وطن امروز

روزنامه صبح ایران

VATANEMROOZ.IR

دوشنبه | ۲۸ مهر ۱۴۰۴ | ۲۷ ربیع‌الثانی ۱۴۴۷ | ۲۰ اکتبر ۲۰۲۵ | سال هفدهم | شماره ۴۴۴۱ | ۸ صفحه | ۱۰ هزار تومان

| ۱۱۹۱ سال و ۴۹ روز گذشت |

VATAN-E-EMROOZ | VOL.17 | NO.4441 | MON.OCT.20, 2025 | ISSN:2008-2886

گزارش «وطن امروز» به مناسبت آغاز چهل‌ودومین جشنواره فیلم کوتاه تهران

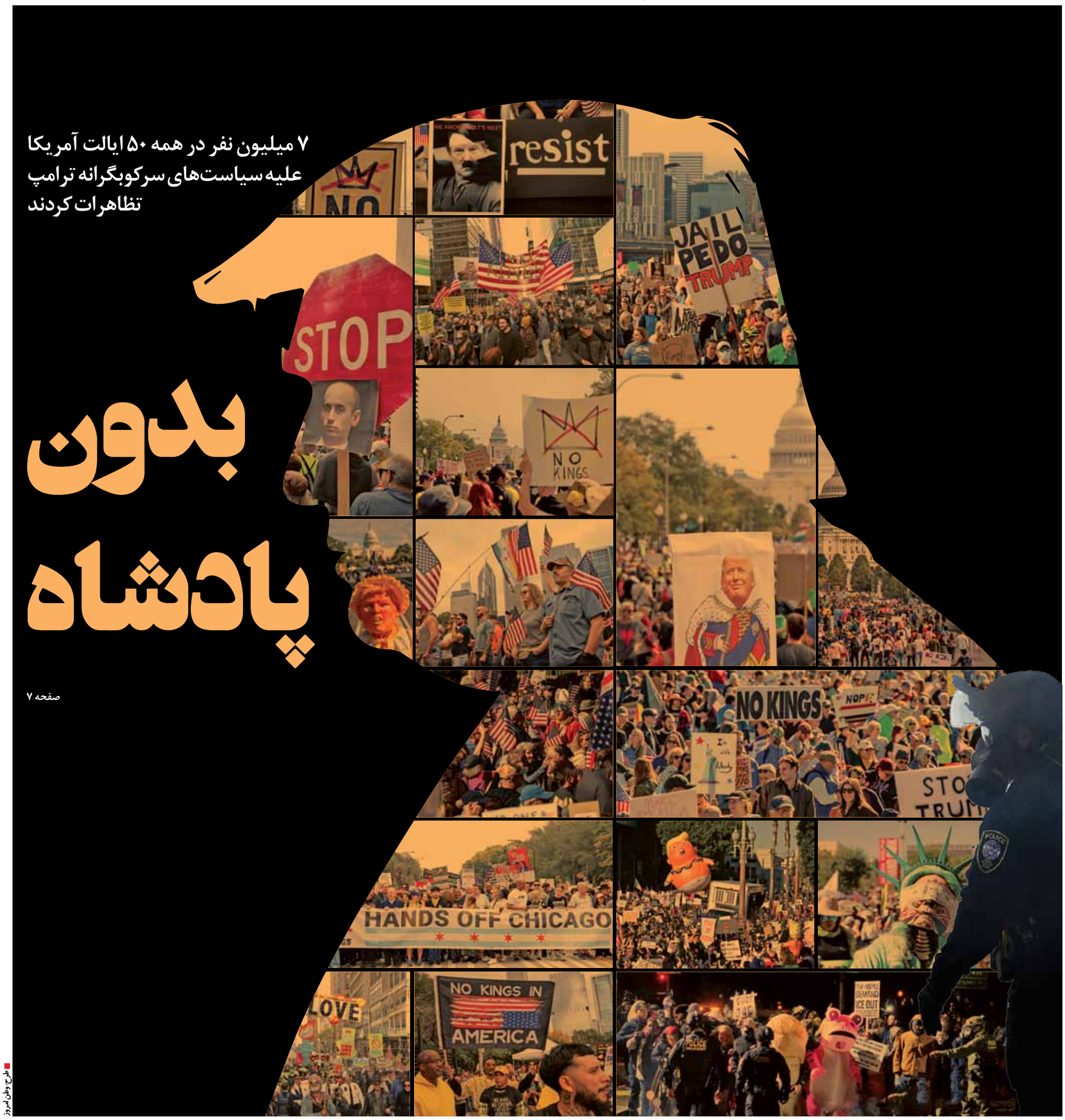
جشنی با حضور ستاره‌های فردا

صفحه ۸

رضا درویش نخستین قربانی باخت پرسپولیس در خرم‌آباد

بالاخره تسلیم شد!

صفحه ۶



۷ میلیون نفر در همه ۵۰ ایالت آمریکا علیه سیاست‌های سرکوبگرانه ترامپ تظاهرات کردند

بدون پادشاه

صفحه ۷

طرح وطن امروز

تیترهای امروز

یک دهه برای فهمیدن این واقعیت کافی بود؟

پایان توهم رفع تحریم

صفحه ۲

درباره فیلم منتشر شده علیه شمخانی از عملیات موساد تا ضرورت رعایت حقوق عامه

ترور زرد!

صفحه ۲

رژیم صهیونیستی با نقض آتش‌بس رفح و خان‌یونس را بمباران کرد

جنگ در کمین غزه

صفحه ۷

«وطن امروز» از پیامدهای حقوقی و قضایی اجاره حساب و کارت‌های بانکی به غیر گزارش می‌دهد

ویژه

مجرمان اجاره‌ای!

صفحه ۴

فروپاشی پارادایم اقتصاد آزاد جهانی و نیاز به بازآرایی نوین

نگاه

محمدامین حقگو

بسیاری از تحلیلگران و رهبران فکری برای دهه‌ها به مفهوم «اقتصاد آزاد جهانی» باور داشتند و آن را مسیر ناگزیر رفاه و ثبات می‌پنداشتند اما واقعیت‌های کنونی جهان حاکی از فروپاشی این ایده است. بر اساسی گزارشی که اخیرا فارن افرز منتشر کرده است، در واقع ریشه‌های این گسست نه‌تنها به دوران ریاست‌جمهوری دونالد ترامپ و سیاست‌های تجاری تهاجمی او بازنمی‌گردد، بلکه بسیار قبل‌تر، حتی در دوران پیش از روی کار آمدن وی، نفس‌های این نظم اقتصادی به شماره افتاده بود. رویدادها و تصمیمات مهمی در طول یک قرن گذشته این روند از هم‌گسیختگی را عمیق‌تر کرده است. به این معنی که اقتصاد جهان به شکلی که پیش‌تر می‌شناختیم، دیگر قادر به ادامه راه تجارت جهانی و آزاد نیست و سیاست‌های قدرت‌های بزرگ که اغلب به جای همکاری چندجانبه بر منافع ملی و یک‌جانبه‌گرایی استوار بوده، این وضعیت را آشکارتر کرده است.

■ **ردپای دگردیسی**

نگاهی به تاریخچه بازآرایی‌های بزرگ اقتصادی در قرن اخیر این موضوع را روشن می‌کند. نخستین بازآرایی بزرگ در «برتون وودز (۱۹۴۴)» رخ داد؛ جایی که ایالات متحده، با سوءاستفاده از موقعیت قدرت پس از جنگ دوم جهانی، سایر جهان را به پذیرش یک نظم اقتصادی بین‌المللی مبتنی بر دلار و مدیریت مرکزی واداشت. هرچند این سیستم به ظاهر چندجانبه بود اما در ماهیت به نفع ایالات متحده تمایل داشت و بنیان‌های آن برابری و توازن کامل را شامل نمی‌شد. دومین بازآرایی را ریچارد نیکسون، رئیس‌جمهور وقت آمریکا با رها کردن ستون مرکزی سیستم پولی برتون وودز (یعنی قابلیت تبدیل دلار به طلا) به شکلی یک‌جانبه اجباری کرد. در آن زمان، جان کانلی وزیر خزانه‌داری آمریکا، با بی‌توجهی به نگرانی‌ها درباره خشم متحدان گفت: «کشورهای دیگر دوست ندارند؛ خب! که چی؟!» این مواضع، حتی در دوران اوج دیپلماسی اقتصادی نشانه‌هایی از بی‌اعتمادی و فروپاشی رویکردهای واقعا چندجانبه و آزادی اقتصاد در بلندمدت را در خود داشت. حتی رونالد ریگان، نماد تجارت آزاد برای مقابله با صنعتی‌زدایی، تعرفه‌های ۱۰۰ درصدی بر محصولات ژاپنی اعمال کرد که نشانگر انحراف از اصول خالص اقتصاد آزاد دهه‌ها پیش از ترامپ بود.

■ **فرسایش و ناتوانی نهادهای جهانی**

با گذر زمان، ضعف‌ها و ناکارآمدی‌های سازمان تجارت جهانی نیز به این روند گسست کمک شایانی کرد.

ادامه در صفحه ۷

گروه هکری حنظله اطلاعات بیش از ۲۰ دانشمند صهیونیست در حوزه هسته‌ای و نظامی را منتشر کرد

پرونده‌های روی میز

گزارش

حسین کیامنش

گروه هکری حنظله اطلاعات بیش از ۲۰ دانشمند صهیونیست در حوزه هسته‌ای و نظامی را منتشر کرد

در جهانی که جنگ‌ها نه‌تنها با تسلیحات فیزیکی، بلکه با کدهای دیجیتال و نفوذهای سایبری پیش می‌رود، گروه هکری «حنظله» به عنوان نیرویی برجسته در این میدان ظاهر شده است. این گروه که از اواخر سال ۲۰۲۳ پس از عملیات توفان‌الاقصی فعال شده، با حملات سایبری متعدد علیه زیرساخت‌های حساس رژیم صهیونیستی، مرزهای جنگ سایبری را جابه‌جا کرده است. در روزهای اخیر حنظله در عملیاتی بی‌سابقه، هویت و اطلاعات شخصی بیش از ۲۰ متخصص ارشد نظامی و دانشمند اسرائیلی را افشا کرد؛ افرادی که در قلب پروژه‌های هسته‌ای، موشکی و دفاعی رژیم قرار دارند. جنگ سایبری ایران و اسرائیل که ریشه‌ای چنددهه‌ای دارد، از ۷ اکتبر ۲۰۲۳ و آغاز توفان‌الاقصی به اوج جدیدی رسید. گزارش سالانه مایکروسافت در سال ۲۰۲۵ مدعی است ایران از آن زمان «۷۰۰ درصد افزایش» در عملیات سایبری علیه اسرائیل داشته و این رژیم را به هدف اصلی خود تبدیل کرده است. بر اساس این گزارش که داده‌های ژوئیه ۲۰۲۴ تا ژوئن ۲۰۲۵ را پوشش می‌دهد، رژیم صهیونیستی از نظر تعداد حملات سایبری در صدر لیست اهداف ایران قرار دارد. این آمار، اسرائیل را نه‌تنها به عنوان هدف سیاسی، بلکه به عنوان کانون «جنگ هیبریدی» (ترکیب سایبری و اطلاعاتی) معرفی می‌کند و حنظله، بخش قابل توجهی از این موج سایبری است. این گروه هکری از نوامبر ۲۰۲۴ تاکنون با بیش از ۵۰ عملیات، سیستم‌های حساس اسرائیلی‌ها را هدف قرار داده است.

سابقه حنظله نشان‌دهنده عمق و گستردگی فعالیت‌هایش است. از نوامبر ۲۰۲۴ این گروه چندین عملیات بزرگ انجام داده؛ نفوذ به مراکز هسته‌ای دیمونا و سورک و استخراج نقشه‌های داخلی و ایمیل‌های محرمانه، هک تلفن «ایهود شانی» رئیس واحد سایبری ارتش صهیونیستی و سرقت ۲,۱ ترابایت داده از پلیس و وزارت امنیت در فوریه ۲۰۲۵ شامل پروفایل‌های روانی افسران و پرونده‌های جنایی. یکی از عملیات‌های غیرمنتظره حنظله، هک شبکه اینترنشنال در تابستان ۲۰۲۵ بود که طی آن حساب‌های تلگرامی خبرنگاران این شبکه (مستقر در لندن) هک شد و اطلاعات شخصی‌شان لو رفت. این اقدام نشان داد حنظله نه‌تنها علیه اسرائیل، بلکه علیه شبکه‌های وابسته به رژیم نیز عمل می‌کند. سایر حملات شامل هک رادارها، ارسال ۵۰۰ هزار پیام تهدیدآمیز در آوریل ۲۰۲۴ و نفوذ به شرکت‌های دفاعی مانند البیت و رافائل در ژوئن ۲۰۲۵ بود. این سابقه، حنظله را به ابزاری چندوجهی برای جنگ سایبری تبدیل کرده است. عملیات اخیر این گروه که اخیرا انجام شده، اطلاعات تعدادی از دانشمندان رژیم صهیونیستی را افشا کرد.

اطلاعات افشاشده شامل نام، وابستگی شغلی و تصاویر است. این افراد از شرکت‌های دفاعی کلیدی مانند آموس اسپیس کام (ارتباطات فضایی)، سیستم البیت (تجهیزات نظامی)، رافائل (تسلیحات پیشرفته)، نیروی هوایی اسرائیل، واحد ۸۲۰۰ (بخش سایبری ارتش صهیونیستی)، ایندور رباتیکز (رباتیک دفاعی)، آیرون درون (پهپادهای جنگی) و حیفای‌سی (فناوری محلی) هستند. در ادامه، لیست افراد به همراه محل فعالیت‌شان آورده شده است:

شای لوی (آموس اسپیس کام): متخصص ارتباطات ماهواره‌ای

ماتار بیتون (آموس اسپیس کام): مهندس فضایی، فعال در توسعه زیرساخت‌های ارتباطی برای پشتیبانی از مأموریت‌های نظامی

کابی کوهن (آموس اسپیس کام): مدیر پروژه‌های ماهواره‌ای

یعقوب کوهن (آموس اسپیس کام): فعال در حوزه امنیت سایبری ارتباطات فضایی

آمیتای ایتسکوویچ (آموس اسپیس کام): متخصص نرم‌افزارهای فضایی

تومر گرینبرگ (نیروی هوایی اسرائیل): فعال در توسعه تسلیحات هوایی برای عملیات در غزه و لبنان

سارا آبابه (نیروی هوایی اسرائیل): تحلیلگر رادار و فعال در حوزه پروژه‌های سیستم‌های دفاع موشکی

ساموئل منگشا (سیستم البیت): مهندس پهپاد و توسعه‌دهنده سلاح‌های خودکار برای عملیات نظامی

ایتای گولان (نیروی هوایی اسرائیل): متخصص حوزه موشک

گای ماخلف (نیروی هوایی اسرائیل): مدیر عملیات هوایی

عیران گرین (سیستم البیت): طراح سیستم‌های الکترونیکی

مائور عینی (واحد ۸۲۰۰): تحلیلگر سایبری و فعال در نفوذ به شبکه‌های دشمن

گای کوهن (سیستم البیت): مهندس تسلیحات و توسعه‌دهنده پهپادهای انتحاری برای عملیات تهاجمی

یانا چن (نیروی هوایی اسرائیل): متخصص هوش مصنوعی در عملیات هوایی

داویر ساسون (رافائل): طراح موشک، با نقش در پروژه‌های گنبد آهنین و تسلیحات هسته‌ای

عومر آرتزی (رافائل): مهندس سیستم‌های دفاعی

تساخ شورمن (نیروی هوایی اسرائیل): مسؤول تست سلاح‌های جدید در میدان

ماتان شالو (ایندور رباتیکز لیمیتد): توسعه‌دهنده ربات‌های جنگی

جریس دانیال (حیفای‌سی): متخصص الکترونیک و فعال در زمینه تولید قطعات تسلیحاتی برای ارتش صهیونیستی

بن توبول (آیرون درون): طراح پهپاد

حنظله ادعا می‌کند این اطلاعات از نفوذهای عمیق به سیستم‌های حساس رژیم صهیونیستی استخراج شده، از جمله ۲۰ گیگابایت داده از مرکز سورک در نوامبر ۲۰۲۴ و ۱۹۷ گیگابایت از دیمونا.

بیانیه حنظله، این افراد را «معماران ویرانی» معرفی و اعلام کرده آدرس‌های منزل، ایمیل‌ها، شماره تلفن‌ها و ارتباطات کاری دانشمندان و متخصصان صهیونیست (از جمله با شرکت‌های آمریکایی و اروپایی) را در اختیار دارد. رسانه‌های صهیونیستی مانند هاآرتص و تایمز اسرائیل، حنظله را مرتبط با ایران می‌دانند و شواهد این ادعای‌شان، همسویی اقدامات حنظله در راستای مواجهه ایران با اسرائیل است اما نکته حیاتی این است: آنچه منتشر شده، احتمالاً تنها «نوک کوه یخ» است. حجم عظیم داده‌ها (مانند ۲,۱ ترابایت از پلیس یا ۱۹۷ گیگابایت از دیمونا) نشان می‌دهد اطلاعات بسیار بیشتری – از نقشه‌های زیرساختی گرفته تا جزئیات پروژه‌های محرمانه – در دسترس هکرها قرار دارد. اگر ادعاهای رسانه‌های صهیونیستی درباره ارتباط حنظله با ایران درست باشد، این داده‌ها اکنون در اختیار ایران است. این شامل اطلاعات حساس درباره زیرساخت‌های هسته‌ای (دیمونا و سورک)، شبکه‌های ارتباطی نظامی (آموس اسپیس کام)، سیستم‌های دفاعی (رافائل و گنبد آهنین) و حتی ارتباطات خارجی با آمریکا و اروپا می‌شود. چنین اطلاعاتی از اهمیت بالایی برخوردار است.

برای مثال، نقشه‌های داخلی دیمونا می‌تواند نقاط ضعف این مرکز هسته‌ای را مشخص کند و داده‌های واحد ۸۲۰۰ می‌تواند شبکه‌های جاسوسی سایبری اسرائیل در منطقه را افشا کند. این حجم از اطلاعات نشان می‌دهد زیرساخت‌های امنیتی رژیم صهیونیستی – برخلاف ادعاهای رسمی این رژیم – پر از حفره‌های بحرانی است. موفقیت‌های مکرر حنظله، از هک سیستم‌های اضطراری تا نفوذ به مراکز هسته‌ای، ثابت می‌کند اسرائیل در برابر حملات سایبری بسیار شکننده‌تر از چیزی است که به نظر می‌رسد.