# مستندات اجمالی
# بیانیه شماره ۱ آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
# در خصوص سانحه دلخراش هواپیمای مسافربری اکراینی

۲۳ دی ۱۳۹۸

## فهرست مطالب

## مقدّمه

حادثه‌ی تأسف‌بار هواپیمای مسافربری اوکراینی که به‌واسطه‌ی آن جمعی از هموطنان عزیز درگذشتند، فارغ از تمامی مباحث سیاسی و حواشی رسانه‌ای، اتکا بر ابعاد فنی و تخصصی دارد که لازم است مورد بررسی قرار گیرد. از این رو گزارش حاضر در حد وسع اطلاعاتی و اسنادی، به بررسی این مهم خواهد پرداخت.

## اشارات فنی فرمانده‌ی نیروی هوافضای سپاه پاسداران انقلاب اسلامی

مبتنی بر توضیحات سردار سرتیپ پاسدار حاجی‌زاده مورخ ۲۱ دی ۱۳۹۸ در رسانه‌ی ملی، دو کلیدواژه‌ی اساسی از جنبه‌ی تخصص سایبرنتیک وجود دارد:

۱. ثبت موشک کروز توسط رادار سامانه‌ی پدافند موشکی
۲. اخلال در ارتباطات سامانه با رده‌های بالاتر

## بررسی اسناد و رفتار نظامی ایالات متحده‌ی آمریکا در میدان منازعات سخت

مجموع بررسی اسناد رسمی دفاعی ایالات متحده‌ی آمریکا و سابقه‌ی اقدامات میدانی ارتش آمریکا در منازعات سخت حاکی از آن است که بخش چشمگیری از اتکای نیروهای مسلح آمریکا در میدان عمل متکی بر عملیات‌های جنگ سایبرنتیک است. زیرا کشورهای مقابل آمریکا، همگی دارای ارتش‌های پیشرفته هستند و تجهیزات راهبردی آنها توسط **سیستم‌های فرماندهی و کنترل** مدیریت و هدایت می‌شود که سامانه‌های موشکی ایران نیز از این دسته است. در این صورت اگر بخش فرماندهی و کنترل هر سامانه را تحت تأثیر قرار دهد، یا متوقف می‌شود یا عملکرد آن تضعیف و دچار خطا می‌گردد. در نتیجه تسلیحات یا تجهیزات مبتنی بر آن غیر فعال شده یا دچار خطا در فعالیت می‌شود.

نیروهای مسلح آمریکا به‌منظور اجرای جنگ سایبرنتیک و فرماندهی – کنترل، تجهیزات بسیاری دارند که اکثر آنها هوایی است و شامل ماهواره‌ها، پهپادها و هواپیماهای مختلف می‌شود. شایان ذکر است شرکت بویینگ که هواپیمای اوکراین متعلق به آن است، بزرگترین سازنده‌ی تجهیزات هوایی جنگ سایبرنتیک و الکترونیک برای ارتش ایالات متحده‌ی آمریکا و مجموعه‌ی ناتو می‌باشد.

## راهبرد دفاعی اخلال در پرتاب

بر اساس این قاعده‌ی مهم در ارتش ایالات متحده، راهبردهای مختلفی در سال‌های گذشته تدوین و منتشر شده است. یکی از آنها که در سال ۲۰۱۵ انتشار یافت، سندی راهبردی با عنوان «اخلال در پرتاب»[1] است که به راهکارهای مقابله با توان موشکی دشمنان، پیش از پرتاب موشک‌ها می‌پردازد. متن سند در خصوص اصطلاح اخلال در پرتاب چنین توضیح داده است:

> **این راهبرد مبتنی بر اقدام پیشگیرانه توسط تکنولوژی‌های غیر سینتیکیِ جدید مانند امواج الکترومغناطیسی و حملات سایبری به‌منظور دفع تهدیدات موشک‌های بالستیک است که قبل از پرتاب؛ شناسایی شده و علیه آنها اقدام می‌شود.[2]**

[1] Left of Launch

[2] http://missiledefenseadvocacy.org/alert/3132/

بر اساس سند مذکور، راهبرد پرتاب در اخلال طی چند سال گذشته در آزمایشگاه‌های پنتاگون و دولت به‌عنوان بخشی از تلاش برای کاهش هزینه‌های استفاده از سیستم‌های دفاع موشکی و مقابله با حمله‌ی تعداد بی‌شماری از موشک‌های بالستیک در حال بررسی بوده و برای گسترش آن در سراسر جهان باید توسط آمریکا و تمامی متحدانش اجرا شود.[۳]

در این سند صراحتاً به ایران و کره‌ی شمالی به‌عنوان دو کشوری که از راهبرد اخلال در پرتاب علیه آنها استفاده خواهد شد، اشاره شده است:

> **ایالات متحده قطعاً نیاز به سرمایه گذاری، توسعه و ایجاد سیاست‌های قابل قبول دارد تا در نهایت تکنولوژی‌ها و سیستم‌های اخلال در پرتاب را برای جلوگیری از تهدید ناگهانی و رو به افزایش، توسعه دهد. اما در واقعیت، اتکای صرف به قابلیت اخلال در پرتاب برای دفاع در برابر موشک‌های بالستیک کشورهایی نظیر ایران یا کره‌ی شمالی مشکل‌ساز است؛ زیرا این امر بستگی به حملات پیشگیرانه‌ی ایالات متحده علیه کشورهای هسته‌ای مانند کره‌ی شمالی و احتمالاً ایران در آینده دارد پیش از آنکه آنها بتوانند حمله‌ای را آغاز نمایند.**[4]

به‌طور خلاصه، راهبرد اخلال در پرتاب دارای دو فرض اصلی است:

۱. احتمال اینکه دشمن دست به اقدامات گسترده‌ی موشکی بزند، بسیار زیاد است.
۲. هیچ سامانه‌ی پدافند موشکی، توان مقابله با حجم بالایی از موشک‌های پرتاب شده را ندارد و قطعاً بخش چشمگیری از آنها به اهداف از پیش تعیین شده اصابت خواهد کرد.

ایالات متحده در این راهبرد برای رفع مشکل فوق بیان می‌دارد که در نتیجه باشد پیش از آنکه موشک پرتاب شود؛ از شلیک آن ممانعت شود یا هدفی جعلی برای آن تعریف گردد که پرتاب موشک را منحرف سازد. برای عملیاتی‌سازی این راهبرد، لازم است از جنگ سایبرنتیک استفاده گردد.

این راهبرد در مواقع مختلفی مورد آزمایش قرار گرفته و موفقیت آن احراز شده است. در این باره خبرگزاری تلگراف انگلیس در خبری با عنوان «حملات سایبری آمریکا ممکن است سیستم‌های موشکی کره‌ی شمالی را از کار بیندازد.»[5] چگونگی عملکرد این راهبرد را از حیث فنّی چنین توضیح داده است:

> **شیوه‌های [اجرایی] راهبرد اخلال در پرتاب عبارتند از انتشار امواج الکترومغناطیسی و حملات سایبری علیه موشک‌ها بلافاصله پس از رهاسازی.[6] امواج الکترومغناطیس با آلوده‌سازی سلاح، سیستم فرماندهی – کنترل یا سیستم‌های هدف گیری را مختل می کند.**[7]

در متن خبر فوق بیان شده که در سال ۲۰۱٤، اوباما علی‌رغم وجود موشک‌های ضد سکوهای موشکی، دستور به تحقیقات بیشتر درخصوص راهبرد اخلال در پرتاب داده و خاصتاً کره‌ی شمالی را مدنظر داشته است.

---

[۳] همان

[4] همان

[5] US cyber attacks may be bringing North Korean missiles down

[۶] بر اساس منابع رسمی و موثق، راهبرد اخلال در پرتاب، پیش از رهاسازی موشک مؤثر است نه پس از آن. لذا آنچه در متن خبر اشاره شده صحیح نیست.

[7] https://www.telegraph.co.uk/news/2017/04/06/left-of-launch-attacks-may-bringing-north-korean-missiles/

همچنین خبرگزاری ایندیپندنت انگلیس در یک خبر تحلیلی ضمن تأکید بر نقاط ضعف سیزده‌گانه که توسط چتم‌هاوس بیان شده است، اظهار داشته:

**سیستم‌ها دارای مواردی از آسیب‌پذیری هستند که باعث می‌شود مهاجمان سایبری به آنها نفوذ کرده و با راه‌اندازی موشک‌ها، عواقب مرگباری را موجب شوند. این احتمال وجود دارد که هکرها حتی به سیستم‌های پیچیده‌ی هسته‌ای نیز دست یابند. اگر این حملات سایبری، مهاجمان را قادر به نصب برنامه‌های مخرب یا ویروس نماید، باعث می‌شود کشور به‌دلیل تولید اطلاعات نادرست دچار تصمیمات اشتباه شود. اگر سیستم‌ها متوقف شوند، ممکن است کشور تصور کند دچار حمله شده است در حالی که اینگونه نیست و حتی ممکن است به اشتباه کلاهک‌های هسته‌ای مرگبار را پرتاب نماید.**[8]

در این خبر به دو نوع از تهدیداتی که قبلاً بیان شده بود، اشاره شده است: تهدیدات علیه رکن اینتلیجنس و تهدیدات علیه رکن محاسبات. رکن اینتلیجنس از طریق نفوذ ویروس و بدافزار و ارسال اطلاعات اشتباه به فرماندهی –کنترل موشک تهدید شده و رکن محاسبات نیز از طریق حملاتی که به صدور اخطارهای اشتباه درباره‌ی حمله‌ی دشمن منتج می‌شود، دچار خطای جدی می‌گردد که می‌تواند حتی باعث پرتاب موشک شود.

این راهبرد در جولای ۲۰۱۷ به‌صورت مفصل توسط اندیشکده‌ی آتلانتیک[9] ایالات متحده در مقاله‌ای تخصصی با عنوان «اخلال در پرتاب: مقابله با موشک‌های بالستیک در صحنه»[10] مورد تحلیل و بررسی قرار گرفته است.

موشک‌های TBM آن دسته از موشک‌های بالستیک هستند که برد آنها بین ۳۰۰ الی ۳۵۰۰ کیلومتر بوده و برای انهدام اهداف در صحنه استفاده می‌شوند.[11] از این رو به آنها موشک‌های بالستیک در صحنه گفته می‌شود. بر این اساس مشخص می‌شود که راهبرد اخلال در پرتاب خاصتاً برای موشک‌های TBM است و همه‌ی موشک‌ها را شامل نمی‌شود.

از سوی دیگر برد اکثر موشک‌های آفندی و پدافندی ایران اسلامی که پایه‌ی قدرت موشک‌های بالستیک را تشکیل می‌دهند نیز در همین رده است.

در ابتدای مقاله‌ی اندیشکده‌ی آتلانتیک، راهبرد اخلال در پرتاب چنین معرفی شده است:

**زمان آن فرا رسیده است که بازی از حالت کاملاً تدافعی به مبارزه علیه منابع تبدیل شود. حمله به منابعی که شامل سیستم‌های پرتاب موشک‌های TBM و زیرساخت‌های پشتیبانی آن است؛ پیش از آنکه موشک پرتاب شود. پرتاب یک موشک TBM به سادگی آخرین اتصال در یک زنجیره‌ی پیچیده از وقایع مورد نیاز است تا آثار سینتیکی محقق شود. تمام بخش‌های زنجیره که باعث می‌شوند پرتاب موشک انجام شود، در برابر اختلال یا تخریب به‌صورت بالقوه آسیب‌پذیر هستند و زمان عنصر بسیار مهمی برای اخلال در پرتاب موشک‌های TBM به‌منظور مقابله با تهدیدات آنها است.**[12]

همچنین در خصوص گستره‌ی انواع لانچرهای موشک‌های TBM که این راهبرد توان مقابله با آنها را دارد، بیان شده است:

[8] https://www.independent.co.uk/life-style/gadgets-and-tech/news/nuclear-weapons-warhead-weapon-hack-cyber-attack-a8153526.html
[9] http://www.atlanticcouncil.org/publications/issue-briefs/left-of-launch
[10] Left of Launch: Countering Theater Ballistic Missiles
[11] https://fas.org/nuke/intro/missile/tbm.htm
[12] Left of Launch: Countering Theater Ballistic Missiles - Page 2

**برای اجرایی نمودن اخلال در پرتاب به‌عنوان زیرمجموعه‌ای از عملیات هوایی، باید معماری عملیاتی مقابله با لانچرهای متحرک TBM نیز توسعه یابد؛ یک معماری که بتواند لانچرهای متحرک TBM و عناصر حمایت‌کننده‌ی آن را شناسایی و ردیابی نموده، اطلاعات هدفمند را به‌منظور حمله به سیستم‌ها ارسال کرده و سلاح را روی هدف مذکور [لانچر موشک] تنظیم نماید. علاوه بر آن، این راهبرد باید در شرایطی موفقیت‌آمیز باشد که پدافند هوایی مرگبار در حال فعالیت بوده و اختلال در ارتباطات بسیار شدید است.**[13]

از متن فوق، علاوه بر آنکه مشخص می‌شود راهبرد اخلال در پرتاب برای هر دو نوع لانچرهای ثابت و متحرک کارایی دارد، روشن می‌گردد که نحوه‌ی اجرای آن از آسمان بوده و مجری آن نیروی هوایی دشمن است.

بر اساس این سند، مکانیسم فنّی راهبرد اخلال در پرتاب در صحنه‌ی نبرد، به‌صورت زیر است:

**نیروی هوایی ایالات متحده در حال تولید یک مفهوم حساس به‌عنوان سرویسی است که با اتکا به سیستم ماهواره‌های تجاری است و می‌تواند اهداف متحرک و پنهان شده را در خطر قرار دهد.**

**تا سال ۲۰۱۸، ماهواره‌هایی مانند SmallSAT با تکنولوژی EO[14]، IR[15]، MSI[16]، HSI، و قابلیت‌های راداری ممکن است قادر به ارائه‌ی تصاویر با رزولوشن ۰.۵ تا ۵ متر و پوشش شکاف در حدود ۱ تا ۱۰ دقیقه باشند.**

**سیستم‌های مادون قرمز مبتنی بر فضا[17] قادر به ارائه‌ی هشدار زودهنگام موشک، پدافند موشکی و آگاهی از صحنه‌ی نبرد؛ از این رو SBIRs[18] عملیات اکتشاف را به‌سرعت برای یافتن مناطق لانچرهای موشک TBM شناسایی می‌کند. در این حالت منابع ISR باید بر پشتیبانی عملیات ضد حمله تمرکز یابند.**

**بهترین پشتیبانی از الزامات پلت‌فرم حمله با توجه به فرض قطع شدن ارتباطات خودی، پدافند هوایی سنگین دشمن و افت GPS، توسط جنگنده‌هایی از نسل پنجم امکان‌پذیر است که مسلّح به تسلیحات اهداف ثابت و متحرک بوده و مبتنی بر هدایت ترمینال با حسگرهای داخلی باشد.**[19]

همچنین «انستیتو خدمات متحد هندوستان»، در مطلبی با عنوان «راهبرد دفاعی اخلال در پرتاب آمریکا»[20] به واکاوی این راهبرد پرداخته است. مهم‌ترین نکته‌ی متن اذعان دارد:

[13] Left of Launch: Countering Theater Ballistic Missiles - Page 5
[14] Electrooptical
[15] Infrared
[16] Multispectral Imaging
[17] SBIRSs
[18] The space-based infrared systems
[19] Left of Launch: Countering Theater Ballistic Missiles - Page 6 and 7
[20] The American ‘Left of Launch’ Defense Strategy

**استفاده از حملات غیر جنبشی علیه سیستم‌های سایبرنتیکی موشک‌ها، سنسورها و دیگر شبکه‌ها، توسط تکنولوژی‌های سطح بالا به این معنا است که موشک‌ها روی زمین از پای در می‌آیند. در جنگ‌های آینده این شیوه بر شیوه‌های دیگر ترجیح داده می‌شود. ویژگی اصلی این راهبرد، حمله سایبری و الکترومغناطیسی به سیستم‌های فرماندهی - کنترل است.**[۲۱]

در مجموع می‌توان نتیجه گرفت آمریکا و متحدانش با راهبرد اخلال در پرتاب و دیگر راهبردهای مشابه، تمرکز اصلی خود را در میدان نبرد بر متوقف‌سازی توانمندی‌های دشمنانشان پیش از هرگونه استفاده از آنها قرار داده‌اند که بستر اصلی دستیابی به این هدف، سیستم‌های فرماندهی – کنترل به‌کار رفته در تجهیزات و سامانه‌های نظامی آفندی و پدافندی دشمن می‌باشد.

## نمونه‌هایی از عملیات‌های سایبری علیه قدرت موشکی ج. ا. ایران

هر چند سیستم کلان فرماندهی – کنترل نیروهای مسلّح در جمهوری اسلامی ایران مطابق قواعد و پروتکل‌های ناتو و ایالات متحده‌ی آمریکا نیست، اما فرایندهای اساسی در یک سیستم فرماندهی – کنترل از اصول اساسی که در گزارش حاضر به آنها اشاره شد، تبعیت می‌کند. لذا تهدیدات پایه و اصلی علیه تمامی سیستم‌های فرماندهی – کنترل در سراسر جهان –از جمله ایران– یکسان بوده و ارتباط مؤثری با معماری فرماندهی – کنترل کشور ندارد. از این رو حملات سایبری علیه سیستم‌های موشکی ایران نیز مؤثر خواهد بود و بر اساس اطلاعات موجود، سابقاً نیز رخ داده است که در ادامه به چند مورد آن با حفظ طبقه‌بندی‌های آنها اشاره خواهد شد.

### یک) حمله به رکن فرمان موشک

حدوداً یک سال و نیم گذشته در آزمایش موشکی، یک موشک بالستیک دو مرحله‌ای[۲۲] توسط سپاه پاسداران پرتاب شد. آنچه رخ داد این بود که موتور مرحله‌ی اول با موفقیت روشن شد و مأموریت خود را به پایان رسانده و از بدنه‌ی موشک جدا شد. پس از آن موتور مرحله‌ی دوم نیز با موفقیت روشن شد اما پس از چند ثانیه دستور «خاموش» به موتور موشک رسید. در نتیجه موشک خاموش شده و در مکانی نامطلوب سقوط کرد.

شواهد عینی و میدانی حاکی از آن است که این رخداد بر اساس نقص فنّی نبوده بلکه اپراتورهای سیستم فرماندهی – کنترل موشک، به‌وضوح دریافت دستور خاموش توسط موشک را رصد نموده‌اند اما نسبت به اینکه از کجا ارسال شده مطلع نیستند. آنچه صرفاً مشخص شده این است که یک سیگنال ناشناس به موشک نفوذ کرده و دستور خاموش را صادر کرده است.

در این نمونه‌ی عینی، دقیقاً رکن فرمان در سیستم فرماندهی – کنترل موشک مورد حمله قرار گرفته و اثری بر آن گذاشته که موجب صدور دستور خاموش برای موتور موشک است. یعنی نوع حمله از میان پنج حالت حذف، توقف، تحریف، تأخیر در اجرا و جابجایی اولویت، مصداق توقف بوده است.

آنچه لازم به‌ذکر است این است که سیستم راهبری موشک مذکور، بر اساس INS بوده که مسئولان مربوطه نسبت به امنیت آن اطمینان زیادی دارند.

[21] http://usiblog.in/2016/04/the-american-left-of-launch-defense-strategy/

[۲۲] به‌دلیل رعایت ویژگی‌های طبقه‌بندی اطلاعات حساس، امکان ذکر نام موشک و تاریخ دقیق آن به‌صورت مکتوب وجود ندارد.

### دوم) حمله به سیستم TT&C ماهواره‌های موشک

از حیث فنّی، فرماندهی – کنترل بعضی از موشک‌ها توسط ماهواره‌های مخصوص صورت می‌پذیرد که TT&C نام دارد. یکی از نگرانی‌های جدی (که شواهدی بر وقوع آن علیه ایران وجود دارد) حمله به ماهواره‌های TT&C است.

به‌طور کل TT&C مخفف Telemetry, Tracking, and Command به معنای «تله‌متری (که قبلاً در همین گزارش توضیح داده شد)، رهگیری و فرمان» است و نوعی کامل از سیستم فرماندهی – کنترل می‌باشد زیرا از تمامی ارکان این سیستم‌ها برخوردار است.

بر اساس شواهد و اطلاعات موجود، اعتقاد بر این است که از سوی دشمن به‌ویژه رژیم صهیونیستی، احتمال قوی برای حمله به TT&C ایران پس از رهاسازی در جو زمین وجود دارد و این حمله می‌تواند منجر به صدور فرمان‌های اشتباه، سرقت و استراق سمع اطلاعات آنها، قطع ارتباط با مرکز زمینی، ارائه‌ی اطلاعات غلط و حتی آسیب‌های جدی سخت‌افزاری گردد.

صدور فرمان‌های اشتباه مرتبط با رکن فرمان، استراق سمع اطلاعات و قطع ارتباطات با مراکز زمینی مرتبط با رکن ارتباطات و ارائه‌ی اطلاعات غلط مرتبط با رکن اینتلیجنس در سیستم فرماندهی – کنترل است. از این رو بر اساس منطق فنی باید تهدیدات حاصل از حمله به ارکان کنترل و محاسبات را نیز در نظر گرفت.

## نمونه‌هایی از عملیات‌های مبتنی بر راهبرد اخلال در پرتاب علیه سامانه‌های موشکی سوریه

۱. پایگاه «دفاع و امنیت»[۲۳] ایتالیا در خبری تحلیلی با عنوان «سوریه هدف یک حمله‌ی سایبری قرار گرفته که به وسعت حمله‌ی موشکی است»[۲۴] بخشی از حملات سایبری به زیرساخت‌های حساس سوریه را بیان و تشریح نموده است. به گفته‌ی این پایگاه:

> **به‌نظر می‌رسد که سوریه، علاوه بر اقدامات بریتانیا، آمریکا و فرانسه [در حمله‌ی موشکی]، قربانی اقدامات سایبری نیز می‌باشد. برخی از عناصر نشان می‌دهد که مرکز گزارش‌دهی و کنترل دمشق هک شده است، به همین دلیل آژیر هشدار غلط نسبت به ورود موشک‌ها به محدوده‌ی پدافند موشکی سوریه انتشار یافته است. عملکرد این مرکز بدین‌گونه است که تمام اطلاعات مربوط به حفاظت از حریم هوایی ملی سوریه را دریافت می‌کند و آنها را به واحدهای مربوطه می‌فرستد.**[۲۵]

بر اساس خبر فوق، تلاش ائتلاف آمریکایی بر این بوده است تا مرکز فرماندهی – کنترل هشدار زودهنگام حملات هوایی و موشکی سوریه را توسط یک حمله‌ی سایبری مختل سازند تا در هنگام شلیک موشک به خاک دمشق، سیستم پدافند هوایی قادر به تشخیص و رهگیری موشک‌ها نباشد.

در ادامه‌ی خبر، در خصوص عاملان این حمله بیان شده است

> **اگر چه هنوز تأیید قطعی به‌دست نیامده است اما همه‌ی چشم‌ها بر ایالات متحده و اسرائیل قرار دارد، زیرا این دو کشور در حملات سایبری گذشته‌ی خود، موفق عمل کرده‌اند. کافی است که [سلاح سایبری] استاکس‌نت و ایران را به‌خاطر آورید!**

---

[23] Difesa e sicurezza

[24] Syria has probably undergone a cyber attack as well as an offensive with missiles

[25] https://www.difesaesicurezza.com/en/defence-and-security/syria-has-probably-undergone-a-cyber-attack-as-well-as-an-offensive-with-missiles/

۲. در خبر دیگری با عنوان «حمله‌ی سایبری آمریکا و اسرائیل علیه سیستم‌های دفاع موشکی»[۲۶] که خبرگزاری «تایمز آو اسرائیل»[۲۷] منتشر کرده، به نقل از یک افسر سوری در خصوص حملات سایبری اخیر به سوریه چنین عنوان شده است

**یکی از فرماندهان رژیم اذعان کرد متخصصان روسیه، پس از حادثه‌ی شب گذشته در حمص –که دلیل اصلی شلیک سیستم‌های دفاع موشکی بود– به سوریه کمک کردند. هشدار اشتباهی که پخش شد به علت «عملیات الکترونیک مشترک» آمریکا و اسرائیل علیه سیستم‌های دفاع موشکی سوریه بود که در نتیجه‌ی آن چند موشک نیز اشتباهاً شلیک شد.**[۲۸]

## چرا پدافند موشکی ایران، هواپیمای اوکراین را هدف قرار داد؟

بر اساس توضیحات ارائه شده، می‌توان صحنه‌ی نبرد را در وضعیت‌های شناسایی، پردازش، تشخیص و شلیک موشک از سوی سامانه‌ی پدافند موشکی ایران به هواپیمای مسافربری اوکراین را توصیف نمود.

هواپیمای مسافربری پس از برخاست از فرودگاه و افزایش ارتفاع تا ۸۰۰۰پا، در برد و شناسایی رادار سامانه‌ی پدافندی قرار گرفته و آشکار می‌شود.

همزمان اقدامات جنگ سایبری هواپیماهای ریوت جوینت در ایجاد شرایط «مِه» سایبری علیه بخش فرماندهی و کنترل سامانه‌ی پدافند موشکی (جنگ مِه یا Fog of War یکی از شاخه‌های جنگ سایبری است) باعث می‌شود سامانه در تشخیص هواپیما دچار فریب شده و آن را به‌عنوان **موشک کروز** به کاربر انسانی سامانه معرفی نماید.

از طرف دیگر به‌دلیل اقدام همزمان دشمن در جنگ سایبرنتیک برای ایجاد اختلال در بخش ارتباطی سامانه با سایر اجزای رینگ پدافندی، امکان کسب خبر کاربر انسانی سامانه از دیگر بخش‌ها میسر نبوده است. لذا کاربر انسانی با تشخیص و شناسایی موقعیت و جهت حرکت نزدیک‌شونده‌ی موشک به سمت سامانه و شهر تهران، و همچنین عدم دریافت دستور شلیک یا تأیید ماهیت پرنده‌ی شناسایی شده؛ اقدام به شلیک می‌نماید.

همچنین از آنجا که این سامانه، آخرین سامانه قبل از ورود موشک ثبت شده در رادار به شهر تهران بوده است، امکان خطر و عدم برخورد با آن به‌هیچ عنوان مهیا نبوده.

بر این اساس لازم به‌ذکر است در سانحه‌ی هواپیمای مسافربری هیچگونه خطای انسانی رخ نداده و خطای مذکور ناشی از بخش کامپیوتری سامانه است.

[26] Israel-US cyberattack triggered missile defenses

[27] The Times of Israel

[28] https://www.timesofisrael.com/syrian-officer-israel-us-cyberattack-triggered-missile-defenses/

## اخبار تکمیلی

در این خصوص اسناد و اخبار تکمیلی وجود دارد که از منظر فنی و اثبات اینکه عملیات سایبری برای فریب سیستم فرماندهی و کنترل سامانه پدافند موشکی ایران، از پیش طراحی و در دستور کار قرار گرفته است؛ بسیار حائز اهمیت می‌باشد.

اداره‌ی هوانوردی فدرال آمریکا، در یک بیانیه‌ی اضطراری مورخ ۸ژانویه ساعت ۰۰:٤ به وقت تهران، محدودیت اضطراری پرواز را بر فراز ایران به‌علت «امکان محاسبه‌ی اشتباه یا شناسایی اشتباه» سیستم‌های راداری در منطقه اعلام می‌دارد.[۲۹]

این در حالی است که وقوع سانحه در ساعت ۵:۱۵ به وقت تهران رخ داده است. لذا هشدار فوق یک هشدار پیشگیرانه است که حاکی از اطلاع سازمان هوانوردی آمریکا از اقدام جنگ سایبری ارتش این کشور بر فراز منطقه‌ی پروازی ایران می‌باشد.

از سوی دیگر بوریس جانسون، نخست‌وزیر بریتانیا در اظهار نظری پیرامون چگونگی رخداد سانحه‌ی هواپیمای مسافربری اوکراین، به موضوع جنگ مِه به‌عنوان محتمل‌ترین گزینه اشاره نموده است.[۳۰]

همچنین برخی از منابع خبری – تحلیلی انگلیسی زبان نیز به بررسی فنی احتمال جنگ مِه پرداخته و رخداد آن را تأیید کرده‌اند[۳۱]

حجت‌الاسلام والمسلمین سید ابراهیم رئیسی، رئیس قوه‌ی قضاییه در جلسه شورای عالی قضائی مورخ دوشنبه ۲۳ دی ۱۳۹۸ در خصوص نتایج تحقیقات علل وقوع این سانحه، ضمن اشاره به پیچیدگی علل رخداد آن تأکید نمود: «سازمان قضایی نیروهای مسلح لازم است از **کارشناسان سایبری** مشورت گرفته و نظرات آنها را مورد توجه قرار دهد.»[۳۲]

[29] https://www.washingtonpost.com/politics/faa-issues-emergency-restriction-for-persian-gulf-airspace-citing-potential-for-miscalculation-or-mis-identification/2020/01/07/44a2a440-31b7-11ea-971b-43bec3ff9860_story.html

[30] https://www.telegraph.co.uk/news/2020/01/09/crashed-iran-plane-trying-return-airport-initial-report-says/

[31] https://time.com/5762527/was-a-ukrainian-passenger-plane-lost-in-the-fog-of-war/

[۳۲] شبکه‌ی خبر صدا و سیمای جمهوری اسلامی ایران، ۲۳ دی ۱۳۹۸