که شکست دادن یا کشتن آنها با گلوله امکان‌پذیر نیست، معرفی کرده بود.»

او شکست داعش را نتیجه استفاده از کانال‌های شبکه‌های اجتماعی و قدرت جوانان می‌داند. آنها دروغ‌های داعش را افشا کردند و گسترش بی‌اعتمادی را برای داعش سخت کردند. به همین دلیل، اردوی الکترونیک و دستگاه رسانه‌ای داعش از فعالان مدنی، نهادهای معلوماتی و قوای ائتلاف شکست خورد. در واقع آنها مسیر شکست داعش را در میدان جنگ طی کردند.

دگر جنرال قیس با آگاهی از این که جنگ نسل چهار، پنج و شش به تکنالوژی‌های نوین متکی است، به اردوها توصیه می‌کند که با تحولات تکنالوژی همگام شوند تا بتوانند با تهدیدات جاری و آینده که معمولاً در کتگوری جنگ نامتقارن قرار می‌گیرد، مقابله کنند.

اردوها باید ابزارهای دفاع آنلاین را تقویت کنند و به ایجاد نهادهای معلوماتی سایبری بپردازند. این نهادها باید از قابلیت تفتیش فعالیت دشمن و مقابله با مخاطرات تهدیدکننده امنیت ملی و جلوگیری از حملات سایبری گروپ‌های خرابکار برخوردار باشند. به ادعای دگر جنرال، تکنالوژی مدرن، انترنت و طیاره بی‌سرنشین باعث پیچیده‌تر شدن نهادهای امنیتی شده است.

دگر جنرال قیس در مقطع زمانی 2004 الی 2008 قومندان لوای 10 منطقه تل‌عفر بود. القاعده با فعالیت در این منطقه باعث شده بود که عراق در مسیر خطرناکی قرار بگیرد. درگیری‌های فرقه‌ای و فعالیت گروپ‌های تروریستی در این شهرها رایج بود.

او می‌گوید: «به دلایل متعددی مجبور به اجرای ماموریت‌ها و وظایف پیچیده بودیم که مهم‌ترین آنها حضور قوای القاعده در شهر و مناطق اطراف بود. ترکیب جمعیتی شهر شامل فرقه‌ها و آیین‌های گوناگون بود. زمانی که من قومندانی لوای 10 را به عهده گرفتم، ترس و نومیدی

تانک M1A1 فرقهٔ 9 زرهی وارد میدان جنگ موصل می‌شود. 2017

همه جای عراق را فرا گرفته بود و ترس از مرگ ذهن همه را مصروف کرده بود. سرویس پولیس تا فعلاً شکل نگرفته بود و اردو وظیفه حفظ امنیت را به عهده داشت. رشته اعتماد مردم و قوای امنیتی گسسته شده بود و این ذهنیت وجود داشت که این قوا قادر به محافظت از شهر در مقابل تروریستان نیستند.»

با همکاری قوای ائتلاف، وضعیت به‌تدریج رو به ثبات نهاد. آنها بالای امنیت و استخبارات متمرکز شدند و برای ایجاد ثبات به شهر از منابع ملکی و ملی کمک گرفتند. آنها همچنان از ساکنان سنی تل‌عفر خواستند که به قوای اردو و پولیس ملحق شوند و این یکی از اهداف مهمی بود که ما تعقیب می‌کردیم. آنها برای کاهش فاصله بین جنبه‌های قومی و مذهبی نظام قضایی، اعتمادسازی، مقابله با فرقه‌گرایی و ایجاد ارتباط با مردم سعی کردند.»

در اوایل اکتوبر 2019، تظاهراتی در بغداد برای اعتراض به مشکلات اقتصادی و فساد دولتی برگزار شد. ایجاد خشونت از طرف گروپ‌های نافرمان باعث شد که این تظاهرات با خون‌ریزی همراه شود. این وضعیت عراق را در آستانه گرداب خطرناکی قرار داد. رهبران سیاسی و نظامی چاره‌ای جز برکناری مدیران امنیتی این مناطق نداشتند. آنها باید قومندانان برخوردار از صفات خویشتن‌داری، وطن‌دوستی و شجاعت را انتخاب می‌کردند. در این مقطع نام دگر جنرال قیس برای اعطای این مسئولیت سخت مطرح شد.

جنرال می‌گوید: «تلفات ملکی باعث ایجاد شکاف عمیق در رابطه بین مردم و قوای امنیتی شد و این تصویر امنیتی آشفته اوضاع را بدتر ساخت. کمبود قوای تخصصی که از دانش و تجهیزات لازم برای فعالیت در این سرویس برخوردار باشند، مشکل کلانی بود. البته، این وظایف و ماموریت‌های ویژه بیش از آن که به تجربه نظامی و هنر مدیریت هنرمند وابسته باشد، به درایت، وطن‌دوستی، خویشتن‌داری و دلسوزی ضرورت دارد. محافظت از جمعیت معترض و جلوگیری از اقدامات تحریک‌آمیز از طرف قوای امنیتی باعث جلب اعتماد مردم می‌شود.»

اقدام در چوکات اختیارات قانون اساسی و قوانین مقابله با شورش و مقابله با تظاهرکنندگان خشن که بدون مراعات الزامات قانونی تظاهرات مسالمت‌آمیز به تهداب‌ها و قوای امنیتی حمله می‌کردند، بسیار مهم بود.

جنرال عنوان کرد: «به محض پذیرش این مقام، اقدام به ایجاد جزوتام‌ها مسئولیت، تعریف حوزه وظایف تک‌تک صاحب‌منصبان، ایجاد موانع آشکار برای مراعات پیمان‌های بین‌المللی حقوق بشر، و جداسازی تظاهرکنندگان از قوای امنیتی کردم.

کمره‌هایی روی موانع و پوسته‌های امنیتی برای تفتیش موارد بی‌نظمی نصب شد. من با صدور دستورهای سختگیرانه از همه صاحب‌منصبان تعهد گرفتم که به هیچ عنوان به طرف تظاهرکنندگان فیر نکنند و استفاده از مرمی پلاستیکی و اسپری گاز اشک‌آور را نیز منع کردم.»

او هر روز با فعالان صلح‌طلب و تظاهرکنندگان ارتباط برقرار می‌کرد. شرایط به‌سرعت رو به بهبود نهاد.

جنرال می‌گوید: «ما احترام را به اردو و قوای امنیتی بازگرداندیم. هر چه باشد، آنها طرفدار مردم هستند و توان و اراده خود را از مردم می‌گیرند.»

راست: گروپی در مرکز رسانه وزارت دفاع عراق در حال تفتیش رسانه‌ای برای مقابله با تبلیغات تروریستی.

چپ: دگر جنرال قیس، قومندان وقت عملیات بغداد، در حال گفتگو با فعالان عراقی در میدان تحریر، 2019

اقدام لبنان در تقویت پروسه تفتیش الکترونیکی قاچاق

کارکنان یونیپاث

قوای مسلح لبنان (LAF) سیستم نظارت کشوری را برای پر نمودن شکاف‌های امنیتی در سرحد سوریه فعال ساخته اند.

مشکل قاچاق و نفوذ چنان شدت گرفته است که لبنان از 2009 تا فعلاً چهار غُند را در سرحدات شمالی و شرقی خود مستقر نموده است.

برای انسداد مسیرهای قاچاق، قوای مسلح لبنان شبکه‌ای از برجهای تفتیش الکترونیکی را به مرکز عملیات و معلومات مشترک در قومندانی اردوی لبنان متصل کرده است. این سیستم امکان تفتیش دائم روزانه و شبانه را فراهم می‌کند و به جزوتام‌ها سیار مسئول مقابله با تخلفات هشدارهای زودهنگام ارائه می‌کند. این ادعای جنرال جوزف حداد، رئیس کمیته مشترک حفظت از سرحدات لبنان، است.

مرحله دو این پروگرام که از نومبر 2021 آغازشد، بشمول ادغام رادارهای نظارت ساحلی در برجهای تفتیش داخلی است. حداد اظهار کرد که این سیستم یکپارچه «نقش مهمی در صدور هشدار زودهنگام در شرایط بحرانی دارد.»

غُند اول سرحدات زمینی قوای مسلح لبنان محدوده دریای مدیترانه الی شهر وادی‌خالد را در این منطقه پوشش می‌دهد. غُند دوم سرحدات زمینی مسئول نیمه بالایی سرحد بعبلک-هرمل با سوریه است. غُند سوم سرحدات زمینی در منطقه کوهستانی نزدیک راشیا فعال است وغُند چهارم سرحدات زمینی نیمه پایینی بعبلک-هرمل را پوشش می‌دهد.

تعهد لبنان به حفظ امنیت سرحدات باعث جلب حمایت همکاران بین‌المللی شده است. یان کولارد، سفیر بریتانیا در لبنان، دوروتی شی، سفیر ایالات متحده، و چنتل چستنی، سفیر کانادا در نومبر 2021 با جنرال جوزف حداد، قومندان اردوی لبنان، دیدار و درباره امنیت سرحد لبنان-سوریه گفتگو نمودند.

سفیر بریتانیا اظهار کرد: «این گفتگوها بالای ماموریت قوای مسلح لبنان در حوزه تامین امنیت تمام خط سرحد لبنان-سوریه و چالش‌های ناشی از بحران‌های مختلف لبنان متمرکز بود.»

در این جلسه، سفیر کولارد از تخصیص $1.4 ملیون برای تقویت آمادگی لبنان از طریق تامین پروزه جات اضافی موترهای لندرور دریافتی از بریتانیا و تجهیزات محافظ شخصی مخصوص عساکر مونث مستقر در مناطق سرحدی خبر داد.

بعد از اعلان خبر کمک بریتانیا، در سپتمبر 2021 ایالات متحده اعلان کرد که مبلغ $47 در قالب کمک نظامی به لبنان اهدا کرده است.

جوانا ورونکا، هماهنگ‌کننده مخصوص سازمان ملل در امور لبنان، در جریان سخنرانی در شورای امنیت سازمان ملل خواستار اعطای کمک‌های خارجی برای تقویت قوای مسلح لبنان شد و نقش حیاتی این کمک‌ها در محافظت از امنیت و ثبات لبنان را یادآورد شد.

منابع: دفتر هماهنگ‌کننده مخصوص سازمان ملل در امور لبنان، arabweekly.com، defensenews.com

قوای امنیتی لبنان در بندر سرحدی القاع، در سرحدات سوریه، مستقر شده‌اند.

آژانس خبری فرانسه/تصاویر گتی

اراده قرقیزستان برای اصلاحات داخلی

کارکنان یونیپاث

اتحادیه اروپا کمک‌هایی را برای حمایت از اصلاحات دولتی، پروگرام‌های حقوق بشری و حفظ امنیت آبی قرقیزستان اختصاص داده است.

در دسمبر 2021، اتحادیه اروپا کمک مالی به ارزش 62 ملیون یورو را در قالب پروگرام کمک‌رسانی چهار-ساله به قرقیزستان تصویب نمود.

در قسمت حکمرانی و دیجیتل‌سازی، این پول صرف ترویج و بهبود پروسه حاکمیت قانون و تحول دیجیتل خواهد شد.

انکشاف بشری، بشمول بهبود کیفیت تعلیم و ترویج برابری جنسیتی و حقوق بشر نیز بخشی از کمک‌های اتحادیه اروپا به بیشکک محسوب می‌شود.

اتحادیه اروپا همچنان بالای ضرورت قرقیزستان به یکپارچه‌سازی و توزیع منابع آبی در منطقه نیمه‌خشک این کشور تاکید کرده است. امنیت آبی در کشورهای آسیای میانی از زمان فروپاشی اتحاد شوروی همواره یکی از مسائل عمده دیپلماتیک بوده است.

این اولویت‌های مالی از طریق رایزنی قرقیزستان با کشورهای عضو اتحادیه اروپا تعیین شده است. این اولویت‌ها با پروگرام 2030 سازمان ملل، توافق اقلیمی پاریس و ستراتیژی دروازه جهانی اتحادیه اروپا مطابقت دارد.

سفیر ادوارد آور، رئیس هیات نمایندگی اتحادیه اروپا در قرقیزستان، در جریان پروگرام انعقاد قرارداد تامین مالی در اواخر 2021 اظهار کرد: «اتحادیه اروپا رابطه دیرینی با جمهوری قرقیزستان، منحیث یکی از همکاران اصلی و مطمئن حوزه انکشاف، دارد.

امروز ما گام مهمی در مسیر همکاری، تعهد به حمایت درازمدت از حکمرانی، دیجیتل‌سازی، تعلیم، رشد سبز و دیگر حوزه‌های موردعلاقه طرفین برمی‌داریم. این پروگرام جدید چندساله سند معتبری برای اثبات حمایت متداوم اتحادیه اروپا از مردم قرقیزستان است.»

منابع: Vesti.kg، Vecherniy Bishkek

رئیس‌جمهور قرقیزستان، سدیر جباروف، همراه همسرش در انتخابات پارلمانی در نومبر 2021 در بیشکک اشتراک می‌کند.

آژانس خبری فرانسه/تصاویر گتی

ترکمنستان اهداف سیاست خارجی خود را اعلان کرد.

کارکنان یونیپاث

قربان‌قلی بردی‌محمدوف، رئیس‌جمهور ترکمنستان، در جریان سخنرانی در مجمع عمومی سازمان ملل در 21 سپتمبر 2021، کشورش را متعهد به پیگیری صلح، امنیت و دیپلماسی دانست.

رئیس‌جمهور بردی‌محمدوف اعلان کرد که کشورش در دسمبر 2021 در عشق‌آباد میزبان جلسه به نام «پالیسی صلح و اعتماد - مبنای امنیت، ثبات و انکشاف بین‌المللی» خواهد بود.

او در سخنرانی خود در سازمان ملل پیشنهاد ایجاد منطقه صلح، اعتماد و همکاری با عنوان «آسیای میانه - منطقه خزر» را مطرح نمود. او تاکید کرد که ترکمنستان به بازگشت صلح، تعادل و وحدت به افغانستان کمک خواهد کرد.

رئیس‌جمهور بردی‌محمدوف در خاتمه سخنرانی خود بر آمادگی ترکمنستان برای پیگیری گفتمان درباره رسیدن به اهداف انکشاف متداوم، به شمول تداوم تمرکز بالای کاهش آثار بیابان‌زایی در اطراف دریای آرال، تاکید کرد. او برای ایجاد پروگرام مخصوص سازمان ملل در حوزه آبریز دریاچه آرال، در کنار دیگر کشورهای منطقه، ابراز آمادگی کرد.

منابع: Turkmenportal، سازمان ملل

متهم شدن حوثی‌ها به اعدام اشخاص ملکی

کارکنان یونیپاث

دولت قانونی یمن به اعدام غیرقانونی نُه نفر، بشمول یک پسر 17-ساله، که حوثی‌ها آنها را به همدستی در قتل رهبرشان متهم کرده بودند، اعتراض کرد.

این نُه نفر خودسرانه بازداشت شده بودند و بعد از متهم شدن به مشارکت در قتل صالح‌الصمد (2018) مورد شکنجه و آزار قرار گرفته بودند.

معمر العریانی، وزیر معلومات یمن، با صدور هشدار درباره تداوم این کشتار ملکی‌ها از طرف شبه‌نظامیان حوثی، این اعدام‌های فراقضایی را قتل عمدی با اتهامات واهی توصیف کرد.

الصمد به همراه شش تن دیگر در حمله هوایی قوای «ائتلاف احیای مشروعیت یمن» کشته شد. او برجسته‌ترین مقام این گروپ و رئیس شورای عالی سیاسی حوثی‌ها بود.

رسانه‌های منطقوی نام و عکس یمنی‌های اعدام‌شده را نشر کرده‌اند: علی الغوزی، عبدالمالک حمید، محمد حق، محمد الغوزی، محمد نوع، ابراهیم عاقل، محمد المشخری، عبدالعزیز الاسود و معز عباس، که همگی آنها از منطقه قناویس در ولایت الحدیده بودند.

سازمان‌های حامی حقوق بشر، مانند ائتلاف تفتیش موارد نقض حقوق بشر در یمن، SAM حقوق و آزادی‌ها، رادار حقوق بشر، انجمن مادران ربوده‌شده، و انجمن ملی دفاع از حقوق و آزادی‌ها مشترکاً با صدور بیانیه‌ای اقدام حوثی‌ها در اعدام اشخاص مسلکی را شدیداً محکوم نمودند.

جنگ 8-ساله باعث ویرانی یمن، تحمیل رنج شدید به مردم و آوارگی بیش از 4 ملیون تن از مردم یمن شده است. از زمان شروع جنگ داخلی در سپتمبر 2014، بیش از 233,000 تن کشته شده‌اند. 102,000 نفر از این تعداد بر اثر مستقیم جنگ و 131,000 نفر به دلایلی مانند قحطی و نبود امکانات صحی جان باخته‌اند.

نقض آشکار قوانین بین‌المللی بشردوستانه و سوءاستفاده از حقوق بشر از طرف شبه‌نظامیان حوثی در شکل‌گیری کلانترین بحران انسانی دنیا نقش داشته است. ضمناً، ممانعت حوثی‌ها از رسیدن کمک‌های بشردوستانه باعث شیوع گسترده مریضی، ازجمله وبا و کووید-19، شده است.

منابع: CNN، Alhurra، الجزیره

گفتگو و دیپلماسی بین ازبکستان و ایالات متحده

کارکنان یونیپاث

ازبکستان در دسمبر 2021 میزبان نخستین جلسه گفتگوی همکاری استراتیژیک با ایالات متحده بود که با هدف بررسی تعهدات دو کشور در قسمت تقویت امنیت در آسیای میانه شکل گرفته بود.

این جلسه در تاشکند و با میزبانی عبدالعزیز کمیلوف، وزیر خارجه ازبکستان، و دونالد لو، معاون وزیر خارجه ایالات متحده در امور آسیای جنوبی و مرکزی برگزار شد.

هر دو طرف بالای تداوم همکاری در قسمت مقابله با تهدیدات تروریستی و افراط‌گرایی و جلوگیری از ایجاد ناامنی در افغانستان تاکید کردند. قرضه‌دهی ازبکستان به ترمینال باری ترمذ با هدف تسهیل ارسال کمک‌های بشردوستانه به افغانستان مورد تحسین طرف امریکایی قرار گرفت.

دفتر کمیساریای عالی پناهندگان سازمان ملل و پروگرام جهانی غذای سازمان ملل از مرکز ترمذ برای ارسال غذا، خیمه، ظروف غذایی، کمپل و دیگر امکانات به افغانستان استفاده می‌کنند.

قرار شد که واشنگتن میزبان جلسه بعدی «گفتگوی همکاری ستراتیژیک» باشد. جلسه سال 2022 با جشن سی‌امین سالروز شکل‌گیری روابط دیپلماتیک بین ازبیکستان و ایالات متحده همزمان خواهد بود.

روابط ازبیکستان و ایالات متحده در دوره شش-ساله ریاست‌جمهوری شوکت میرضیایف، ریس‌جمهور وقت ازبکستان، بهبود یافته است و با گسترش همکاری‌ها و تعلیمات نظامی همراه بوده است.

عبدالعزیز کمیلوف، وزیر خارجه ازبکستان، چپ، در 2021 در واشنگتن دی.سی با آنتونی بلینکن، وزیر خارجه ایالات متحده، ملاقات کرد.

آژانس خبری فرانسه/تصاویر گتی

منابع: Anadolu Agency ،Gazeta.uz ،Caravanserai

امارات متحده عربی و تقویت امنیت سایبری

کارکنان یونیپاث

کمپنی اماراتی Majid Al Futtaim Retail، که جزو سوپرمارکت‌های برتر شرق میانه، جنوب آسیا و شمال افریقا محسوب می‌شود، جایزه برتر مراعات پروسیجرهای امنیت سایبری را بدست آورد.

در جریان نمایشگاه تکنالوژی امارات خلیج فارس (GITEX)، نمایشگاهی تجاری که در اکتوبر 2021 در دوبی برگزار شد، Majid Al Futtaim از طرف کمپنی Trend Micro به دلیل مساعی تامین امنیت زنجیره صدها خوراکه فروشی، منحیث برنده جایزه معرفی شد. Majid دارنده امتیاز و مدیر زنجیره Carrefour، مستقر در فرانسه، است.

Trend Micro اعلان کرد که Majid از بیش از 10,000 کمپیوتر، لپ‌تاپ و دستگاه همراه و 2,500 سرور در مقابل نفوذ هکرها و مجرمین محافظت می‌کند.

«در پنج سال گذشته، مشاهده اقدامات Majid Al Futtaim Retail در قسمت ایجاد تحول دیجیتل لذت‌بخش بوده است. ... خوشبختانه ما در این اقدامات شریک بوده‌ایم.» این گفته داکتر معتز بن علی، معین و مدیرعامل Trend Micro، است.

این کمپنی که نام آن برگرفته از ماجد الفطیم، موسس آن، است، یک کمپنی هولدینگ اماراتی مستقر در دوبی است که مراکز خرید و سرگرمی مختلفی را مدیریت و با Carrefour همکاری می‌کند.

Trend Micro یک کمپنی سافتویر چندملیتی امریکایی-جاپانی در حوزه امنیت سایبری است که دفترهای آن در توکیو، جاپان، و اروین، تگزاس، ایالات متحده، مستقر است.

امارات متحده عربی با درک تهدیدات سایبری رو به رشد در سرتاسر جهان، مساعی چشمگیری را برای پیشگامی در مسیر مقابله با تهدیدات بالقوه حوزه امنیت سایبری انجام داده است. داکتر محمد الکویتی، مشاور دولت امارات در امور امنیت سایبری، در جریان جلسه بین‌المللی ارتباطات دولتی 2021 که در سپتمبر 2021 در شارجه برگزار شد، خواستار توجه به مخاطرات سایبری شد.

الکویتی از حامیان تبادل معلومات بین کارگروپ‌های ملی امنیت سایبری و آگاهی‌بخشی درباره ضرورت محافظت از دستگاه‌های بخش دولتی و خصوصی محسوب می‌شود.

در جلسه بین‌المللی ارتباطات دولتی 2021 که در دو روز و با حضور 79 کارشناس از 11 کشور برگزار شد، زمینه تبادل تجربه و استراتیژی در حوزه محافظت از ارتباطات سریع جهانی فراهم شد.

منابع: Zawya.com، Al Ittihad، Emirates News Agency

اقدام پاکستان و ایالات متحده در کشف چند تن مواد مخدر غیرقانونی در افغانستان

کارکنان یونیپاث

دولت پاکستان راپور داد که مقدار بی‌سابقه‌ای مواد مخدر غیرمجاز از یکی از بندر سرحدی اصلی این کشور با افغانستان کشف کرده است.

طی صرفاً چند هفته در دسمبر 2021 و جنوری 2022، مقامات پاکستانی در بندر سرحدی تورخم مانع قاچاق 524 کیلوگرام چرس، 255 کیلوگرام هرویین، 280 کیلوگرام تریاک، و تقریباً 22 کیلوگرام کریستال شدند.

قوای امنیتی پاکستان مقادیر هنگفتی هرویین تولید افغانستان را در بندر سرحدی تورخم کشف کردند.

آژانس خبری فرانسه/تصاویر گتی

در 6 جنوری 2022، پاکستان موفق به کشف دو مخفیگاه جداگانه نگهداری هروئین شد. از یکی از آنها 100 کیلوگرام و از دیگری 130 کیلوگرام مواد مخدر کشف شد. مقدار مواد مخدر در مورد دوم در گذرگاه تورخم بی‌سابقه بوده است. به گفته احمد رضا خان، مامور ارشد گمرک در پیشاور، مقامات پاکستان در ترمینال وارداتی تورخم، با وعده دادن جایزه، موفق به کشف هرویین جاسازی‌شده در داخل یک موترلاری شدند.

قوای مبارزه با مواد مخدر پاکستان نیز مقادیر هنگفتی مواد مخدر غیرمجاز در نقاط مختلف این کشور کشف کرده است. در اواخر دسمبر، این سازمان اعلان کرد که موفق به کشف 2.2 تن مواد مخدر، شامل هرویین و کریستال شده است. در روزهای نخست جنوری نیز بیش از 3 تن مواد مخدر کشف شد.

به گفته عزلان اسلم، از مقامات اداره عوارض، مالیات و کنترول مواد مخدر در ولایت خیبر پختونخوا، مواد مخدر از مبداء افغانستان در «مقادیر هنگفت» وارد پاکستان می‌شود. این در حالی است که دولت جدیداً تشکیل‌شده طالبان وعده داده بود که مانع تجارت غیرقانونی مواد مخدر شود.

افغانستان همچنان منبع اصلی تامین همه ضروریات مربوط به تریاک و هرویین در سراسر دنیا محسوب می‌شود. این کشور در تولید کریستال و چرس نیز نقش مهمی دارد. تعداد مخفیگاه‌های مواد مخدر تولیدشده در افغانستان در ایران، جنوب شرقی اروپا و ترکیه نیز چند برابر شده است.

در دسمبر 2021، قوای بحری ایالات متحده 385 کیلوگرام هرویین را از قایقی ایرانی در دریای عربستان کشف کرد. دو هفته قبل از آن، یکی از کشتی‌های امریکایی پنج ملوان ایرانی را از یک قایق در حال سوختن در خلیج عمان نجات داده بود. ایرانی‌ها قایق را برای نابود کردن آثار جرم آتش زده بودند ولی ملوانان امریکایی توانستند 1,750 کیلوگرام چرس، 500 کیلوگرام کریستال و 30 کیلوگرام هرویین کشف کنند.

منابع: TRT World، قوای بحری ایالات متحده، Daily Pakistan

جنگ قوای مسلح عمان با گردباد شاهین

کارکنان یونیپاث

اقدام پیش‌دستانه قوای مسلح سلطان‌نشین عمان جان صدها شهروند عمانی ساکن در مسیر گردباد شاهین را در اکتوبر 2021 نجات داد.

مقامات عمانی بیش از 600 نفر را از طوفانی که بخشهایی از این کشور را درگیر ساخته بود، نجات دادند. این طوفان نتیجه وزش باد با سرعت حدود 150 کیلومتر/ساعت و ایجاد موجهایی با ارتفاع 10 متر بود.

عبور مردم از سرکی که بر اثر گردباد شاهین در شهر شمالی المصنعه در اکتوبر 2021 دچار جمع شدن آب شده بود

آژانس خبری فرانسه/تصاویر گتی

برای کاهش تلفات ناشی از گردباد، سرویس امنیت داخلی عمان رفت‌وآمد در ولایات البطینه شمالی و البطینه جنوبی را منع و صرفاً به موترهای عاجلی و حامل اقلام ضروری اجازه حرکت داد. جریان برق در القرم، در شرق مسقط، برای جلوگیری از وقوع حادثه قطع شد و بیش از 2,700 نفر به پناهگاه‌های عاجلی هدایت شدند.

مقامات عمانی به کارمندان دولتی رخصتی دادند و پروازهای ورودی و خروجی به/از میدان‌هوایی بین‌المللی مسقط را تا برطرف شدن خطر گردباد به تعویق انداختند. میزان ریزش باران در الخبوره، در شمال‌غربی پایتخت، مسقط، به 369 ملی‌متر رسید.

عالی‌جناب سلطان هیثم بن طارق یک کمیته وزارتی را برای ارزیابی خسارت مالی ناشی از گردباد تشکیل داد. دوستان عمان در منطقه نیز برای کمک‌رسانی اعلان آمادگی کردند. متعاقب تماس شهاب بن طارق، معین صدراعظم عمان در امور دفاعی، کویت اقدام به اعزام قوای نظامی به عمان کرد.

عالی‌جناب ملک عبدا... (دوم) بن آل حسین، پادشاه اردن، در تماس تلیفونی با سلطان هیثم بن طارق، مراتب همدردی و تسلیت خود را ابراز کرد و به مردم عمان وعدهٔ حمایت داد. منابع: BBC، رویترز، alkhaleejonline

همکاری استراتیژیک قزاقستان با ایالات متحده

کارکنان یونیپاث

در راستای انکشاف همکاری‌های دیپلماتیک و امنیتی، دیپلمات‌های عالی‌رتبه قزاقستان و ایالات متحده وعده دادند که کشورهای متبوع‌شان برای تقویت همکاری در قسمت مقابله با تروریزم، جلوگیری از گسترش سلاح‌های هسته‌ای و تامین امنیت سرحدات کوشش کنند.

جلسه دسمبر 2021 در آستانه، پایتخت قزاقستان، بین آکان رحمتولین، معاون وزیر خارجه قزاقستان، و دونالد لو، معین وزیر خارجه ایالات متحده در امور آسیای جنوبی و مرکزی، برگزار شد.

لو از طرف مقامات ایالات متحده از قزاقستان به خاطر مساعی جدی این کشور در قسمت رسیدگی به چالش‌هایی مانند امنیت سرحدات، مقابله با تروریزم، صلح‌بانی، جلوگیری از تکثیر سلاح‌های هسته‌ای، تغییرات اقلیمی و امنیت منطقوی قدردانی کرد.

او اقدامات قزاقستان در قسمت بازگرداندن جنگجویان خارجی و فامیل‌های آنان از مناطق جنگی را ستود و خواستار تداوم همکاری‌های دوجانبه در حوزه بازپروری و هم‌آمیزی این اشخاص شد.

دو طرف بر نقش مدیریتی بین‌المللی قزاقستان در جلوگیری از گسترش سلاح‌های هسته‌ای تاکید کردند. ایالات متحده بالای تعهد دیرین خود به همکاری با قزاقستان در قسمت خارج ساختن ضیاعات رادیواکتیو از مرکز آزمایش هسته‌ای سمی‌پلاتینسک که از دوران تسلط مسکو بالای منطقه باقی مانده است، تاکید کرد.

هر دو دیپلمات خواستار تحکیم روابط بین اردوهای متبوع، نهادهای سرحدی و گمرکی و نهادهای اجرایی شدند. این روابط قرار است ذریعه پلان پروگرام همکاری نظامی پنج-ساله بین وزارت دفاع قزاقستان و وزارت دفاع ایالات متحده گسترش یابد.

منابع: Voice of America، Baige News

عبیر عبدا... الراشد، عسکر سعودی، در نشستی خبری درباره تامین امنیت در مراسم سالانه حج در مکه معلومات‌رسانی می‌کند. رویترز

حضور مشتاقانه زنان سعودی در اردو

کارکنان یونیپاث

در رویدادی تاریخی، نخستین گروپ از عساکر مونث سعودی در سپتمبر 2021 و بعد از 14 هفته حضور در اردو از مرکز تربیت پایوران زن قوای مسلح عربستان سعودی فارغ‌التحصیل شدند.

مناحیل بنت صالح بن حمید، مربی نظامی، اظهار کرد: «پروگرام تعلیم روزانه با بازرسی صبحگاهی آغاز می‌شود و با درس تربیت‌بدنی تحت نظر مربیان آمادگی جسمانی ادامه می‌یابد. بعداً اشخاص برای صرف صبحانه رخصت می‌شوند و تعلیمات میدانی بعد از چاشت آغاز می‌شود. در خاتمه، اشخاص در صنوف نظری حاضر می‌شوند.»

جواز ورود زنان سعودی به اردو در 2019صادر شد. البته فعالیت عمومی نخستین عساکر زن در مراسم حج که در جولای 2021 در مکه برگزار شد، آغاز شد.

یکی از بانوان فارغ‌التحصیل نظامی اظهار کرد: «یکی از دلایلی که باعث پیوستن من به قوای مسلح شد، احساس امنیتی بود که با دیدن نگهبانان امنیتی یونیفورم‌پوش در اماکن عمومی به من دست می‌داد. به همین دلیل، با فراهم شدن فرصت رسیدن به این احساس امنیت، از این فرصت استفاده کردم.»

در مراسم فارغ‌التحصیلی، تورن جنرال عادل بن محمد البلوی، رئیس اداره تعلیم و ارشاد قوای مسلح عربستان سعودی، در سخنرانی خود به کارکرد «مرکز تربیت کادر زن» اشاره نمود.

«چشم‌انداز عربستان سعودی 2030» شامل ترویج برابری جنسیتی است. تصمیم‌سازان سعودی به این عقیده هستند که اصول حقوق معاصر زنان با آنچه در شریعت اسلام تضمین شده است، سازگاری دارد.

با دیدگاه بلندپروازانه، این پادشاهی در سال 2018 امکان فعالیت زنان در اداره امنیت عمومی وزارت داخله را در هفت منطقه از 13 منطقه عربستان سعودی فراهم کرد: ریاض، مکه، القسیم، المدینه، عسیر، الشرقیه و البها. از آن زمان تا فعلاً، تعداد قوای مونث افزایش یافته است.

منابع: CNN، الجزیره، رویترز

کویت شرایط پذیرش عساکر مونث را بررسی می‌کند.

کارکنان یونیپاث

در اقدامی برای تقویت قوای نظامی، قوای مسلح کویت در حال بررسی مزایای پذیرش زنان در اردو است.

تورن جنرال خالد الکندری، معین قوای بشری رئیس ارکان، اعلان کرد که بررسی‌های مربوط به پذیرش زنان تا ختم سال 2021 صورت خواهد گرفت.

مباحث مربوط به ضرورت پذیرش زنان در قوای مسلح در سپتمبر 2021 و در جریان کمپاین استخدامی که وزارت دفاع کویت با عنوان «در میان آنان باش» راه‌اندازی کرده بود، شکل گرفت.

کویت اقدام مشابهی را در سال 2018 انجام داده بود. در آن سال، شیخ ناصر الصباح، وزیر دفاع وقت کویت، از پذیرش زنان برای خدمت در اردو حمایت کرده بود. شیخ ناصر در آن زمان اظهار کرده بود: «اگر زنان بخواهند، مخالفتی با حضور آنان در اردوی ملی وجود ندارد.»

زنان هم‌اکنون در دیگر بخشهای امنیتی کویت وظیفه می‌کنند ولی تا فعلاً وارد اردو نشده‌اند. تعلیم مامور پولیس مونث از سال 2008 و با برگزاری صنف -40نفره آغاز شد. در مارچ 2016، پنج مامور زن پولیس منحیث نگهبانان مجمع ملی کویت به قوای امنیتی پیوستند.

مساعی کشورهای حوزه خلیج عربی برای توانمندسازی زنان پیشرفت آرام ولی مستمری داشته است. در بعضی از این کشورها زنان در جایگاه‌هایی

لمری بریدمن، سارا الصراف، بیرون از تعمیر مجمع ملی کویت مصروف پهره است. آژانس خبری فرانسه/تصاویر گتی

مصروف کار شده‌اند که قبلاً مختص مردان دستگاه‌های نظامی و امنیتی بود.

بیش از 30 سال قبل، قوای دفاعی بحرین جواز ورود زنان به بخشهای مختلف اردو را صادر کرد و بعضی از زنان به مدارج عالی رسیدند. در سال 2009، دو نظامی مونث بحرینی با اشتراک در پروگرام قومندانی و ستاد کل تاریخ‌ساز شدند و منحیث صاحب‌منصبان ستادی از کالج سلطنتی قومندانی، ستاد و دفاع ملی بحرین فارغ‌التحصیل شدند.

امارات متحده عربی نخستین کالج نظامی زنان در میان کشورهای حوزه خلیج عربی، یعنی «مکتب نظامی خوله بنت العزیز»، را در سال 1991 دایر نمود. زنان قطری برای نخستین بار در سال 2018 جواز ورود داوطلبانه به خدمت ملی را دریافت نمودند. منابع: الجزیره، Al Hurra

تاجیکستان و ازبیکستان: مقابله با تروریزم یک وظیفه مشترک است.

کارکنان یونیپاث

با هدف تقویت امنیت منطقوی در آسیای میانه، پارلمان تاجیکستان قراردادهای همکاری در قسمت دفاع هوایی و معلومات نظامی با ازبیکستان را تصویب کرد.

این قراردادها در جریان سفر رسمی شوکت میرضیایف، رئیس‌جمهور ازبیکستان، به تاجیکستان در جون 2021 امضا شده بود ولی تصویب نهایی آن از طرف مسئولین تاجیکستان در دسمبر 2021 صورت گرفت.

در قسمت دفاع هوایی، هر دو کشور با تبادل تجربه در حوزه هوانوردی و دفاع هوایی، برگزاری مانورهای مشترک، کمک‌رسانی به طیاره‌های یکدیگر در شرایط بحرانی و تبادل معلومات درباره ترافیک هوایی توافق نمودند.

تبادل معلومات عمدتاً بشمول تبادل داده‌های مربوط به فعالیت‌های مشکوک تروریستی و گروپ‌های افراط‌گرای مذهبی می‌شود. پروسه معلومات‌رسانی بشمول حامیان و همدستان تروریستان و سلاح‌ها، اردوهای تعلیمی و پایگاه‌های تروریستی است.

تاجیکستان و ازبیکستان همچنان درباره معلومات‌رسانی متقابل درباره تهدیدات تروریستی جدی، شامل مسائل مربوط به استقلال و تمامیت ارضی دو کشور، توافق کردند. این قرارداد که زمینه گسترش همکاری را فراهم می‌کند، امکان برگزاری مانورهای نظامی مشترک بین جزوتام‌های جنگی و معلوماتی را نیز فراهم می‌سازد.

قرارداد سوم بالای استفاده مشترک از حریم هوایی و میدان‌هوایی‌ها و ایجاد میکانیزم ورود خدمه هوایی از یک کشور به حریم هوایی کشور دیگر با هدف کمک‌رسانی در شرایط بحرانی و عاجلی متمرکز است. این قرارداد پنج سال اعتبار دارد.

تاجیکستان و ازبیکستان روابط دیپلماتیک و امنیتی خود را بعد از قدرت گرفتن رئیس‌جمهور میرضیایف در 2016 بهبود بخشیده‌اند.

منابع: Radio Free Europe/Radio Liberty، Eurasia Daily، Asia Plus

تامین امنیت انتخابات پارلمانی در عراق

کارکنان یونیپاث

مساعی مشترک صدها هزار تن از مامورین پولیس و پرسونل نظامی عراق منجر به تامین امنیت انتخابات پارلمانی شد. این رویداد در اکتوبر 2021 در سراسر این کشور برگزار شد.

کارمندان کمیسیون عالی مستقل انتخابات در حال شمارش ورق‌های رای در بغداد در اکتوبر 2021

آژانس خبری فرانسه/تصاویر گتی

وزارت داخله عراق اعلان کرد که کدام راپوری درباره حمله تروریستی، حادثه یا مشکل امنیتی دریافت نشده است. قابل یادآوری است که در انتخابات قبلی محدودیت رفت‌وآمد وضع شده بود.

پروگرام تامین امنیت انتخابات بشمول استقرار 300,000 تن از اعضای اردو، پولیس، قوای هوایی، هوانوردی نظامی و دفاع مدنی بود. مصئونیت 8,278 مرکز رای‌گیری در عراق در مقابل حملات تروریستی با اقدامات نظارتی هوایی تضمین شد.

«این انتخابات با انتخابات قبلی تفاوت اساسی دارد... و آن را می‌توان تقریباً یا کاملاً سازگار با استندردهای بین‌المللی دانست.» این گفته برید جنرال غالب العطیه، سخنگوی کمیته عالی انتخابات عراق، است.

حدود 9 ملیون عراقی از بین جمعیت 25 ملیون نفری واجدان شرایط رای دادن در این انتخابات اشتراک نمودند. در این دوره 329 نماینده مجلس از بین 3,200 نامزد مربوط به 167 حزب انتخاب می‌شوند.

عراق ابتدا قصد داشت این انتخابات را در سال 2022 برگزار کند، ولی مصطفی الکاظمی، صدراعظم، در جواب به اعتراضات عمومی مربوط به بیکاری و اختلالات خدمات عمومی، تاریخ انتخابات را تغییر داد. در قانون جدید انتخابات، پروسه رای دادن آسان شده است و تمهیداتی برای حضور نمایندگان گروپ‌های اقلیت و زنان عراقی پیش‌بینی شده است. منابع: رویترز، BBC، الجزیره

اقدام قطر در تقویت روابط بین اردوها با ترکیه

کارکنان یونیپاث

قوای بحری امیرنشین قطر ناوگان خود را با برگزاری مراسم رونمایی از ناوچه آبخاکی تقویت کرد. این ناوچه می‌تواند صدها نفر را روی عرشه خود انتقال دهد.

ناوچه آبخاکی تانک-بَر (LCT) با نام Fuwairit را کمپنی کشتی‌سازی آنادولو ترکیه در سپتمبر 2021 تولید کرده است.

LCT Fuwairit که نام آن برگرفته از یک قریه ساحلی در قطر است، می‌تواند 260 قوای مسلح کاملاً مجهز را روی عرشه 400 فت مربعی خود جای دهد. این ناوچه آبخاکی که 25 خدمه دارد، می‌تواند سه دستگاه تانک جنگی را همراه موترهای دیگر جابجا کند.

قطر قرار بود این شناور -یکی از شش کشتی که از ترکیه خریده است- را در تابستان 2022 تسلیم شود.

سوات ریفان آتیلان، مدیرعامل کمپنی کشتی‌سازی آنادولو، درباره خرید این شناور اظهار کرد: «ما قصد داریم همه جلسات امتحانی و تعلیمی را در 24 ماه آینده انجام دهیم و این شناورها را به قطر تسلیم نماییم.»

ضمن ناوچه آبخاکی، قطر فرمایش چندین کشتی را نیز به کشتی‌سازی آنادولو داده است و قرار است از آنها برای تعلیم صاحب‌منصبان کالج دریایی قطر استفاده کند. این کشور دارای خط ساحلی 563 کیلومتری در حاشیه خلیج عربی است.

این خریدها بخشی از قرارداد دفاعی مشترکی است که قطر در سال 2017 با ترکیه عقد کرده بود. این دو کشور برای تقویت روابط بین اردوهای خود، «قوای مشترک ترکیبی ترکیه-قطر» را در سال 2019 ایجاد نمودند. مقر این قوا در دوحه قرار دارد و نام آن از قومندان نظامی عرب قرن هفتم، خالد بن ولید، گرفته شده است.

قوای هوایی امیرنشین قطر در مانور چندملیتی دو-هفته‌ای «عقاب آناتولی» که در تابستان 2021 در قونیه برگزار شد، اشتراک نمود. پیلوتان پرواز با جت‌های جدیداً-خریداری‌شده فرانسوی Rafale را که به لوای جت 1 پایگاه هوایی تمیم تعلق داشت، تمرین کردند.

بربنیاد قرارداد تخنیکی بسته‌شده بین اردوهای دو کشور، قطر پیلوتان خود را به مدت پنج سال در ترکیه تعلیم می‌دهد و تا 250 تن از پرسونل و 36 فروند از طیاره‌های خود را در ترکیه مستقر می‌کند. منابع: Naval News، الجزیره، ahvalnews.com

انعقاد قرارداد امنیتی بین اردن و قطر

کارکنان یونیپاث

اردن و قطر در سپتمبر 2021، با عقد قرارداد همکاری امنیتی پنج-ساله، همکاری جدید خود در قسمت تبادل معلومات و تکنالوژی در حوزه مقابله با جرم را آغاز نمودند.

دو کشور برای تقویت همکاری‌های دوجانبه موجود در امر مبارزه با انواع جرایم تلاش خواهند نمود. این جرایم شامل تروریزم و تامین مالی مرتبط؛ جرایم سازمان‌یافته؛ قاچاق غیرقانونی سلاح، مهمات، مواد انفجاری و مواد هسته‌ای، رادیواکتیو، کیمیاوی و بیولوژیکی؛ قاچاق انسان و مهاجرت غیرقانونی؛ قاچاق، تولید و توزیع مواد مخدر؛ پول‌شویی؛ و جعل پاسپورت، اسعار و دیگر اوراق بهادار می‌شود.

از دیدگاه اقتصادی، این قرارداد بر محافظت مشترک از اموال معنوی، دارایی‌های تخنیکی، سیستم‌های معلوماتی و بنادر و سرحدات تمرکز داشت. در این قرارداد به مساعی مشترک در قسمت مقابله با دزدی دریایی و جرایم سایبری نیز اشاره شده است.

محمد بن عبدالرحمان آل ثانی، وزیر خارجه قطر، چپ، و ایمن الصفدی، وزیر خارجه اردن، در آگوست 2021 در نشستی خبری در عمان اشتراک نمودند. رویترز

قطر و اردن از زمان مستقل شدن قطر در سال 1971 روابط دیپلماتیک و نظامی مستحکمی داشته‌اند. کارشناسان اردنی در بخشهای اقتصادی، تعلیمی و نظامی قطر مصروف هستند.

جلالت مآب فقید ملک حسین بن طلال، پادشاه اردن، نخستین مقام رسمی خارجی بود که در سال 1995 وارد قطر شد و قدرت گرفتن جلالت مآب شیخ حمد بن خلیفه آل ثانی را به او تبریک گفت.

جلالت مآب ملک عبدا... دوم، پادشاه اردن، نخستین رهبر عربی بود که در جون 2013 به قطر سفر کرد و گزینش جلالت مآب شیخ تمیم بن حمد آل ثانی به عنوان امیر قطر را به او تبریک گفت.

اردوهای اردن و قطر بارها مانورهای مشترک برگزار کرده‌اند. قوای عملیات خاص قطر در سپتمبر 2019 در مانور چندملیتی «شیر در کمین» در اردن اشتراک نمودند. قوای اردنی نیز، در کنار قوای هفت کشور دیگر، در مارچ 2021 در مانور «نگهبان شکست‌ناپذیر» در قطر اشتراک نمودند.

منابع: alaraby.co.uk، Jordan News Agency، ammonnews.net

تقویت روابط مصر و قبرس

کارکنان یونیپاث

مصر و قبرس در ختم مانور «بطلمیوس 2021» در ماه سپتمبر بر تقویت روابط نظامی خود تاکید کردند.

این مانور شامل تمرین فیر با سلاح، تمرین جنگ تن‌به‌تن، حملات شبیه‌سازی‌شده به مخفیگاه‌های تروریستان و عملیات انتقال طبی بود. این همکاری دوجانبه تضمین نمود که مصر و قبرس از توانایی سنجش همکاری متقابل نظامی برخوردار هستند.

مصر و قبرس روابط نظامی محکمی دارند. قوای قبرسی -بشمول قوای بحری و عملیات خاص- بازیگران اصلی مانور دو-هفته‌ای چندملیتی «ستاره درخشان» بودند. این مانور به میزبانی قبرس در سپتمبر 2021 در پایگاه نظامی محمد النجیب برگزار شد.

«روابط در سطح فردی و در سطح قوای مسلح مصر و قبرس عالی و برادرانه است.» این ادعای رئیس ستاد کل قوای مسلح قبرس، دگر جنرال دموکریتوس زرواکیس، است که در حضور همتای وقت مصری خود ابراز کرد.

ضمناً مصر، قبرس و یونان نشست‌های سه‌جانبه‌ای را برای بررسی مسائل همکاری و هماهنگی در قسمت امور مرتبط با دریای مدیترانه شرقی، بشمول تعیین حدود سرحدات دریایی مشترک و مناطق اقتصادی خاص، برگزار می‌کنند.

در سپتمبر 2021، جلسه سران مصر و قبرس در قاهره با حضور عبدالفتاح السیسی، رئیس‌جمهور مصر، و نیکوس آناستاسیادس، رئیس‌جمهوری قبرس، برگزار شد. امنیت، دیپلماسی، تجارت، سیاحت و زراعت جزو موضوعات مورد بحث در این جلسه بود.

رئیس‌جمهور السیسی اظهار کرد: «همکاری استراتیژیکی که در مدیترانه شرقی شکل گرفته است، هماهنگی مستمر برای رسیدن به ثبات منطقوی و پایبندی به حمایت متقابل در همه حوزه‌های دارای منافع مشترک را ایجاب می‌کند.» منابع: egypttoday.com، defensearabia.com، Al Ahram

بحرین راه‌های تمویل تروریزم را مسدود می‌کند.

کارکنان یونیپاث

طبق شاخص ضدپول‌شویی بازل 2021، بحرین با پایین‌ترین آمار پول‌شویی، بهترین رتبه را در بین کشورهای عرب‌زبان دارد.

این سازمان مستقر در سوییس رتبه‌بندی خود را بربنیاد داده‌های دریافتی از کارگروپ اقدام مالی، شفافیت بین‌الملل، بانک جهانی و مجمع جهانی اقتصاد ارائه می‌کند.

شیخ سلمان بن عیسی آل خلیفه، معین رئیس بانک مرکزی بحرین، اظهار کرد: «این پادشاهی با کسب امتیاز 4.5 در بین کشورهای شرق میانه، بعد از اسرائیل، در قسمت مقابله با پول‌شویی در جایگاه دوم قرار دارد ولی در جهان عرب رتبه اول را در اختیار دارد.»

در جولای 2021، ستره محکمه جنایی بحرین شش مسئول Future Bank مستقر در بحرین را مجرم اعلان کرد. هریک از این اشخاص به جرم پول‌شویی به نفع بانک مرکزی ایران (CBI) به تحمل 10 سال حبس و پرداخت $2.5 ملیون جریمه محکوم شدند.

شیخه می بنت محمد آل خلیفه، مدیر اداره استخبارات مالی وزارت داخله، اظهار کرد که نهاد متبوعش در پی ارتقای رتبه منطقوی و بین‌المللی بحرین در قسمت مقابله با پول‌شویی و تامین مالی تروریزم است.

Future Bank متهم به پروسس تعاملات مشکوک مربوط به نهادهای مالی ایران، بشمول CBI، بود. این عمل ناقض قوانین و مقررات بحرین محسوب می‌شود. ارزش مبادلات -صورت‌گرفته با اسعار مختلف- به بیش از 1 میلیارد دالر می‌رسید.

منابع: alkhaleejonline.net ،baselgovernance.org

منطقه مالی بحرین در منامه

سهیم ساختن دانش

یونیپاث مجله‌ای است که بصورت مجانی در اختیار آنان که با مسائل امنیتی در شرق میانه و آسیای میانه و جنوبی سروکار دارند، قرار داده می‌شود.

درمجله یونیپاث سهم بگیرید

همه نظریات حکایوی، نامه به مدیر مسئول، مقالات حاوی نظریات، عکس‌ها، و دیگر مسائل را به دفتر مدیریت مسئول یونیپاث به آدرس الکترونیکی CENTCOM.UNIPATH@MAIL.MIL بفرستید.

چگونگی مراتب ارسال

- ترجیح داده می‌شود تا محتوای متن به لسان مادری‌تان باشد. یونیپاث مسئول ترجمه مطالب می‌باشد.
- مقالات نباید از مرز 1,500 لغت بگذرد.
- لطفاً شرح حال مختصر و معلومات در مورد چگونگی تماس با خودتان را ضمیمه هر مطلب ارسالی نمائید.
- حجم دیجیتالی عکس باید حداقل 1 میگا بایت باشد.

حقوق

مؤلفین مطالب حق تصاحب آنرا دارند. مع الوصف، ما حق تعدیلات در مقالات را به منظور جا دادن و پیرایش سبک آن را محفوظ نگه میداریم. ارسال مقالات متضمن طبع و نشر آن نمی‌باشد. با یاری رسانیدن به یونیپاث شما با این شرایط موافقت می‌نمائید.

برای اشتراک **مجانی** به آدرس زیر به ما ایمیل بزنید: CENTCOM.UNIPATH@MAIL.MIL

به این آدرس نامه بنویسید:
Unipath
U.S. Central Command
7115 S. Boundary Blvd.
MacDill AFB, FL 33621 USA

لطفاً اسم، شغل، القاب رسمی و یا سمت، آدرس پوستی و آدرس ایمیلی‌تان را شامل سازید.

HTTPS://UNIPATH-MAGAZINE.COM/FA