ضرورت و الزامات تأسيس قرارگاه سايبري محور مقاومت

# فرمايشات مقام معظّم رهبري (حفظه‌الله)

1. «شما و اين حضرات نقش بي‌بديل رسانه و تبليغ را در پيكارهاي كنوني جهان-كه بيش از هميشه است- مي‌دانيد. امروز پيروزي يك طرف را توانايي او در گرفتن و رساندنِ پيام و روايت او از واقعيت رقم مي‌زند، بسيار پيش و بيش از آن‌كه ابزارهاي نظامي وارد ميدان شوند و در آن اثر بگذارند. ما در اين عرصه مهم بايد دقت و تلاش و ابتكار خود را مضاعف كنيم» (10/10/1403)
2. «امروز شما در دنيا اين را مي‌بينيد، قبل از دوران امام حسين (عليه السّلام) هم اين دوجبهه‌ وجود داشت، در زمان بعد از ايشان هم وجود داشته، امروز هم وجود دارد، تا آخر هم وجود خواهد داشت. در همه‌ي اينها «اِنّي سِلمٌ لِمَن سالَمَكم»؛ با هر كسي كه در جبهه‌ي شما است، من خوبم؛ «حَربٌ‌ لِمَن حارَبَكم‌»، با هر كسي كه با جبهه‌ي شما مي‌جنگد، مي‌جنگم. اين جنگ اَشكال مختلفي دارد: در دوران شمشير و نيزه يك جور است، در دوران اتم و هوش مصنوعي و امثال اينها يك جور ديگر است، ولي هست؛ در دوران تبليغات به وسيله‌ي شعر و قصيده و حديث و بيان كلمات يك جور است، در دوران اينترنت و كوانتوم و امثال اينها هم يك جور ديگر است، ولي هست… «حَربٌ‌ لِمَن‌ حارَبَكم» هميشه به معناي تفنگ به دست گرفتن نيست؛ به معناي درست انديشيدن، درست سخن گفتن، درست شناسايي كردن، دقيق به هدف زدن است؛ «حَربٌ‌ لِمَن حارَبَكم» اين‌جوري است. بدانيد وظيفه چيست، بشناسيد راهي را كه بايد بپيماييد.» (4/6/1403)
3. «اگر ما امروز در زمينه‌ي علوم شناختي و فنّاوري‌هاي شناختي تلاش نكنيم، كار نكنيم، حركت جدّي نكنيم -چون ديگران دارند [كار] ميكنند ديگر، با همه‌ي وجود دارند [تلاش] ميكنند؛ امروز مثلاً فرض كنيد ايشان نشان دادند كه در زمينه‌ي هوش مصنوعي مثلاً ما چهاردهم هستيم در دنيا- اگر چنانچه يك ذرّه غفلت كنيم و خوابمان ببرد، بسرعت سقوط خواهيم كرد و پنجاه سالِ ديگر خواهيم شد پنجاهم، خواهيم شد صدم، يعني دنيا از ما جلو مي‌افتد و ميرود. اين نكته‌ي مهمّي است و بايد همه به اين توجّه كنند؛ هم شما دانشمندان و محقّقين و پژوهشگران بايد به اين توجّه كنيد يعني شما ديگر شب و روز نبايد بشناسيد، هم مسئولين كشور و دولتي‌ها بايد توجّه كنند. اينكه بنده اين ‌همه روي مسئله علم تكيه ميكنم، به خاطر اين است» (3/11/1397)
4. «اوّلين مطلبي كه در باب سياست خارجي مي‌خواهم عرض بكنم اين است: در مقابل امواج و حوادث جهاني و بخصوص منطقه‌اي، برخورد كشور، برخورد فعّال باشد، برخورد اثرگذار باشد، نه برخورد منفعل. مسائل گوناگوني چه از لحاظ سياسي، چه از لحاظ علمي، چه از لحاظ پيشرفت‌ها و ابتكارات فوق‌العاده و عجيب علمي ــ فرض كنيد مثل هوش مصنوعي ــ در دنيا اتّفاق مي‌افتد؛ با اين، فعّال برخورد كنيد، منفعل برخورد نكنيد؛ اثرگذار برخورد كنيد. غفلت و تغافل از آنچه در دنيا پيش مي‌آيد، در منطقه پيش مي‌آيد، جايز نيست. هر حادثه‌اي پيش مي‌آيد، ما يك موضعي در قبال آن داريم؛ اين موضع را صريح، روشن، با قوّت و متانت ابراز كنيم تا دنيا بشناسد و بفهمد كه ايران اسلامي در اين قضيه چه ميگويد.» (7/5/1403)
5. «اين دانش‌هايي كه بشر كشف مي‌كند - حالا امروز علوم شناختي، كه اينها جزو كشفيات جديد بشر است؛‌ يك روزي مثلاً هفتاد هشتاد سال پيش، صد سال پيش، علومِ مربوط به اتم و كاركردهاي اتم و امثال اين‌ها - هر كدام از اينها يك دريچه‌اي است كه به روي انسان باز ميشود تا عالَم وجود را و هستي را كه صُنع الهي است بيشتر بشناسد؛ اين يك فتوح الهي است؛ اينها فتوحات الهيه است؛ ما بايستي از اين فتوح الهي استقبال كنيم،‌ استفاده كنيم. خداوند در قرآن ميگويد كه «وَ استَعمَرَكم فيها» شما را در روي اين زمين وادار كرده و از شما خواسته آباد كردنِ اين زمين را. آباد كردن زمين به معناي آباد كردن جسم بي‌جان نيست بلكه به معناي مجموعه‌ي آن چيزي است كه زمين حامل آن است كه عمده وجود انسان است. اين علوم -هم علومي كه امروز بتدريج دارد كشف ميشود، هم آنچه قبلاً كشف شده و هم آن چيزهايي كه بعدها كشف خواهد شد- ما را به اين «اِستَعمَرَكم فيها» نزديك ميكند.» (3/11/1397)
6. «هر ملّتي كه امروز در زمينه‌ي اين دانش‌هاي جديد…عقب بيفتد، سرنوشتش، سرنوشت آن ملّتهايي است كه در آغاز انقلاب صنعتي عقب افتادند و سرنوشتشان شد استعمارزدگي، شد زير دست بودن، شد فقير ماندن، شد ذليل شدن.» (3/11/1397)
7. «من پيشنهاد مي‌كنم يكي از مسائلي كه مورد تكيه و توجّه و تعميق واقع ميشود، مسئله هوش مصنوعي باشد كه در اداره‌ي آينده‌ي دنيا نقش خواهد داشت؛ حالا يا در معاونت علمي رئيس‌جمهور يا در دانشگاه بايد كاري كنيم كه ما در دنيا حدّاقل در [بين] ده كشور اوّل در مورد هوش مصنوعي قرار بگيريم كه امروز نيستيم؛ امروز كشورهايي كه درجه‌ي اوّل در مسئله هوش مصنوعي هستند، حالا غير از آمريكا و چين و مانند اينها كه در رده‌هاي بالا هستند، بعضي از كشورهاي آسيايي هم هستند، بعضي كشورهاي اروپايي هم هستند [امّا] ما نيستيم؛ البتّه كشورهاي آسيايي ظاهراً بيشتر هم هستند؛ در آن ده‌ رتبه‌ي اوّل، تعداد كشورهاي آسيايي بيشتر است. بايد كاري كنيم كه حدّاقل به ده كشور اوّل دنيا در اين مسئله برسيم.» (26/8/1400)
8. «علم خيلي مهم است: اَلعِلمُ سُلطان؛ علم به معناي واقعي كلمه قدرت است. اين شعرِ معروفِ «توانا بود هر كه دانا بود» حرف درستي است. «توانا بود هر كه دانا بود»؛ دانش براي يك كشور توانايي مي‌آورد، اقتدار مي‌آورد.» (28/11/1400)
9. «امروز هوش مصنوعي با يك شتاب حيرت‌دهنده‌اي [دارد پيش مي‌رود]؛ يعني انسان متحير ميشود از شتابي كه اين فنّاوري عجيب در دنيا پيدا كرده و دارد پيش ميرود… در مسئله هوش مصنوعي، بهره‌بردار بودن امتياز نيست؛ اين فنّاوري لايه‌هاي عميقي دارد كه بايد بر آن لايه‌ها مسلّط شد؛ آن لايه‌ها دست ديگران است. اگر شما نتوانيد لايه‌هاي عميق و متنوّع اين فنّاوري هوش مصنوعي را تأمين كنيد، فردا اينها يك ايستگاهي مثل آژانس اتمي درست مي‌كنند براي هوش مصنوعي - كه الان دارند مقدّماتش را فراهم ميكنند - كه اگر چنانچه به آن ايستگاه رسيديد، بايد اجازه بگيريد كه در فلان بخش از هوش مصنوعي استفاده كنيد، در فلان بخشِ ديگر حق نداريد استفاده كنيد! اين‌جوري است؛ زرنگ‌هاي دنيا، فرصت‌طلب‌ها و قدرت‌طلب‌هاي دنيا دنبال اين چيزها هستند.» (6/6/1403)
10. «ما بايد همان سه تحوّلي را كه امام در داخل كشور، در سطح امّت و در سطح جهان ايجاد كرد، تعقيب كنيم، دنبال كنيم، حفظ كنيم. دنبال كردن اين هدف امروز البتّه اقتضائاتي دارد كه با اقتضائات زمان امام فرق ميكند؛ اين را مي‌دانيم. مسلّماً در دوران هوش مصنوعي و كوانتوم و اينترنت و امثال اين پيشرفت‌هاي علمي، نميشود با همان شيوه‌هاي چهل سال قبل، دوران تلفن‌هاي كذايي و ضبط‌صوت‌هاي كذايي، با آن ابزارها امروز كار كرد. امروز براي پيشرفت اين هدف، ابزارها بايستي متناسب با زمان انتخاب بشود؛ ترديدي در اين نيست. ابزارها تغيير پيدا ميكند، امّا آنچه تغيير پيدا نميكند جبهه‌‌بندي‌ها است.» (14/3/1402)
11. «امروز انواع و اقسام شيوه‌هاي پراكندن پيام وجود دارد كه در گذشته حتّي فكرش را هم نميكردند؛ از تلويزيون و ماهواره بگيريد تا اينترنت و پسااينترنت؛ اين چيزهاي جديدي كه پيش آمده، هوش مصنوعي و امثال اينها. حالا چيزهاي ديگر هم در راه است. خب، با يك‌ چنين شرايطي، با يك‌ چنين وضعيتي كه در دست دشمن شمشيرهاي آخته‌ي برّانِ خون‌ريز وجود دارد، ما چه ‌كار ميخواهيم بكنيم؟ تبليغ، اينجا اهمّيتِ مضاعف پيدا ميكند. امروز، هم سخت‌افزارهاي مخالف، معارض و معاند تطوّر پيدا كرده، پيشرفت پيدا كرده كه اشاره كردم، هم نرم‌افزارها؛ شيوه‌هاي باورپذير كردن پيام را - چيز‌هايي كه در گذشته، هيچ كس بلد نبود - با پشتيباني علمي روانشناسي و امثال اينها رايج كردند؛ اينها ابزارهاي نرم‌افزاري است، اينها خيلي مهم است.» (21/2/1402)
12. «امروز فضاي مجازي در زندگي مردم، ديگر مثل پنج سال پيش و ده سال پيش نيست؛ گسترش فضاي مجازي يك گسترش بسيار وسيع و عظيمي است. خب، اين فضاي مجازي منافعي دارد، امكاناتي دارد، خطراتي هم دارد، خطرات بزرگي هم دارد. اگر چنانچه اين فضا ناامن باشد براي مردم، ضررش را مردم مي‌بَرند… ما بيشتر از خيلي از كشورها، دشمن داريم؛ دشمن هم راه‌هاي نفوذ را پيدا ميكند و يكي از راه‌هاي نفوذ، همين مسئله فضاي مجازي است. شما هم ميتوانيد نقش ايفا كنيد، نقش مهمّي ميتوانيد ايفا كنيد؛ در اين مسئله به ‌طور كامل، به صورت جدّي وارد بشويد.» (8/2/1398)
13. «امروز هم فضاي مجازي يك صحراي بي‌پاياني است كه از همه طرفش ميشود حركت كرد؛ ديگر مثل سابق نيست كه شما بخواهيد يك مطلبي را بيان كنيد، ناچار باشيد روي كاغذ بنويسيد، آن را پلي‌كپي كنيد يا فتوكپي كنيد ده نسخه، صد نسخه، دويست نسخه؛ اين‌جوري نيست. هر يك نفري كه بتواند با رايانه كار بكند يك رسانه است. مي‌نشينند پخش ميكنند شبهات را، حرفها را، جوانهاي مؤمن را، جوانهاي سالم را گمراه ميكنند. اينها را بايد شناخت. چه كسي بايستي بيايد وسط ميدان و سينه سپر كند و مانع بشود از گمراهي جوانان؟ چه كسي بايد مانع بشود از اقدام دشمن براي انحراف ذهن جوانان؟ به عهده‌ي چه كسي است اين كار؟» (16/6/1395)
14. «الان واقعاً فضاي مجازي، يك بخش حقيقي از زندگي مردم شده؛ حالا دولت الكترونيك و از اين قبيل كه به جاي خود محفوظ است- شكي نيست [امّا] آنچه عرضِ من است و من روي آن تكيه ميكنم اين است كه فضاي مجازي بدون اختيار ما، از بيرون از اختيارِ ما دارد مديريت ميشود؛ بحث اين است. فضاي مجازي يك چيزي نيست كه آدم بتواند مثل يك آب رواني هر جور كه ميخواهد از آن استفاده بكند؛ ديگران دارند اين آب را به يك سمتي كه خودشان ميخواهند هدايت ميكنند؛ آن‌ها دارند مديريت ميكنند اين فضا را. خب وقتي كه ما ميدانيم كساني از بيرون دارند فضاي مجازي را -كه ما هم دست‌اندركارش هستيم و مبتلابهِ ما است- هدايت ميكنند و مديريت ميكنند، ما نميتوانيم بي‌كار بنشينيم در مقابل او؛ ما نميتوانيم مردممان را كه با فضاي مجازي ارتباط دارند، بي‌پناه رها كنيم در اختيار آن مديري كه دارد پشت پرده، فضاي مجازي را اداره ميكند. عوامل مسلّط بين‌المللي در اين زمينه‌ها بشدّت فعّالند: از لحاظ خبردهي، خبررساني، تحليل داده‌ها و امثال گوناگون؛ هزاران كار دارد انجام ميگيرد روي فضاي مجازي.» (2/6/1399)

# مطالبات مقام معظّم رهبري (حفظه‌الله)

1. استفاده از پيشرفت‌هاي علمي و آخرين دستاوردهاي بشري
   1. دستيابي به توانايي و اقتدار با پيشرفت علم و فناوري
   2. جلوگيري از استعمارزدگي و فقر و ذلت به‌وسيله پيشرفت در دانش‌هاي جديد
   3. استقبال از دانش‌هاي بشري به عنوان فتوحات الهيه براي آباد كردن زمين
   4. تغيير و تحوّل روش مبارزه و جهاد متناسب با زمان و پيشرفت‌هاي فناوري
   5. سقوط در صورت فقدان حركت جدّي در زمينه علوم و فناوري‌هاي جديد
2. اهتمام به مديريت فضاي مجازي و پيام‌رساني
   1. پيروزي در گروي توانمندي گرفتن و رساندن پيام و روايت از واقعيت
   2. جلوگيري از نفوذ دشمن از طريق فضاي مجازي
   3. اهميّت مضاعف تبليغ از طريق اينترنت و ابزارهاي نرم‌افزاري پيشرفته
   4. شناخت فضاي مجازي به‌مثابه يك صحراي بي‌پايان براي حركت و فعاليت
   5. تبديل شدن آحاد مردم به رسانه؛ هر يك نفر كه بتواند با رايانه كار كند
3. تسلّط بر لايه‌هاي عميق هوش مصنوعي
   1. تغيير شكل جنگ بين دو جبهه حق و باطل با پيدايش هوش مصنوعي
   2. تكيه و توجه به نقش هوش مصنوعي در اداره آينده دنيا
   3. تسريع در مسلّط شدن بر هوش مصنوعي با توجه به شتاب حيرت‌آور پيشرفت آن
   4. استفاده از هوش مصنوعي به‌عنوان فناوري جديد براي پراكندن پيام
   5. برخورد و مواجهه فعّال، اثرگذار و غيرمنفعل با پيشرفت‌هاي هوش مصنوعي

# اهميّت فضاي مجازي

## آسيب‌ها و مخاطرات

فضاي مجازي به عنوان يك ابزار پرقدرت و گسترده، امروزه تأثير زيادي بر زندگي روزمره افراد دارد. با اين حال، استفاده از آن با برخي آسيب‌ها و مخاطرات همراه است كه بايد به آن‌ها توجه كرد. اين آسيب‌ها مي‌توانند به جنبه‌هاي مختلف زندگي فردي، اجتماعي، سياسي، فرهنگي و اقتصادي آسيب وارد كنند. در زير به برخي از اين آسيب‌ها و مخاطرات اشاره مي‌كنيم:

### تهديدات امنيتي

سرقت اطلاعات: هكرها مي‌توانند با استفاده از ابزارهاي مختلف به اطلاعات محرمانه دسترسي پيدا كرده و آن‌ها را براي مقاصد سوء مختلف به كار ببرند.

حملات فيشينگ: در اين حملات، كلاهبرداران تلاش مي‌كنند اطلاعات حساس مانند كلمات عبور، شماره كارت بانكي و اطلاعات حساس ديگر را از طريق ايميل‌ها يا وب‌سايت‌هاي جعلي به دست آورند.

نشت اطلاعات: اطلاعات كاربران در پلتفرم‌هاي مختلف به راحتي مي‌تواند نشت كرده و در دسترس افراد غيرمجاز قرار گيرد.

### تهديدات جسمي و رواني

استرس و اضطراب: اعتماد به اخبار شبكه‌هاي اجتماعي مي‌تواند منجر به استرس و اضطراب در افراد شود. فريب خوردن از تصاوير و محتواي غيرواقعي مي‌تواند به اضطراب و افسردگي دامن بزند.

توهين، تهديد و آزار اينترنتي: در فضاي مجازي، افراد مي‌توانند به راحتي ديگران را مورد آزار و اذيت قرار دهند. اين نوع تهديدات مي‌تواند افراد را وادار به همكاري با دشمن نمايد.

موضع‌گيري نادرست: حجم اطلاعات غلط وقتي به‌صورت منسجم و برنامه‌ريزي شده يك فرد يا گروه را هدف قرار دهد، بر رفتار و مواضع سياسي و اجتماعي آن‌ها تأثير مي‌گذارد.

بيماري: اطلاعات غلط درباره مسائل پزشكي و سلامت در فضاي مجازي به راحتي گسترش مي‌يابد. افراد ممكن است به اشتباه اطلاعات نادرستي را در مورد داروها، روش‌هاي درماني يا پيشگيري از بيماري‌ها بپذيرند كه مي‌تواند به ضرر سلامت‌شان باشد.

خودآزاري: انتشار تصاوير يا اطلاعات شخصي افراد و يا تهديد در اين زمينه مي‌تواند منجر به خودكشي فرد يا آزار رساندن به خود شود.

### تأثيرات منفي بر روابط اجتماعي

انزوا: ارتباطات مجازي نمي‌توانند جايگزين كامل روابط چهره به چهره باشند و استفاده بيش از حد از فضاي مجازي مي‌تواند منجر به كاهش تعاملات اجتماعي واقعي شود. افراد ممكن است در معرض انزواي اجتماعي قرار گيرند و مهارت‌هاي ارتباطي و انساني خود را از دست بدهند.

بي‌اعتمادي: جبهه خودي نياز به همبستگي و اتحاد دارد و اين جز از طريق اعتمادسازي حاصل نمي‌شود. فضاي مجازي با جداسازي فرد و ايجاد تنهايي صوري و ايجاد شك و ترديد، اعتماد را از بين برده و تعامل را دشوار مي‌كند.

ترس: جدا شدن دروني فرد از محيط واقعي خارج، احساسي كه اگر چه واقعي نيست، ولي به‌صورت ذهني و رواني فرد را تنها مي‌كند، استقلالي بدون حمايت اطرافيان؛ خانواده و دوستان، در افراد ترس ايجاد مي‌كند و دشمن مي‌تواند از اين ترس توهّمي براي مسلّط شدن بر فرد استفاده كند.

شايعات: در فضاي مجازي، شايعات و تبليغات فريبنده مي‌توانند به سرعت منتشر شوند. اين شايعات مي‌توانند به راحتي باور افراد را تغيير دهند و حتي باعث ايجاد بحران‌هاي اجتماعي شوند.

### تهديدات مالي و اقتصادي

كلاهبرداري‌هاي آنلاين: كلاهبرداران از روش‌هاي مختلفي مانند فروش كالاهاي جعلي يا خدمات بي‌كيفيت، ايجاد سايت‌هاي تقلبي يا ارسال ايميل‌هاي فيشينگ، اقدام به كلاهبرداري از كاربران مي‌كنند.

هك حساب‌هاي بانكي و مالي: با سوءاستفاده از اطلاعات شخصي افراد، هكرها مي‌توانند به حساب‌هاي بانكي يا مالي افراد دسترسي پيدا كرده و آن‌ها را به سرقت برند.

فروش كالاي هدفمند: با ايجاد فروشگاه‌ها و روابط ساختگي و مصنوعي مي‌توانند فرد يا گروهي را وادار به خريد كالايي كنند كه اصالت ندارد و مي‌تواند كاربرد جاسوسي يا تخريب داشته باشد.

## فرصت‌ها و قابليت‌ها

فضاي مجازي با وجود آسيب‌ها و مخاطرات زيادي كه ممكن است به همراه داشته باشد، فرصت‌ها و قابليت‌هاي قابل توجهي را نيز براي افراد و جوامع فراهم كرده است. اين فضا به ويژه در عصر ديجيتال امروزي نقش اساسي در تحول‌هاي اجتماعي، اقتصادي و فرهنگي ايفا مي‌كند. در اينجا به برخي از مهم‌ترين فرصت‌ها و قابليت‌هاي فضاي مجازي اشاره مي‌كنيم:

### دسترسي به اطلاعات و آموزش

آموزش آنلاين: فضاي مجازي اين امكان را به افراد مي‌دهد تا به دوره‌هاي آموزشي آنلاين، وبينارها و منابع آموزشي دسترسي داشته باشند. اين دسترسي به دانش و اطلاعات در هر زمان و مكاني، موجب افزايش فرصت‌هاي يادگيري و بهبود مهارت‌ها براي افراد در سطوح مختلف اجتماعي و حرفه‌اي مي‌شود.

دسترسي به اطلاعات عمومي و تخصصي: از طريق اينترنت، افراد مي‌توانند به منابع علمي و خبري متنوع دسترسي پيدا كنند و از آخرين اخبار و اطلاعات در حوزه‌هاي مختلف آگاه شوند.

### ارتباطات و شبكه‌سازي

ارتباط آسان با ديگران: فضاي مجازي اين امكان را براي افراد فراهم مي‌آورد كه با افراد در سراسر جهان ارتباط برقرار كنند. اين امر باعث تسهيل در تعاملات اجتماعي، تبادل فرهنگي و ايجاد روابط شخصي و حرفه‌اي مي‌شود.

شبكه‌هاي اجتماعي: افراد مي‌توانند از شبكه‌هاي اجتماعي و پيام‌رسان‌هاي رايج براي برقراري ارتباط با دوستان، همكاران، خانواده و حتي كساني كه از نظر جغرافيايي دور هستند، استفاده كنند.

### فرصت‌هاي كسب‌وكار و تجارت الكترونيك

بازارهاي آنلاين: فضاي مجازي به كسب‌وكارها اين امكان را مي‌دهد كه محصولات و خدمات خود را در بازارهاي جهاني عرضه كنند. اين امر به ويژه براي كسب‌وكارهاي كوچك و متوسط كه امكان فروش در بازارهاي فيزيكي را ندارند، فرصت‌هاي جديدي ايجاد مي‌كند.

تجارت الكترونيك و فروش آنلاين: فروشگاه‌هاي آنلاين، خدمات پرداخت آنلاين و اپليكيشن‌هاي خريد و فروش، امكان خريد و فروش كالاها و خدمات را از هر نقطه‌اي در دنيا فراهم كرده‌اند.

تبليغات ديجيتال: كسب‌وكارهاي كوچك و بزرگ مي‌توانند از تبليغات آنلاين براي جذب مشتريان جديد و ارتقاي برند خود استفاده كنند.

### توسعه فرهنگي و هنري

پلتفرم‌هاي اشتراك محتوا: هنرمندان، نويسندگان، فيلم‌سازان و توليدكنندگان محتوا مي‌توانند آثار خود را از طريق پلتفرم‌هاي اختصاصي فيلم و تصوير به مخاطبان جهاني عرضه كنند.

دسترسي به آثار فرهنگي و هنري: افراد مي‌توانند به راحتي به آثار هنري و فرهنگي از سراسر جهان دسترسي پيدا كنند. اين دسترسي باعث گسترش تبادل فرهنگي و آگاهي‌هاي هنري ميان اقوام و ملت‌هاي مختلف مي‌شود.

همكاري‌هاي آنلاين: هنرمندان و توليدكنندگان محتوا مي‌توانند از فضاي مجازي براي همكاري‌هاي بين‌المللي استفاده كنند و پروژه‌هاي مشترك ايجاد كنند.

### توانمندسازي و فعال‌سازي اجتماعي

حمايت از حقوق بشر و گروه‌هاي كم‌برخوردار: فضاي مجازي ابزار قدرتمندي براي فعالان حقوق بشر، گروه‌هاي مدني و سازمان‌هاي غيرانتفاعي است تا اطلاعات و مطالب مربوط به حقوق انسان‌ها را منتشر كرده و پويش‌هاي آگاهي‌بخشي راه‌اندازي كنند.

توانمندسازي افراد: افراد در فضاي مجازي مي‌توانند به گروه‌هاي مختلف با اهداف مشابه بپيوندند، ايده‌ها و پروژه‌هاي خود را به اشتراك بگذارند و از حمايت‌هاي اجتماعي و مشاوره‌اي بهره‌مند شوند.

### توسعه فناوري و نوآوري

پشتيباني از نوآوري‌ها و شركت‌هاي دانش‌بنيان: فضاي مجازي بستري مناسب براي استارتاپ‌ها و شركت‌هاي نوپا است تا ايده‌هاي نوآورانه خود را معرفي كرده و به جذب سرمايه‌گذاران و مشتريان جديد بپردازند.

انتقال فناوري و دانش: فضاي مجازي امكان تبادل سريع و آسان دانش و فناوري‌هاي نوين بين دانشگاه‌ها، مراكز تحقيقاتي و صنايع را فراهم مي‌آورد.

### سلامت و پزشكي

دوركاري و مشاوره آنلاين: پزشكان و مشاوران مي‌توانند از طريق فضاي مجازي به بيماران خود مشاوره بدهند و حتي برخي از خدمات درماني از راه دور ارائه كنند. اين امر به ويژه در شرايط بحران‌ها مانند پاندمي‌ها بسيار مفيد واقع شده است.

اطلاعات بهداشتي و آموزش سلامت: افراد مي‌توانند از طريق فضاي مجازي به منابع معتبر پزشكي، مقالات علمي و اطلاعات بهداشتي دسترسي پيدا كرده و به ارتقاي سلامتي خود كمك كنند.

### حكمراني و سياست

آگاهي‌سازي سياسي و اجتماعي: فضاي مجازي به شهروندان اين امكان را مي‌دهد تا از مسائل سياسي و اجتماعي آگاه شوند، در بحث‌ها و تصميم‌گيري‌هاي عمومي شركت كنند و خواسته‌هاي خود را به مقامات منتقل كنند.

تأثيرگذاري سياسي: فضاي مجازي مي‌تواند به عنوان ابزار قدرتمندي براي برگزاري انتخابات آنلاين، نظرسنجي‌هاي عمومي و مشاركت مردم در فرآيندهاي حكمراني استفاده شود، به‌نحوي كه تغييراتي را در عملكرد دولت‌ها پديد آورند.

### تسهيل در فعاليت‌هاي روزمره

دولت الكترونيك: از طريق دولت الكترونيك، افراد مي‌توانند خدمات مختلفي از جمله: ثبت‌نام، پرداخت ماليات، درخواست گواهي‌نامه و بسياري ديگر از خدمات دولتي را آنلاين دريافت كنند.

مديريت زمان و برنامه‌ريزي: اپليكيشن‌ها و ابزارهاي مختلف در فضاي مجازي به افراد كمك مي‌كنند تا زمان خود را بهتر مديريت كنند، برنامه‌هاي روزانه و هفتگي خود را تنظيم كنند و بهره‌وري بيشتري داشته باشند.

# اهميّت هوش مصنوعي

## آسيب‌ها و مخاطرات

هوش مصنوعي (هومَص) يكي از بزرگ‌ترين دستاوردهاي علمي و فناوري در قرن اخير است كه به سرعت در حال توسعه و گسترش است. اما مانند هر فناوري ديگري، استفاده از آن مي‌تواند با آسيب‌ها و مخاطراتي همراه باشد كه بايد به دقت مورد بررسي قرار گيرد. در زير به برخي از اين آسيب‌ها و مخاطرات اشاره مي‌كنيم:

### تهديدات امنيتي و سوءاستفاده از هوش مصنوعي

هك و دستكاري: استفاده از هوش مصنوعي در زمينه‌هايي مانند سيستم‌هاي امنيتي، خودروهاي خودران و زيرساخت‌هاي حياتي مي‌تواند آسيب‌پذيري‌هايي ايجاد كند كه در صورت هك شدن، به طور جدي تهديداتي براي امنيت عمومي ايجاد كند.

حملات سايبري: هكرها مي‌توانند از هوش مصنوعي براي ايجاد حملات پيچيده‌تر و هدفمندتر استفاده كنند. به عنوان مثال، حملات فيشينگ يا مهندسي اجتماعي مي‌توانند با استفاده از يادگيري ماشين، بسيار واقعي‌تر و متقاعدكننده‌تر شوند.

ربات‌هاي خودكار و تسليحات هوشمند: استفاده از هوش مصنوعي در زمينه تسليحات مي‌تواند خطرات جديدي ايجاد كند. ربات‌ها و سيستم‌هاي تسليحاتي كه به صورت خودكار عمل مي‌كنند، در صورتي كه تحت كنترل نباشند، مي‌توانند منجر به تخريب بيشتري شوند.

### مسائل اجتماعي و اقتصادي

از دست دادن شغل‌ها و بيكاري: يكي از بزرگ‌ترين تهديدات اقتصادي كه هوش مصنوعي به همراه دارد، از دست رفتن شغل‌هاست. سيستم‌هاي هوش مصنوعي قادرند بسياري از كارهاي تكراري و دستي را جايگزين انسان‌ها كنند، كه اين موضوع ممكن است منجر به بيكاري گسترده در برخي صنايع شود.

نابرابري‌هاي اقتصادي: استفاده ناعادلانه از هوش مصنوعي ممكن است باعث ايجاد شكاف‌هاي بزرگتر بين افراد و كشورهاي ثروتمند و فقير شود. شركت‌هايي كه به فناوري‌هاي پيشرفته دسترسي دارند، مي‌توانند بهره‌وري خود را افزايش دهند، در حالي كه كشورهاي يا شركت‌هاي كمتر پيشرفته ممكن است از رقابت عقب بمانند.

تمركز قدرت: هوش مصنوعي مي‌تواند موجب تمركز قدرت در دست تعداد كمي از شركت‌ها و دولت‌ها شود. به عنوان مثال، شركت‌هاي بزرگ فناوري كه در زمينه هومَص پيشرفت كرده‌اند، مي‌توانند با استفاده از داده‌هاي كاربران، كنترل زيادي بر روي اطلاعات و تصميمات اقتصادي و اجتماعي مردم داشته باشند.

### مسائل اخلاقي و انساني

پذيرش خودكار تصميمات: بسياري از سيستم‌هاي هوش مصنوعي براي تصميم‌گيري‌ها استفاده مي‌شوند، مانند سيستم‌هاي قضاوت در عدالت كيفري يا تصميمات پزشكي. اين موضوع مي‌تواند باعث بروز مشكلات اخلاقي شود، زيرا سيستم‌هاي هوش مصنوعي ممكن است تحت تأثير داده‌هاي ناقص يا نادرست قرار بگيرند يا نتايج غيرانساني به دنبال داشته باشند.

سوگيري و تبعيض: يكي از مشكلات رايج در سيستم‌هاي هوش مصنوعي، سوگيري (bias) است. اگر داده‌هايي كه به سيستم‌هاي هومَص وارد مي‌شوند داراي تبعيض باشند (مثلاً از نظر نژادي، جنسيتي يا اقتصادي)، اين سوگيري‌ها مي‌توانند به تصميم‌گيري‌هاي نادرست يا غيرمنصفانه منجر شوند.

از دست رفتن كنترل انساني: به طور خاص در سيستم‌هاي پيچيده‌تر، مانند ربات‌هاي خودمختار يا سيستم‌هاي هوش مصنوعي پيشرفته، ممكن است انسان‌ها نتوانند به طور كامل بر روي تصميمات و عملكرد اين سيستم‌ها نظارت داشته باشند. اين امر مي‌تواند منجر به خطراتي در مواقع بحراني شود.

### مسائل حريم خصوصي و جمع‌آوري داده‌ها

نظارت و حريم خصوصي: هوش مصنوعي مي‌تواند براي جمع‌آوري و تحليل داده‌هاي شخصي از افراد استفاده شود. اين امر ممكن است منجر به نقض حريم خصوصي افراد و استفاده نادرست از اطلاعات شخصي شود.

سرقت داده‌ها: اطلاعات جمع‌آوري‌شده توسط سيستم‌هاي هوش مصنوعي، اگر به دست هكرها يا افراد نادرست بيفتد، مي‌تواند مورد سوءاستفاده قرار گيرد. اين امر مي‌تواند تهديدات امنيتي جدي به همراه داشته باشد.

### اتكاي بيش از حد به هوش مصنوعي

اعتماد: در برخي از حوزه‌ها، مانند پزشكي، افراد و حتي متخصصان ممكن است بيش از حد به سيستم‌هاي هومَص اعتماد كنند و نتيجه‌گيري‌ها يا تشخيص‌هاي غلط آن‌ها را به راحتي بپذيرند. اين مي‌تواند خطرات جدي در زمينه سلامت و تصميم‌گيري‌هاي حياتي ايجاد كند.

توانايي‌هاي محدود هوش مصنوعي: بسياري از سيستم‌هاي هوش مصنوعي هنوز به سطحي از تكامل نرسيده‌اند كه قادر به درك كامل و تصميم‌گيري منطقي در شرايط پيچيده انساني باشند. اتكا به اين سيستم‌ها در موارد پيچيده مي‌تواند منجر به اشتباهات بزرگي شود.

### آسيب به هويت و استقلال انساني

تهديد به هويت انسان: در صورتي كه هوش مصنوعي پيشرفت كند و به جايي برسد كه قادر به انجام بسياري از فعاليت‌ها و وظايف انساني باشد، ممكن است سوالاتي درباره هويت و نقش انسان در جامعه مطرح شود.

كاهش استقلال فردي: در برخي موارد، مردم ممكن است تحت تأثير الگوريتم‌ها و سيستم‌هاي هوش مصنوعي قرار بگيرند. به عنوان مثال، سيستم‌هاي توصيه‌گر (مانند آنچه در شبكه‌هاي اجتماعي يا فروشگاه‌هاي آنلاين مشاهده مي‌شود) مي‌توانند انتخاب‌هاي افراد را تحت تأثير قرار داده و به نوعي به دستكاري رفتارهاي آن‌ها منجر شوند.

تأثير بر تصميم‌گيري‌هاي فردي و اجتماعي: هوش مصنوعي مي‌تواند به گونه‌اي عمل كند كه تصميمات افراد يا جوامع را به نفع يك ديدگاه خاص هدايت كند. اين مي‌تواند شامل تبليغات هدفمند، اخبار و محتواي تحريف‌شده باشد كه ممكن است باورها و رفتارهاي افراد را دستكاري كند.

## فرصت‌ها و قابليت‌ها

هوش مصنوعي يكي از بزرگ‌ترين پيشرفت‌هاي علمي و فناوري است كه توانسته‌ است تحولاتي عظيم در بسياري از حوزه‌ها ايجاد كند. در زير به برخي از مهم‌ترين فرصت‌ها و قابليت‌هاي هوش مصنوعي اشاره مي‌كنيم:

### آموزش و يادگيري هوشمند

آموزش شخصي‌شده: هوش مصنوعي مي‌تواند فرآيند آموزش را براي هر دانش‌آموز يا دانشجو به صورت شخصي‌شده و مطابق با نيازهاي فردي طراحي كند. سيستم‌هاي هومَص مي‌توانند نقاط قوت و ضعف يادگيرندگان را شناسايي كرده و محتوا و روش‌هاي تدريس را بر اساس نيازهاي آن‌ها تنظيم كنند.

يادگيري خودكار (Machine Learning): هوش مصنوعي از طريق يادگيري خودكار قادر است مهارت‌ها و مفاهيم جديد را به مرور زمان ياد بگيرد و براي بهبود عملكرد خود از تجربه‌هاي گذشته استفاده كند.

دسترس‌پذيري آموزش: استفاده از AI مي‌تواند به دسترس‌پذيري آموزش در سطح جهاني كمك كند. پلتفرم‌هاي آموزش آنلاين مبتني بر هوش مصنوعي مي‌توانند به افراد از هر نقطه جهان اين امكان را بدهند كه به منابع آموزشي با كيفيت دسترسي پيدا كنند.

### تحقيق و توسعه (R&D)

نوآوري‌هاي علمي: هوش مصنوعي مي‌تواند به شتاب‌دهي فرآيند تحقيق و توسعه كمك كند. با استفاده از AI، پژوهشگران مي‌توانند داده‌هاي آزمايشگاهي را سريع‌تر تحليل كنند و كشف‌هاي علمي جديد را تسريع كنند.

مدل‌سازي و شبيه‌سازي: هوش مصنوعي مي‌تواند در شبيه‌سازي و مدل‌سازي پيچيده مسائل علمي كمك كند.

### امنيت و دفاع

شناسايي تهديدات امنيتي: سيستم‌هاي هوش مصنوعي قادرند الگوهاي رفتاري در شبكه‌هاي كامپيوتري و داده‌ها را شناسايي كنند و از حملات سايبري جلوگيري كنند. اين امر مي‌تواند به افزايش امنيت كمك كند.

دفاع خودكار: در برخي از موارد، AI مي‌تواند به سيستم‌هاي دفاعي كمك كند تا به صورت خودكار تهديدات را شناسايي كرده و پاسخ دهند، بدون نياز به دخالت انساني.

### حمل‌ونقل و خودروهاي خودران

خودروهاي خودران: يكي از بزرگ‌ترين پيشرفت‌ها در حوزه حمل‌ونقل، توسعه خودروهاي خودران است كه توسط هوش مصنوعي كنترل مي‌شوند. اين خودروها قادرند به صورت خودكار حركت كنند، موانع را شناسايي كنند و با ديگر خودروها و شرايط ترافيكي تعامل داشته باشند.

حمل‌ونقل هوشمند: سيستم‌هاي حمل‌ونقل مبتني بر هوش مصنوعي مي‌توانند جريان ترافيك را بهينه كنند و به رانندگان كمك كنند تا مسيرهاي سريع‌تر و كم‌ترافيك‌تر را انتخاب كنند. اين مي‌تواند به كاهش آلودگي و بهبود كيفيت زندگي در شهرهاي شلوغ منجر شود.

### پيشرفت در حوزه هنر و رسانه

توليد محتوا: هوش مصنوعي مي‌تواند در توليد محتواهاي هنري مانند موسيقي، نقاشي و نويسندگي كمك كند. ابزارهاي مبتني بر AI مي‌توانند به هنرمندان و توليدكنندگان محتوا ايده‌هاي جديد بدهند يا حتي آثار هنري كامل را توليد كنند.

تجزيه و تحليل محتواي رسانه‌اي: سيستم‌هاي هوش مصنوعي مي‌توانند به طور خودكار محتواي ويديويي، تصويري و متني را تحليل كرده و آن را دسته‌بندي كنند. اين فناوري مي‌تواند به توليدكنندگان محتوا و پلتفرم‌هاي رسانه‌اي كمك كند تا تجربه بهتري براي مخاطبان خود ايجاد كنند.

### تحول در حوزه‌هاي پزشكي و سلامت

تشخيص بيماري‌ها: هوش مصنوعي مي‌تواند به دقت بالاتري در شناسايي بيماري‌ها كمك كند. به عنوان مثال، سيستم‌هاي مبتني بر AI قادرند تصاوير پزشكي مانند سي‌تي‌اسكن‌ها و اشعه ايكس را تحليل كرده و بيماري‌هايي مانند سرطان، بيماري‌هاي قلبي و مغزي را در مراحل اوليه شناسايي كنند.

پزشكي شخصي‌شده: هوش مصنوعي مي‌تواند به ارائه درمان‌هاي شخصي‌شده و دقيق‌تر كمك كند. با تحليل داده‌هاي ژنتيكي و پزشكي هر فرد، AI مي‌تواند درمان‌هاي مناسب و توصيه‌هاي پزشكي را بر اساس ويژگي‌هاي خاص فرد ارائه دهد.

### ارتقاي بهره‌وري در صنايع

اتوماسيون فرآيندها: هوش مصنوعي مي‌تواند بسياري از فرآيندهاي تكراري و زمان‌بر در صنايع مختلف را اتوماسيون كرده و به كاهش هزينه‌ها و افزايش سرعت توليد كمك كند. به عنوان مثال، در صنعت توليد، ربات‌ها و سيستم‌هاي هومَص مي‌توانند وظايفي مانند مونتاژ قطعات، كنترل كيفيت و بسته‌بندي را به طور خودكار انجام دهند.

تحليل داده‌ها و پيش‌بيني‌ها: هوش مصنوعي مي‌تواند از داده‌هاي عظيم (Big Data) براي پيش‌بيني روندهاي بازار، رفتار مشتريان و ارزيابي عملكرد كسب‌وكار استفاده كند. اين پيش‌بيني‌ها مي‌توانند به تصميم‌گيري‌هاي بهتر و استراتژي‌هاي تجاري مؤثرتر منجر شوند.

بهبود تجربه مشتري: با استفاده از AI در چت‌بات‌ها، سيستم‌هاي توصيه‌گر (Recommendation Systems) و تحليل رفتار مشتري، كسب‌وكارها مي‌توانند تجربه بهتري را براي مشتريان خود ايجاد كنند. به عنوان مثال، سيستم‌هاي هوش مصنوعي در فروشگاه‌هاي آنلاين مي‌توانند محصولات مرتبط با ترجيحات مشتري را پيشنهاد دهند.

### تحول در صنعت خدمات مالي و بانكداري

پردازش و تحليل داده‌هاي مالي: هوش مصنوعي قادر است حجم عظيمي از داده‌هاي مالي را در زمان كوتاه تحليل كرده و پيش‌بيني‌هاي دقيق‌تري از روند بازار ارائه دهد. اين مي‌تواند به سرمايه‌گذاران و مديران مالي كمك كند تا تصميمات بهتري بگيرند.

كاهش تقلب و سرقت هويتي: سيستم‌هاي مبتني بر AI مي‌توانند به شناسايي الگوهاي غيرعادي و اقدامات مشكوك در تراكنش‌هاي مالي كمك كنند. اين فناوري به بانك‌ها و موسسات مالي اين امكان را مي‌دهد كه از تقلب و سرقت‌هاي هويتي جلوگيري كنند.

خدمات مشتري هوشمند: چت‌بات‌ها و دستيارهاي ديجيتال مبتني بر AI مي‌توانند به مشتريان در انجام تراكنش‌هاي مالي، پاسخ به سوالات و حل مشكلات به صورت سريع و ۲۴ ساعته كمك كنند.

### مديريت منابع طبيعي و محيط زيست

مديريت منابع آب و انرژي: هوش مصنوعي مي‌تواند در مديريت منابع طبيعي مانند آب و انرژي به طور مؤثري عمل كند. به عنوان مثال، سيستم‌هاي هوش مصنوعي مي‌توانند مصرف انرژي را بهينه كرده و از اتلاف آن جلوگيري كنند. همچنين مي‌توانند به پيش‌بيني و مديريت بحران‌هاي مربوط به منابع آبي كمك كنند.

پيش‌بيني تغييرات اقليمي: با استفاده از مدل‌هاي پيشرفته AI، دانشمندان قادرند تغييرات اقليمي را شبيه‌سازي و پيش‌بيني كنند. اين پيش‌بيني‌ها مي‌توانند به سياست‌گذاران و سازمان‌ها كمك كنند تا تصميمات بهتري براي مقابله با بحران‌هاي محيطي اتخاذ كنند.

### پيشرفت در كشاورزي

كشاورزي هوشمند: استفاده از هوش مصنوعي در كشاورزي مي‌تواند به افزايش توليد، كاهش مصرف منابع و بهبود كيفيت محصولات كشاورزي كمك كند. از طريق سيستم‌هاي هوش مصنوعي، كشاورزان مي‌توانند به طور دقيق‌تر و بهينه‌تر به مديريت مزرعه و محصولات خود بپردازند و كمترين ضرر و ضايعات را در فرآيند توليد محصول داشته باشند.

# رويكرد سايبري به مسئله فلسطين و محور مقاومت

## آسيب‌ها و مخاطرات

تهديدات سايبري در مسئله فلسطين و كشورهاي محور مقاومت، مانند بسياري از مسائل سياسي و اجتماعي ديگر، به دليل استفاده فزاينده از فناوري‌هاي ديجيتال، شبكه‌هاي اجتماعي و فضاي اينترنت، ابعاد پيچيده‌اي پيدا كرده‌اند. در اين زمينه، تهديدات سايبري مي‌توانند به‌طور مستقيم يا غيرمستقيم بر روندهاي سياسي، اجتماعي و انساني تأثير بگذارند. در زير به برخي از مهم‌ترين تهديدات سايبري در اين زمينه اشاره مي‌كنيم:

### حملات سايبري به زيرساخت‌هاي حياتي

اختلال در خدمات دولتي و نهادهاي حاكميتي: حملات سايبري مي‌توانند زيرساخت‌هاي حياتي را هدف قرار دهند. اين حملات ممكن است شامل حملات به سرورهاي دولتي، سامانه‌هاي ثبت‌نام، بانك‌هاي اطلاعاتي و ساير سيستم‌هاي كليدي باشد كه به آسيب‌رساندن به عملكرد اداري و اقتصادي و سلامت افراد منجر شود.

تخريب داده‌ها و سرقت اطلاعات: يكي از تهديدات مهم در اين زمينه، سرقت اطلاعات حساس است. به عنوان مثال، اطلاعات مرتبط با امنيت ملي، استراتژي‌هاي سياسي يا حتي مذاكرات محرمانه مي‌تواند توسط هكرها به سرقت برود يا تخريب شود. اين امر مي‌تواند تبعات زيادي براي امنيت و روندهاي سياسي آن داشته باشد.

### دستكاري و انتشار اطلاعات غلط (Fake News)

پراكنده‌سازي اطلاعات نادرست و تبليغات سايبري: دشمنان مي‌توانند با استفاده از رسانه‌هاي اجتماعي و ابزارهاي ديجيتال، اطلاعات غلط يا تبليغات مغرضانه منتشر كنند تا افكار عمومي را در سراسر جهان تحت تأثير قرار دهند. به‌طور خاص، گروه‌هاي سياسي، رسانه‌ها و دولت‌ها ممكن است از هوش مصنوعي و ربات‌هاي اينترنتي (Botnets) براي انتشار اخبار جعلي و تحريك احساسات قومي يا مذهبي استفاده كنند.

تحريف حقايق: رسانه‌هاي اجتماعي با بهره‌گيري از هوش مصنوعي مي‌توانند بستري مناسب براي انتشار اطلاعات نادرست و تحريف حقايق فراهم كنند. اين تهديد مي‌تواند موجب افزايش تنش‌ها، گمراه كردن افكار عمومي و آسيب به فرآيندهاي سياسي و اجتماعي شود.

### حملات سايبري به سازمان‌هاي حقوق بشري و گروه‌هاي فعال فلسطيني

مهاجمان سايبري دولتي: گروه‌هاي هكري كه وابسته به دولت‌ها يا سازمان‌هاي سياسي هستند، مي‌توانند گروه‌هاي حقوق بشري و فعالان فلسطيني را هدف قرار دهند. اين حملات ممكن است شامل حملات DDoS، جاسوسي سايبري، يا سرقت اطلاعات فعالان حقوق بشر باشد.

نفوذ در ارتباطات و ارتباطات ديجيتال: گروه‌هاي فلسطيني و مقاومت ممكن است در معرض حملات سايبري براي نظارت بر مكاتبات، دسترسي به اطلاعات محرمانه يا آزارهاي آنلاين قرار گيرند. اين حملات مي‌تواند به هدف سركوب و تضعيف مقاومت‌ها و حركت‌هاي آزادي‌طلبانه در فلسطين انجام گيرد.

### حملات سايبري به رسانه‌ها و گروه‌هاي خبري

سانسور ديجيتال و محدوديت دسترسي به اطلاعات: دولت‌ها يا گروه‌هاي سياسي ممكن است براي كنترل روايت‌هاي خبري، حملات سايبري به وب‌سايت‌ها، رسانه‌هاي اجتماعي و شبكه‌هاي خبري انجام دهند. اين حملات مي‌توانند به تضعيف ظرفيت رسانه‌هاي فلسطيني و جهاني براي پوشش اخبار و حقيقت‌ها منجر شوند.

حملات به خبرنگاران و روزنامه‌نگاران: خبرنگاران و روزنامه‌نگاران فعال در زمينه پوشش اخبار فلسطين ممكن است هدف حملات سايبري قرار گيرند. اين حملات مي‌تواند شامل دزدي اطلاعات، حملات فيشينگ يا حتي جاسوسي ديجيتال باشد.

### حملات سايبري به شبكه‌هاي اجتماعي و پلتفرم‌هاي آنلاين

جنگ سايبري در شبكه‌هاي اجتماعي: فضاي ديجيتال و شبكه‌هاي اجتماعي مانند توييتر، فيسبوك و اينستاگرام، تبديل به عرصه‌اي براي جنگ‌هاي اطلاعاتي و سايبري شده‌اند. در اين زمينه، حملات سايبري مي‌توانند به شكل اختلال در روندها، يا بلوكه كردن حساب‌هاي كاربري فعالان فلسطيني يا گروه‌هاي حقوق بشري باشد.

حذف يا دستكاري محتوا: گروه‌ها و دولت‌ها مي‌توانند از فناوري‌هاي سايبري براي حذف يا دستكاري محتواي حساس و مرتبط با فلسطين استفاده كنند. اين مي‌تواند شامل حذف مطالب مرتبط با نقض حقوق بشر، خشونت‌ها يا مبارزات عليه فلسطيني‌ها باشد.

### حملات به زيرساخت‌هاي اقتصادي

اختلال در بانك‌ها و سيستم‌هاي مالي: حملات سايبري مي‌توانند زيرساخت‌هاي مالي محور مقاومت را هدف قرار دهند و موجب بروز اختلال در نقل و انتقالات و دسترسي به منابع مالي شوند. اين امر مي‌تواند تأثيرات منفي بر اقتصاد، تجارت و زندگي روزمره مردم داشته باشد.

سرقت و تخريب اطلاعات مالي: علاوه بر اختلال در سيستم‌هاي مالي، حملات سايبري مي‌توانند به سرقت داده‌هاي مالي و تخريب اطلاعات اقتصادي مهم منجر شوند.

### حملات سايبري به سازمان‌هاي بين‌المللي

تأثير بر فرآيندهاي ديپلماتيك: حملات سايبري مي‌توانند روندهاي ديپلماتيك، يا حتي فعاليت‌هاي سازمان‌هاي بين‌المللي مانند گزارشگران سازمان ملل را مختل كنند. به‌ويژه در بحران‌هاي پيچيده و حساس، حملات سايبري ممكن است به‌طور عمدي براي تأثيرگذاري بر نتايج تحقيقات و بررسي‌ها طراحي شوند.

سرقت و انتشار اسناد محرمانه: هكرها مي‌توانند اسناد محرمانه و اطلاعات حساس را از سيستم‌هاي دولتي يا بين‌المللي دزديده و در اختيار سازمان‌هاي اطلاعاتي قرار دهند.

### هك و دسترسي به اطلاعات نظامي و امنيتي

نفوذ به سيستم‌هاي نظامي: حملات سايبري مي‌توانند هدف‌هاي نظامي و امنيتي را هدف قرار دهند. در اين راستا، اطلاعات و ارتباطات امنيتي و نظامي فلسطين و محور مقاومت مي‌تواند در معرض سرقت، تخريب يا سوءاستفاده قرار گيرد.

جاسوسي سايبري: جاسوسان مي‌توانند از فناوري‌هاي سايبري براي حفظ ارتباط با سرپل‌ها و ارسال اطلاعات و دريافت دستورات و مأموريت‌ها استفاده كنند، بدون اين‌كه شناسايي شوند.

رديابي و مكان‌يابي: با استفاده از توانمندي هوش مصنوعي در شناسايي روابط و تماس‌ها و پيش‌بيني الگوهاي رفتاري، دشمن مي‌تواند مكان افراد يا تجهيزات را تشخيص داده و دست به ترور يا تخريب بزند.

## فرصت‌ها و قابليت‌ها

فضاي سايبري مي‌تواند فرصت‌هاي زيادي براي حمايت از مسئله فلسطين و محور مقاومت فراهم آورد و در اين راستا به ارتقاي آگاهي جهاني، حمايت از حقوق بشر، بهبود فرآيندهاي سياسي، اجتماعي و اقتصادي و تسهيل مقاومت مدني كمك كند. در اينجا به برخي از مهم‌ترين فرصت‌ها و كاربردهاي سايبري براي مسئله فلسطين اشاره مي‌كنيم:

### افزايش آگاهي جهاني و به اشتراك‌گذاري اطلاعات

رسانه‌هاي اجتماعي و پلتفرم‌هاي آنلاين: فضاي سايبري به فلسطيني‌ها و حاميان آن‌ها اين امكان را مي‌دهد كه از رسانه‌هاي اجتماعي براي به اشتراك‌گذاري اخبار، ويدئوها، عكس‌ها و اطلاعات استفاده كنند. اين ابزارها مي‌توانند براي مستندسازي نقض حقوق بشر، حملات نظامي رژيم صهيونيستي و وضعيت انساني در فلسطين به كار گرفته شوند.

پويش‌هاي جهاني و حمايت‌هاي بين‌المللي: استفاده از هشتگ‌هاي مرتبط مانند #FreePalestine، #SavePalestine و #StandWithPalestine باعث گسترش آگاهي در سطح جهاني مي‌شود و موجب مي‌شود كه مسئله فلسطين در سطح بين‌المللي مورد توجه قرار گيرد. پلتفرم‌هاي آنلاين نقش مهمي در سازمان‌دهي و هماهنگي حركت‌هاي بين‌المللي و تجمعات حمايتي با استفاده از پويش‌هاي آنلاين دارند.

پخش ويدئوهاي مستند: استفاده از ويدئوهاي مستند و گزارشي در شبكه‌هاي اجتماعي مي‌تواند به نهادهاي حقوق بشر و سازمان‌هاي بين‌المللي كمك كند تا گزارشات دقيقي از وضعيت فلسطين ارائه دهند و فشارهاي جهاني را براي تغيير سياست‌هاي حاميان رژيم غاصب صهيونيستي افزايش دهند.

### دفاع از حقوق بشر و مستندسازي نقض‌ها

مستندسازي جنايات جنگي و نقض حقوق بشر: ابزارهاي ديجيتال مانند تلفن‌هاي هوشمند و دوربين‌هاي ديجيتال و پخش آنلاين و برخط تصاوير مي‌تواند به مردم فلسطين كمك كند تا مستندات و شواهد نقض حقوق بشر، حملات نظامي و سركوب‌هاي سياسي را جمع‌آوري كنند. اين مستندات مي‌توانند در دادگاه‌هاي بين‌المللي، سازمان‌هاي حقوق بشري و رسانه‌ها براي معرفي جنايات جنگي و نقض حقوق بشر استفاده شوند.

سايت‌ها و پلتفرم‌هاي گزارش‌دهي آنلاين: وب‌سايت‌ها و پلتفرم‌هاي آنلاين با موضوع مقاومت و حمايت از فلسطين مي‌توانند به عنوان ابزارهايي براي گزارش‌دهي از نقض‌هاي حقوق بشر به كار گرفته شوند.

### تقويت روندها و فرآيندهاي مقاومت

آموزش مقاومت ديجيتال: با استفاده از آموزش‌هاي آنلاين و محتواي آموزشي در فضاي سايبري، فلسطيني‌ها مي‌توانند مهارت‌هاي لازم براي مقاومت و مبارزات ديجيتال را كسب كنند. اين آموزش‌ها مي‌توانند شامل امنيت ديجيتال، مقابله با سانسور و نحوه استفاده از ابزارهاي آنلاين براي سازمان‌دهي اعتراضات و مجاهدات باشند.

استفاده از فناوري‌هاي رمزنگاري: در مواقعي كه ارتباطات با تهديدات امنيتي مواجه مي‌شود، استفاده از ابزارهاي رمزنگاري، مانند پيام‌رسان‌هاي امن و VPNها، مي‌تواند به حفظ حريم خصوصي و امنيت ارتباطات كمك كند. اين ابزارها مي‌توانند در هماهنگي و سازمان‌دهي فعاليت‌هاي نظامي، سياسي و اجتماعي مورد استفاده قرار گيرند.

### كمك به فرآيندهاي ديپلماتيك و سياسي

دستگاه ديپلماتيك ديجيتال: استفاده از فضاي سايبري مي‌تواند به تسهيل ارتباطات ديپلماتيك و سياسي كمك كند. نهادهاي فلسطيني و حاميان بين‌المللي مي‌توانند از ابزارهاي ديجيتال براي برقراري ارتباطات سريع‌تر، انعطاف‌پذيرتر و مؤثرتر با دولت‌ها، سازمان‌هاي بين‌المللي و جوامع مختلف استفاده كنند.

رسانه‌هاي اجتماعي براي ايجاد فشار بر دولت‌ها: گروه‌ها و فعالان فلسطيني مي‌توانند از فضاي سايبري براي ايجاد فشار بر دولت‌ها و سازمان‌هاي بين‌المللي براي پذيرش سياست‌هايي در حمايت از فلسطين استفاده كنند. شبكه‌هاي اجتماعي به فعالان اين امكان را مي‌دهند كه به صورت جمعي براي تغيير سياست‌هاي دولت‌ها و نهادها فعاليت كنند.

### كمك به سازمان‌دهي و بسيج اجتماعي

برگزاري پويش‌هاي حمايت از فلسطين: فضاي سايبري مي‌تواند به سازمان‌دهي كمپين‌هاي جهاني براي جمع‌آوري كمك‌هاي مالي، امدادي يا سياسي براي فلسطيني‌ها كمك كند. اين كمپين‌ها مي‌توانند در پلتفرم‌هاي ديجيتال راه‌اندازي شوند و از طريق مشاركت عمومي به اهداف انساني و سياسي كمك كنند.

دعوت به تجمعات و اعتراضات آنلاين: فضاي سايبري به فعالان اين امكان را مي‌دهد كه تجمعات، اعتراضات و فعاليت‌هاي سياسي آنلاين و يا خياباني برگزار كنند. اين اعتراضات مي‌توانند در حمايت از حقوق فلسطيني‌ها يا عليه نقض حقوق بشر و سياست‌هاي رژيم صهيونيستي باشند.

### كمك به بهبود وضعيت اقتصادي و اجتماعي فلسطين

اقتصاد ديجيتال و كار از راه دور: فضاي سايبري مي‌تواند به فلسطيني‌ها اين امكان را بدهد كه از طريق شغل‌هاي ديجيتال و كار از راه دور به درآمد و بهبود وضعيت اقتصادي خود بپردازند. شركت‌ها و سازمان‌ها مي‌توانند از فلسطيني‌ها به عنوان نيروي كار دوركار در زمينه‌هاي مختلف مانند توسعه نرم‌افزار، طراحي گرافيكي و ترجمه استفاده كنند.

ايجاد بازارهاي آنلاين براي محصولات: استفاده از پلتفرم‌هاي تجارت الكترونيك مي‌تواند به كسب‌وكارهاي فلسطيني و يا صنايع دستي آن اين امكان را بدهد كه محصولات خود را به بازارهاي بين‌المللي معرفي كنند. اين امر مي‌تواند به رشد اقتصادي و توسعه اشتغال در مناطق فلسطيني كمك كند.

### كمك به ارتقاي آموزش و آگاهي‌سازي در فلسطين

آموزش آنلاين و دسترسي به منابع آموزشي: فضاي سايبري مي‌تواند به فلسطيني‌ها اين امكان را بدهد كه به منابع آموزشي و تحصيلي دسترسي پيدا كنند، حتي در شرايط سخت و درگيري‌ها. برنامه‌هاي آموزشي آنلاين مي‌توانند به دانش‌آموزان و دانشجويان فلسطيني كمك كنند تا از فاصله‌گذاري و محدوديت‌هاي فيزيكي عبور كنند.

پلتفرم‌هاي آگاهي‌سازي حقوق بشر: از طريق سايت‌ها و اپليكيشن‌هاي آگاهي‌سازي حقوق بشر، فعالان فلسطيني مي‌توانند به ديگران درباره حقوق خود، قوانين بين‌المللي و نحوه دفاع از حقوق مدني آموزش دهند.

### مقابله با سانسور و محدوديت‌ها

دور زدن سانسور اينترنتي: دولت‌ها و نهادهاي مختلف ممكن است در تلاش باشند تا فضاي سايبري را براي فلسطيني‌ها محدود كنند و دسترسي به اطلاعات و منابع خارجي را مسدود كنند. با اين حال، ابزارهايي مانند VPNها، پروكسي‌ها و تور (Tor) مي‌توانند به فلسطيني‌ها كمك كنند تا به اينترنت آزاد دسترسي داشته باشند و از سانسور دولتي رژيم غاصب جلوگيري كنند.

برقراري ارتباط از طريق رسانه‌هاي مستقل: استفاده از رسانه‌هاي مستقل آنلاين مي‌تواند به فلسطيني‌ها كمك كند تا صداي خود را به گوش جهانيان برسانند و از طريق اخبار و گزارش‌هاي مستقل به مقابله با روايت‌هاي دولتي مغرضانه بپردازند.

## نقاط قوت و برتري‌ها

جبهه مقاومت در استفاده از فضاي سايبري توانسته است از نقاط قوت و برتري‌هاي خاصي برخوردار شود كه به آن كمك كرده تا به‌طور مؤثر در عرصه‌هاي مختلف مبارزه سياسي، اجتماعي و نظامي فعاليت كند. در اين زمينه، فضاي سايبري به‌عنوان ابزاري قدرتمند براي سازمان‌دهي، اطلاع‌رساني، مقاومت ديجيتال و بسيج حمايت‌هاي جهاني از جبهه مقاومت عمل مي‌كند. در زير به برخي از مهم‌ترين نقاط قوت و برتري‌هاي جبهه مقاومت در استفاده از فضاي سايبري اشاره مي‌كنيم:

### توانايي در سازمان‌دهي و بسيج منابع و نيروها

برقراري ارتباطات سريع و مؤثر: جبهه مقاومت نشان داده توانايي و دانش فني لازم را براي برقراري ارتباطات فوري و مؤثر با اعضا، گروه‌ها و طرفداران خود بدون نياز به زيرساخت‌هاي فيزيكي پيچيده دارد.

سازمان‌دهي حركت‌هاي مردمي: جبهه مقاومت توانسته با بهره‌گيري از احساسات انسان‌دوستانه و بشري بدون محدوديت جغرافيايي، تجمعات، اعتراضات و كمپين‌هاي حمايت‌گرايانه را در سطح جهاني برپا كند.

برند و هويّت مقاومت: به مرور زمان و استقامت طولاني‌مدّت محور مقاومت سبب شده تا عنوان آن تبديل به يك برند جهاني براي مبارزه با زورگويي و استكبار شود و اين اهميّت فراواني در جذب همكاري انسان‌هاي آزادانديش دارد.

### برخورداري از صداقت

پخش اخبار و روايت‌هاي جايگزين: يكي از مزاياي عمده فضاي سايبري براي جبهه مقاومت، توانايي در پخش سريع اخبار و روايت‌هاي واقعي و صحيح است. مطابقت روايت مقاومت از واقعيت سبب مي‌شود راحت‌تر از جبهه دشمن بتواند اخبار خود را منتشر سازد و ناگزير به تدوين‌هاي پيچيده نداشته باشد.

مستندسازي نقض حقوق بشر: جبهه مقاومت توانسته با نشان دادن واقعي آن‌چه هست و به‌سادگي ديده مي‌شود از شبكه‌هاي اجتماعي و پلتفرم‌هاي ديجيتال براي مستندسازي و به اشتراك‌گذاري تصاوير و ويدئوهاي مستند از نقض‌هاي حقوق بشر، حملات نظامي و ديگر جنايات رژيم غاصب عليه مردم استفاده كند.

### مطابقت با فطرت و ذات انساني

خيزش جهاني از همه اديان: جبهه مقاوت قادر بوده و هست تا با دل‌هاي انسان‌ها مرتبط شود و فطرت‌هاي پاك و دست‌نخورده و سالم را متأثر سازد. اين سبب شده تا در اقصي نقاط جهان در تمام اديان و مذاهب حركت‌هاي حمايت از ملّت فلسطين شكل بگيرد و راه بيافتد.

نفوذ به درون دولت‌ها و ملّت‌ها: اين هماهنگي دعوت جبهه مقاومت با فطرت بشري سبب شده برخي افرادي كه درون دولت‌هاي كشورهاي مختلف هستند با اين جريان همراه شوند.

### در اختيار داشتن نيروهاي داراي مهارت فني

تحصيلات دانشگاهي و علمي: جبهه مقاومت از افرادي برخوردار است كه تحصيلات مورد نياز براي به‌كارگيري و بهره‌برداي از فناوري‌هاي سايبري و هوش مصنوعي را دارند.

همراهي نيروهاي متخصّص: بسياري از كارشناسان متعهّد و متخلّق و مؤمن در ميان امّت اسلامي و حتي كشورهاي غيراسلامي وجود دارند كه حاضرند با جبهه مقاومت همكاري نمايند.

### اخلاص و نيّت الهي

همّت والا در انجام فعاليت‌ها: يكي از ويژگي‌هاي خاصّ نيروهاي جبهه مقاومت و مبارزان فلسطيني اخلاص و نيّت خالصانه‌اي است كه دارند. اين اخلاص سبب شده تا بتوانند با تمام وجود فعاليت كرده و خستگي‌ناپذير شوند. همين روحيه مي‌تواند در پروژه‌هاي سايبري به كار گرفته شود.

انجام كار درست، بي‌نياز به نظارت: وقتي كاري با اخلاص انجام شود، نياز به ناظر ندارد. زيرا فرد مجهّز به انگيزه‌هاي قوي دروني است و اين انگيزه او را به انجام درست و صحيح كارها هدايت مي‌نمايد. چنين انگيزه‌ قدرتمندي در تمامي نيروهاي جبهه مقاومت به‌وفور يافت مي‌شود.

### امداد و ياري پروردگار

نصرت و ياري خدا: آن‌چه مستضعفان دارند و مستكبران هرگز، هدايت و نصرت الهي است. حتي در بدترين شرايط بحراني و حالاتي كه به نظر دشوار مي‌رسند لطف و امداد الهي جريان دارد و نيروهاي مقاوم و مخلص را همراهي مي‌كند.

پذيرش قضا و قدر الهي: بعضي امور به ظاهر مورد كراهت و عدم پذيرش هستند، ولي نفع و سود آن‌ها بيشتر است كه ما انسان‌ها قادر به درك آن در زمان وقوع نيستيم و در آينده اين مصالح فهميده مي‌شود. جبهه مقاوت به دليل رويكرد ايماني خود، اين درك از قضا و قدر را دارد و اين يك توانايي بسيار بزرگ براي تحمل تلفات و ضربات است.

### فداكاري و توانايي عبور از خود

شجاعت و فقدان ترس در مبارزه: هنگامي‌كه بالاترين و ترسناك‌ترين لطمه‌اي كه دشمن بتواند به تو بزند، دقيقاً هماني باشد كه تو از خدا مي‌خواهي؛ از دست دادن جان و شهادت، ديگر جايي براي ترس باقي نمي‌ماند و اين يكي از بزرگ‌ترين نقاط قوت نيروهاي مقاومت است.

پيش‌قدم شدن در امور خير: تنبلي براي فداكاران فرض بروز و تحقّق ندارد. افراد عادي براي حفظ جان و راحتي خود معمولاً تلاش مي‌كنند تا جايي كه توان دارند از پذيرفتن كارها بپرهيزند و آن‌ها را به ديگران واگذارند. اما در جبهه مقاومت افراد در پذيرفتن و انجام مأموريت‌ها از هم پيشي مي‌گيرند. اين در جبهه مقابل ناممكن است.

## نقاط ضعف و كاستي‌ها

حاميان فلسطين در استفاده از فضاي سايبري با چندين چالش و نقطه ضعف روبه‌رو هستند كه مي‌تواند بر توانايي آن‌ها در بهره‌برداري از اين ابزار قدرتمند براي حمايت از حقوق فلسطيني‌ها و پيشبرد اهداف تأثير منفي بگذارد. اين نقاط ضعف نه تنها بر فعاليت‌هاي ديجيتال حاميان فلسطين تأثير مي‌گذارد، بلكه مي‌تواند بر ميزان تأثيرگذاري آن‌ها در سطح جهاني و در برابر رقبا يا مخالفان سياسي نيز تأثيرگذار باشد. در زير به مهم‌ترين موارد اشاره مي‌كنيم:

### محدوديت‌هاي دسترسي به اينترنت و فناوري

سانسور و محدوديت‌هاي دولتي: بسياري از دولت‌ها، به‌ويژه در كشورهاي منطقه خاورميانه، دسترسي به اينترنت و فضاي ديجيتال را محدود مي‌كنند. در مواردي مانند غزه، اين محدوديت‌ها مي‌تواند شامل قطع اينترنت، محدوديت در دسترسي به شبكه‌هاي اجتماعي، مسدود كردن وب‌سايت‌هاي خاصّ و حتي قطع برق باشد كه به فعالان فلسطيني و حاميان آن‌ها آسيب مي‌زند. در اين شرايط، دسترسي به ابزارهاي ديجيتال براي سازمان‌دهي، ارتباطات و پخش اطلاعات به شدت دشوار مي‌شود.

محدوديت‌هاي فني و زيرساختي: كمبود دسترسي به اينترنت با سرعت بالا، يا حتي به اينترنت در مناطق روستايي يا تحت محاصره، مي‌تواند مانع از بهره‌برداري مؤثر از فضاي سايبري شود. همچنين، بسياري از فلسطيني‌ها ممكن است به فناوري‌هاي پيشرفته يا نرم‌افزارهاي امنيتي دسترسي نداشته باشند كه اين امر تهديداتي براي حريم خصوصي و امنيت اطلاعات آن‌ها به همراه دارد.

### كمبود منابع مالي براي استفاده از ابزارهاي پيشرفته

استفاده از ابزارهاي ديجيتال پيشرفته، مانند سرويس‌هاي VPN، نرم‌افزارهاي رمزنگاري يا حتي راه‌اندازي كمپين‌هاي تبليغاتي در شبكه‌هاي اجتماعي نيازمند منابع مالي است. بسياري از گروه‌ها و سازمان‌هاي حامي فلسطين ممكن است با مشكلات مالي روبه‌رو باشند كه مانع از استفاده بهينه از اين ابزارها مي‌شود. در نتيجه، آن‌ها نمي‌توانند به‌طور مؤثر از فناوري‌هاي نوين براي مقابله با تهديدات سايبري يا سانسور بهره‌برداري كنند.

### حملات سايبري و تهديدات امنيتي

آسيب‌پذيري در برابر حملات سايبري: بسياري از حاميان فلسطين، به‌ويژه در داخل فلسطين و كشورهاي هم‌مرز، ممكن است به‌طور مداوم هدف حملات سايبري قرار گيرند. با توجه به سطح پيشرفته‌تري كه طرف‌هاي مقابل در توانايي‌هاي سايبري دارند، گروه‌هاي حامي فلسطين به‌طور خاص در برابر حملات سايبري آسيب‌پذير هستند.

نداشتن پلت‌فرم‌هاي اختصاصي: يكي ديگر از تهديدات مهم، نظارت‌هاي ديجيتال و جاسوسي آنلاين است. طرف‌هاي مخالف به دليل مالكيت پلت‌فرم‌ها و سكوهاي پيام‌رسان مي‌توانند از قدرت خود براي دسترسي به اطلاعات شخصي فعالان و سازمان‌هاي حامي فلسطين استفاده كنند. اين تهديدات مي‌تواند به افشاي اطلاعات حساس، سركوب فعالان و حتي از دست رفتن امنيت و حريم خصوصي منجر شود.

### عدم يكپارچگي و هماهنگي در استفاده از فضاي سايبري

فقدان استراتژي‌هاي يكپارچه: يكي از چالش‌هاي عمده در فضاي سايبري، نبود هماهنگي بين گروه‌ها و سازمان‌هاي مختلف حامي فلسطين است. به دليل پراكندگي جغرافيايي و تنوع در سازمان‌دهي گروه‌ها، ممكن است اقدامات در فضاي سايبري پراكنده و بدون استراتژي‌هاي يكپارچه انجام شود. اين پراكندگي مي‌تواند منجر به كاهش تأثيرگذاري و عدم موفقيت در هدف‌گذاري‌هاي بلندمدت شود.

### مشكلات در توليد و مديريت محتواي ديجيتال

كمبود منابع براي توليد محتواي حرفه‌اي: توليد محتواي باكيفيت در فضاي سايبري براي جلب توجه جهاني نيازمند منابع مالي و انساني است، زيرا به ابزارهاي تخصّصي صوتي و تصويري نياز دارد. گروه‌هاي حامي فلسطين ممكن است از نظر منابع مالي و تخصصي براي توليد محتواي ويدئويي، گرافيكي يا محتواي چندرسانه‌اي حرفه‌اي محدود باشند. در نتيجه، توليد محتواي مؤثر و جذاب براي جذب مخاطب جهاني به سختي انجام مي‌شود.

نبود تحليل دقيق داده‌ها: در فضاي ديجيتال، استفاده از تحليل داده‌ها و اطلاعات براي شناخت بهتر افكار عمومي و هدف‌گذاري مؤثر در كمپين‌ها ضروري است. گروه‌هاي حامي فلسطين به دليل محدوديت‌هاي مالي و فني نتوانند به طور مؤثر از تحليل داده‌ها استفاده كنند و از سوي ديگر، برخلاف رژيم اشغالگر، دسترسي به داده‌هاي بزرگ و هوش مصنوعي ندارند و اين مي‌تواند مانع از پيشبرد مؤثر كمپين‌هاي ديجيتال شود.

### محدوديت در دسترسي به پلتفرم‌ها و رسانه‌هاي جهاني

تهديدات قانوني و فشارهاي بين‌المللي: برخي از كشورهاي غربي به ويژه ايالات متحده، كشورهاي اتحاديه اروپا و اسرائيل، فشارهايي را بر شركت‌ها و پلتفرم‌هاي فناوري وارد مي‌آورند تا محتواهاي حامي فلسطين را حذف كنند يا عليه آن‌ها اقدام قانوني انجام دهند.

تعريف‌هاي سياسي و حقوقي متناقض: از آنجايي كه مسئله فلسطين به‌طور گسترده در سطح جهاني تحت تأثير تحولات سياسي و حقوقي قرار دارد، فعاليت‌هاي سايبري حاميان فلسطين مي‌تواند با چالش‌هاي قانوني و سياسي روبه‌رو شود. به‌ويژه در كشورهاي مختلف، تشخيص فعاليت‌هاي قانوني و مشروع از فعاليت‌هاي تروريستي يا غيرقانوني مي‌تواند پيچيده و چالش‌برانگيز باشد.

### عدم درك كامل از اصول امنيت سايبري

آگاهي پايين از امنيت سايبري: برخي از گروه‌هاي حامي فلسطين ممكن است از اصول پايه‌اي امنيت سايبري آگاهي كافي نداشته باشند و اين امر مي‌تواند موجب آسيب‌پذيري آن‌ها در برابر حملات سايبري و تهديدات امنيتي شود. همچنين، عدم آگاهي از ابزارهاي رمزنگاري و امنيتي مي‌تواند اطلاعات حساس و ارتباطات گروه‌هاي حامي فلسطين را در معرض خطر قرار دهد.

# ضرورت‌هاي تأسيس قرارگاه سايبري

محور مقاومت به دليل قوّت‌ها و توانمندي‌هاي ذاتي خود كه ناشي از ايمان به خداي متعال و تجربه ايستادگي طولاني‌مدت در برابر ظلم و استكبار است برتري‌هايي نسبت به جبهه كفر جهاني دارد كه ظرفيت‌هايي بي‌بديل را شكل داده‌اند. اگر اين ظرفيت‌ها به‌صورت هم‌جهت و هم‌افزا مورد بهره‌برداري قرار بگيرند، جهش‌هاي بزرگ و حيرت‌آوري را در جبهه مقاومت پديد مي‌آورند.

بسياري از فعاليت‌هاي مقاومت در حال حاضر به صورت خودجوش و طبيعتاً از هم‌گسيخته و پراكنده شكل مي‌گيرد. حركت‌هايي كه از خلوصي معنوي و درك تقابل دو جبهه حق و باطل شكل‌گرفته است. بدين‌‌ترتيب بسياري گروه‌هاي كوچك در سراسر جهان تشكيل مي‌شوند و هر كدام با درك و تشخيص خود و با استفاده از توانمندي‌هاي اندك دست به فعاليت مي‌زنند.

اگر بخواهيم اين حركت‌هاي پراكنده را مانند قطرات آب به هم متصل كنيم، تا سيل و جرياني شديد براي نابودي اسرائيل فراهم آورند، لازم است قرارگاهي تشكيل شود تا به عنوان يك ستاد مشترك و متمركز تمامي اين فعاليت‌ها را همسو كند. اين قرارگاه راهبردها را با همكاري خود نيروهاي جبهه تدوين كرده و سازگار مي‌كند و تكليف هر گروه مشخّص و متمايز از سايرين مي‌شود.

# اهداف و مأموريت‌هاي قرارگاه سايبري

1. شناسايي و تحليل تهديدات سايبري و پيش‌بيني حملات احتمالي
2. تدوين راهبردهاي تهاجمي و دفاعي در مواجهه با تهديدات سايبري
3. توليد نقشه سايبري جامع استقرار و فعاليت نيروهاي جبهه مقاومت
4. تدوين برنامه‌هاي همكاري مبتني بر تقسيم كار در فضاي مجازي
5. جهت‌دهي جريان آگاه‌سازي جهاني و اطلاع‌رساني جامع و پايدار
6. تضمين برقراري ارتباط دائم و پيوسته سايبري نيروهاي جبهه مقاومت
7. برگزاري نشست‌هاي برخط و مجازي در راستاي تقويت همفكري‌ها در جهت دستيابي به راه‌حل‌ها
8. ايجاد فرصت مشاركت و همكاري تمامي نيروهاي جبهه مقاومت در فعاليت‌ها
9. حفظ امنيت گروه‌ها از طريق ارائه آموزش، توصيه‌ها و خدمات سايبري
10. توليد پلت‌فرم‌ها و سكوهاي پيام‌رسان ايمن و مستقل از شبكه‌هاي صهيونيستي
11. دستيابي به سخت‌افزارهاي مطمئن و دور از دسترس شركت‌هاي حامي اسرائيل
12. تزريق فرهنگ اميدواري و اعتماد به خداي متعال و پايداري در راه هدف
13. فراهم آوردن فرصت جذب نيروهاي داوطلب سراسر جهان در گروه‌هاي مقاومت
14. ارائه الگوهاي مبارزه و جهاد سايبري به تمامي نيروهاي فعّال جبهه مقاومت

# الزامات تأسيس قرارگاه سايبري

تأسيس يك قرارگاه سايبري نيازمند رعايت الزامات مختلفي از جنبه‌هاي فني، مديريتي، حقوقي و امنيتي است. اين قرارگاه براي دستيابي به اهداف مختلفي مانند دفاع سايبري، مقابله با تهديدات ديجيتال، جمع‌آوري اطلاعات، ارائه مشاوره فني يا مديريت بحران‌هاي سايبري ايجاد مي‌شود.

### الزامات فني

1. پلتفرم‌هاي نرم‌افزاري و سخت‌افزاري مناسب، سرورها و سيستم‌هاي ذخيره‌سازي براي پردازش داده‌ها، ذخيره‌سازي اطلاعات و اجراي سيستم‌ها، سرورهاي قدرتمند و پايدار.
2. از ابزارهاي مختلف امنيتي مانند فايروال‌ها، سامانه‌هاي تشخيص نفوذ (IDS/IPS)، سيستم‌هاي مديريت تهديد و ضد بدافزارها بايد استفاده شود تا از شبكه و اطلاعات محافظت گردد.
3. ابزارهاي تحليلي و پايش وضعيت شبكه، سيستم‌ها و داده‌ها براي شناسايي تهديدات و آناليز رويدادهاي سايبري و شبكه‌هاي امن و پروتكل‌هاي ارتباطي براي حفاظت از داده‌ها و ارتباطات.

### الزامات انساني

1. متخصصان امنيت سايبري و افراد ماهر در زمينه‌هاي مختلف امنيت سايبري مانند تحليلگران تهديد، هكرهاي اخلاقي، كارشناسان پشتيباني از سامانه‌ها، تحليلگران فضاي ديجيتال و متخصصان شبكه
2. مديران و تصميم‌گيرندگان با تجربه براي هدايت قرارگاه و اتخاذ تصميمات سريع و استراتژيك در مواجهه با بحران‌هاي سايبري، بحران‌هاي اطلاعاتي يا تهديدات روزمره
3. برنامه‌هاي آموزشي براي ارتقاي مهارت‌هاي كاركنان شامل آشنايي با تكنيك‌هاي مقابله با تهديدات سايبري، مديريت بحران‌ها و نحوه استفاده از ابزارهاي امنيتي
4. هماهنگي و همكاري بين‌سازماني براي كار با ديگر نهادها، مانند سازمان‌هاي اطلاعاتي، نظامي و دولتي در هماهنگي، اشتراك‌گذاري اطلاعات و همكاري در سطح ملي و بين‌المللي

### الزامات امنيتي

1. حفاظت از اطلاعات حساس، حفظ محرمانگي، صحت و دسترس‌پذيري اطلاعات
2. استراتژي و برنامه جامع براي شناسايي، ارزيابي و مقابله با تهديدات سايبري و حملات احتمالي شامل سناريوهاي حملات DDoS، حملات فيشينگ، بدافزارها و تهديدات پيشرفته
3. ايجاد شبكه‌هاي مقاوم در برابر حملات خارجي با استفاده از فايروال‌ها، سيستم‌هاي نظارت و دفاع، به‌ويژه در برابر حملات سازمان‌يافته
4. استراتژي‌هاي پشتيبان‌گيري، بازيابي داده‌ها و ادامه‌دادن عمليات پس از حملات سايبري

### الزامات مديريتي

1. تعريف اهداف مشخص و استراتژيك شامل حفاظت از زيرساخت‌هاي حياتي، مقابله با تهديدات سايبري، ارتقاي آگاهي عمومي و ايجاد يك پلتفرم دفاعي جامع
2. برنامه‌ريزي و مديريت بحران براي مقابله با حملات سايبري و حوادث غيرمترقبه، آمادگي براي مقابله با حملات و نقض‌هاي امنيتي، ارزيابي آسيب‌ها و بازسازي زيرساخت‌ها
3. تشكيل گروه‌هاي تخصصي براي انجام وظايف مختلف شامل تيم‌هاي تحليل تهديد، تيم‌هاي پاسخ به حوادث، تيم‌هاي اطلاع‌رساني و مشاوره فني و گروه‌هاي مديريتي براي نظارت بر اقدامات

### الزامات فرهنگي

1. توسعه فرهنگ امنيت سايبري در ميان اعضاي قرارگاه و عموم مردم با ارتقاي آگاهي در زمينه‌هاي امنيت ديجيتال، حفاظت از اطلاعات و مقابله با تهديدات
2. ارتباطات و گزارش‌دهي به گونه‌اي كه اطلاعات به‌طور سريع و مؤثر به تمامي افراد و سازمان‌ها منتقل شود و برنامه‌هايي براي گزارش‌دهي به مقامات دولتي و عمومي در خصوص تهديدات سايبري
3. رصد دائمي تهديدات سايبري جهاني و ارتباط با تيم‌هاي بين‌المللي و نهادهاي امنيتي جهاني

### الزامات مالي و منابع

1. تأمين منابع مالي براي تأسيس و نگهداري از قرارگاه سايبري، خريد تجهيزات، نرم‌افزارها، آموزش و توسعه زيرساخت‌ها
2. تأمين و مديريت منابع انساني متخصص و مجرب در زمينه‌هاي مختلف امنيت سايبري و فناوري اطلاعات، آموزش مستمر و نگهداري و حفظ منابع انساني
3. مشاركت و حضور و همكاري و ارتباط دائمي تمامي گروه‌ها و تشكّل‌هاي حمايت از مقاومت و فلسطين

# مراحل تأسيس قرارگاه سايبري

## تجميع انگيزه‌ها از طريق همدلي ايمان‌محور

### برگزاري نشست‌هاي اوليه و ايجاد گفتمان نياز به قرارگاه متمركز

در نخستين گام بايد جلسات دوبه‌دو و غيرمشترك به صورت حضوري يا غيرحضوري و برخط با گروه‌ها و جريان‌هاي عمده جبهه مقاومت و حامي فلسطين برگزار شود. در اين نشست‌ها گفتگوهايي صورت مي‌پذيرد تا به جمع‌بندي اثباتي و ايجابي ضرورت تأسيس قرارگاه منجر شود. متن حاضر مي‌توان اولين سند و مبنا براي تفاهم فيمابين باشد. فرصت گفتگوي تك‌به‌تك با گروه‌ها اين امكان را فراهم مي‌كند تا به دقّت تمامي نگراني‌ها پاسخ داده شود و شبهات برطرف گردد و مسير بحث به سمتي برود كه نياز گروه مخاطب است.

همدلي موجود ميان گروه‌ها كه بر پايه ايمان به خداي متعال و درستي راه مقاومت در طول زمان شكل‌گرفته است به اين گفتگوها كمك مي‌كند، تا همگرايي حاصل شود.

### برگزاري گردهمايي مشترك نمايندگان تمامي گروه‌هاي مقاومت

ممكن است برخي از گروه‌ها به صورت غيرحضوري در اين گردهمايي مشاركت كنند. ولي محصول اين همايش اعلام رسمي همدلي تحقّق‌يافته است كه انگيزه و اميدي مشترك در تمامي افراد ايجاد مي‌كند. اين گردهمايي با بيانيه‌اي مشترك به پايان مي‌رسد كه همانا ضرورت تأسيس قرارگاه مشترك است.

در همين گردهمايي كميته‌هاي ضروري براي طراحي ساختار قرارگاه تعيين شده و هماهنگ مي‌شوند.

## همسوسازي ديدگاه‌ها از طريق همفكري پژوهش‌محور

### تشكيل گروه‌ها و كميته‌هاي همكاري علمي در راستاي طراحي ساختار قرارگاه

همدلي به تنهايي نمي‌تواند گروه‌ها را با هم همسو كند. زيرا در ارائه راه‌حل انسان‌ها با هم متفاوت هستند. اين تفاوت در تفكر سبب مي‌شود هر كدام به راه خود بروند، با اين باور كه راه رسيدن به هدف همان است، اگر چه هدف همه مشترك باشد.

از اين رو، بايستي گروه‌هاي پژوهشي مشترك به صورت حضوري و مجازي جلساتي تشكيل داده و از طريق تضارب آرا و بدون ملاحظات شخصي و حقوقي گفتگو كنند. از همدلي تا همفكري راه طولاني‌ست و نياز به بحث فراوان دارد. هر فرد يا گروه تلاش مي‌كند تا بر اساس مباني عقلاني خود و تجربياتي كه كسب كرده ديگران را نسبت به رأي خود متقاعد سازد.

محصول اين بررسي‌هاي طولاني‌مدّت دستيابي به باورهايي مشترك به‌عنوان مباني تأسيس قرارگاه و شيوه‌هاي مبارزه و جهاد مي‌شود كه اهميّت فراواني دارد. ديدگاه‌ها به هم نزديك شده و نظرات و آراي باطل به‌صورت خودكار در جريان مباحثات حذف مي‌شوند.

در نهايت همين گروه‌ها بر اساس تكاليف و وظايفي كه دارند، هر كدام بخشي از اساسنامه و چارچوب تأسيس قرارگاه را تدوين مي‌كنند؛ مباني ديني، مباني نظامي، مباني اخلاقي، مباني سايبري، راهبردهاي سخت‌افزاري، نرم‌افزاري و… نقشه وظايف و مسئوليت‌ها را بر اساس چارت سازماني طراحي شده ترسيم كرده و روابط تمامي نهادها را سازمان‌دهي و معماري مي‌نمايند.

### طراحي راهبردها و برنامه‌هاي عملياتي در چارچوب ساختار قرارگاه

پس از تصويب اساسنامه و چارچوب‌هاي فعاليت قرارگاه، كار با نصب مسئولان به‌طور رسمي آغاز مي‌شود و گروه‌هاي جديدي شكل مي‌گيرند تا در همان فضاي ترسيم شده به طراحي راهبردها و برنامه‌ريزي بپردازند. اين گروه‌ها در سراسر جهان گسترده بوده و ممكن است اعضاي آن در نقاط مختلف مكاني حضور داشته، ولي از طريق ارتباط در فضاي سايبري با هم همكاري نمايند.

1. گروه عالي تصميم‌گيري: گروهي از مديران ارشد قرارگاه كه در موضوعات كلان و استراتژيك سايبري تصميم‌گيري مي‌كنند. اين گروه شامل افرادي با تخصص‌هاي مختلف (امنيت سايبري، حقوق، امور نظامي، فن‌آوري اطلاعات) است.
2. گروه‌هاي تحليل تهديد (Threat Intelligence): شناسايي و تحليل تهديدات سايبري، روندها و حملات احتمالي
3. گروه‌هاي واكنش به حوادث سايبري (Incident Response Team): واكنش فوري به حملات سايبري، شناسايي، تشخيص و مقابله با تهديدات و حوادث در سريع‌ترين زمان ممكن، كمك به بازگرداندن سيستم‌ها به وضعيت عادي و انجام بازيابي از داده‌هاي آسيب‌ديده
4. گروه‌هاي امنيت شبكه (Network Security Team): طراحي، پياده‌سازي و نگهداري از سيستم‌هاي امنيتي شبكه‌ها و زيرساخت‌هاي ديجيتال، نظارت مستمر بر ترافيك شبكه و شناسايي آسيب‌پذيري‌هاي احتمالي، مديريت ابزارهاي امنيتي مانند فايروال‌ها
5. گروه‌هاي مقابله با تهديدات پيشرفته (Advanced Persistent Threats - APT): شناسايي و مقابله با تهديدات پيچيده و مداوم كه معمولاً هدف‌شان سازمان‌هاي دولتي يا زيرساخت‌هاي حياتي است، تحليل و شبيه‌سازي حملات پيشرفته و طراحي استراتژي‌هاي دفاعي عليه آن‌ها، پاسخ به حملات APT و متوقف كردن نفوذ مهاجمان پيشرفته
6. گروه‌هاي قانوني و حقوقي (Legal and Compliance Team): نظارت بر مسائل حقوقي و تطابق اقدامات قرارگاه با قوانين ملي و بين‌المللي، مشاوره حقوقي در خصوص مسائل قانوني مرتبط با حملات سايبري
7. گروه‌هاي آموزش و فرهنگ‌سازي (Training and Awareness Team): طراحي و اجراي برنامه‌هاي آموزشي براي تيم‌هاي قرارگاه سايبري، آگاهي‌بخشي به ساير بخش‌ها و كاركنان در خصوص تهديدات سايبري و نحوه پيشگيري از آن‌ها، شبيه‌سازي‌هاي حملات سايبري و آموزش عملي، برنامه‌ريزي آموزش‌هاي عمومي اجتماعي
8. گروه مديريت داده‌ها و اطلاعات (Data Management): ذخيره‌سازي، تحليل و مديريت داده‌هاي به‌دست آمده از حملات و تهديدات، پايش اطلاعات و تطابق آن‌ها با سياست‌ها و پروتكل‌هاي امنيتي، به‌روزرساني مستندات و گزارش‌هاي حوادث
9. گروه فناوري اطلاعات و زيرساخت‌ها (IT Infrastructure): تأمين و نگهداري از زيرساخت‌هاي فناوري اطلاعات قرارگاه، پشتيباني از سيستم‌هاي داخلي، نرم‌افزارها و سخت‌افزارهاي مورد نياز
10. گروه‌هاي همكاري بين‌المللي و هماهنگي (International Coordination Team): تعامل با ساير كشورهاي هم‌پيمان، سازمان‌هاي بين‌المللي و نهادهاي مختلف در خصوص همكاري‌هاي سايبري مشترك، همكاري در جهت تبادل اطلاعات و پيشگيري از تهديدات جهاني، هم‌افزايي با نهادهاي بين‌المللي براي مقابله با حملات سايبري
11. گروه‌هاي مديريت هوش مصنوعي (AI): تجهيز و نصب ابزارهاي هوش مصنوعي، مديريت داده‌ها، آموزش نيروها و گروه‌هاي ديگر براي استفاده از هوش مصنوعي، توليد گزارش‌هاي هوش مصنوعي و آينده‌پژوهانه
12. گروه‌هاي رصد و پايش فضاي مجازي (Monitoring): جمع‌آوري و تحليل داده‌هاي آشكار فضاي مجازي، پيام‌رسان‌ها، خبرگزاري‌ها و سامانه‌هاي عمده توليد و آرشيو محتوا و اطلاعات، توليد گزارشات متنوّع آماري و نموداري از داده‌ها
13. گروه بازرسي، نظارت و ارزيابي: نظارت كلي بر عملكرد قرارگاه و ارزيابي كيفيت عمليات، شفاف‌سازي اهداف، سياست‌ها و برنامه‌ها، ارزيابي و گزارش‌دهي به مقامات عالي‌رتبه
14. گروه ارتباطات و هماهنگي داخلي: تسهيل دسترسي تمامي گروه‌ها به اطلاعات مورد نياز و ارتباط با يكديگر، به‌گونه‌اي كه هماهنگي و ارتباط ميان گروه‌ها به راحتي امكان‌پذير باشد.

محصول فعاليت اين گروه‌هاي همفكر رسيدن به جدولي از برنامه‌هاي عملياتي است كه در قالب پروژه‌هايي زمان‌دار يا پروسه‌هايي دوره‌اي و منظّم براي اجرا تدوين شده است.

## شتابدهي فعاليت‌ها از طريق همكاري برنامه‌محور

### توزيع مناسب برنامه‌ها بر اساس تقسيم كار جهاني گروه‌هاي فعّال جهادي

بر اساس چارت سازماني قرارگاه، گروهي كه مسئول تقسيم كار و هماهنگ‌سازي گروه‌ها و نيروهاي جبهه مقاومت است اين برنامه‌هاي تدوين و قطعي شده را توزيع مي‌نمايد، به‌نحوي كه از يك سو، منابع آن تأمين شود و از سوي ديگر، هماهنگ و يكپارچه به انجام برسد.

وقتي مرحله همفكري پشت سر گذاشته شده باشد، ديگر برنامه‌ها پس‌زده نمي‌شود و سليقه‌هاي مختلف از آن نمي‌كاهد. همه پيشاپيش مباني فكري آن را پذيرفته‌اند و مشكلي با اجراي آن ندارند. پس انگيزه‌هاي دروني و همدلي نيروها به‌سرعت تجميع و به‌خط مي‌گردد. اين سبب هم‌افزايي و جلوگيري از تخالف‌ها شده و كيفيّت و كميّت اجراي برنامه‌ها را افزايش مي‌دهد.

### مستندسازي و تجميع مستمر آمار و گزارش فعاليت‌ها، بازبيني و اصلاح

تمامي افراد، گروه‌ها و نهادهاي عضو قرارگاه در همان چارچوب مشخّص شده در اساسنامه و اَسناد بالادستي قرارگاه دست به مستندسازي و توليد گزارش‌هاي منظّم از فعاليت‌هاي خود مي‌كند. گروه‌هاي رصدي قرارگاه نيز حسب وظيفه تعيين شده وضعيت را شناسايي و گزارش مي‌نمايند.

تمامي اين داده‌ها جمع‌آوري و با استفاده از هوش مصنوعي تجزيه و تحليل مي‌شوند. پيوسته بر دقّت آن‌ها اضافه شده و مجدّداً ابلاغ مي‌گردند.

**فهرست مندرجات طرح**

فرمايشات مقام معظّم رهبري (حفظه‌الله)

مطالبات مقام معظّم رهبري (حفظه‌الله)

اهميّت فضاي مجازي

آسيب‌ها و مخاطرات

* تهديدات امنيتي
* تهديدات جسمي و رواني
* تأثيرات منفي بر روابط اجتماعي
* تهديدات مالي و اقتصادي

فرصت‌ها و قابليت‌ها

* دسترسي به اطلاعات و آموزش
* ارتباطات و شبكه‌سازي
* فرصت‌هاي كسب‌وكار و تجارت الكترونيك
* توسعه فرهنگي و هنري
* توانمندسازي و فعال‌سازي اجتماعي
* توسعه فناوري و نوآوري
* سلامت و پزشكي
* حكمراني و سياست
* تسهيل در فعاليت‌هاي روزمره

اهميّت هوش مصنوعي

آسيب‌ها و مخاطرات

* تهديدات امنيتي و سوءاستفاده از هوش مصنوعي
* مسائل اجتماعي و اقتصادي
* مسائل اخلاقي و انساني
* مسائل حريم خصوصي و جمع‌آوري داده‌ها
* اتكاي بيش از حد به هوش مصنوعي
* آسيب به هويت و استقلال انساني

فرصت‌ها و قابليت‌ها

* آموزش و يادگيري هوشمند
* تحقيق و توسعه (R&D)
* امنيت و دفاع
* حمل‌ونقل و خودروهاي خودران
* پيشرفت در حوزه هنر و رسانه
* تحول در حوزه‌هاي پزشكي و سلامت
* ارتقاي بهره‌وري در صنايع
* تحول در صنعت خدمات مالي و بانكداري
* مديريت منابع طبيعي و محيط زيست
* پيشرفت در كشاورزي

رويكرد سايبري به مسئله فلسطين و محور مقاومت

آسيب‌ها و مخاطرات

* حملات سايبري به زيرساخت‌هاي حياتي
* دستكاري و انتشار اطلاعات غلط (Fake News)
* حملات سايبري به سازمان‌هاي حقوق بشري و گروه‌هاي فعال فلسطيني
* حملات سايبري به رسانه‌ها و گروه‌هاي خبري
* حملات سايبري به شبكه‌هاي اجتماعي و پلتفرم‌هاي آنلاين
* حملات به زيرساخت‌هاي اقتصادي
* حملات سايبري به سازمان‌هاي بين‌المللي
* هك و دسترسي به اطلاعات نظامي و امنيتي

فرصت‌ها و قابليت‌ها

* افزايش آگاهي جهاني و به اشتراك‌گذاري اطلاعات
* دفاع از حقوق بشر و مستندسازي نقض‌ها
* تقويت روندها و فرآيندهاي مقاومت
* كمك به فرآيندهاي ديپلماتيك و سياسي
* كمك به سازمان‌دهي و بسيج اجتماعي
* كمك به بهبود وضعيت اقتصادي و اجتماعي فلسطين
* كمك به ارتقاي آموزش و آگاهي‌سازي در فلسطين
* مقابله با سانسور و محدوديت‌ها

نقاط قوت و برتري‌ها

* توانايي در سازمان‌دهي و بسيج منابع و نيروها
* برخورداري از صداقت
* مطابقت با فطرت و ذات انساني
* در اختيار داشتن نيروهاي داراي مهارت فني
* اخلاص و نيّت الهي
* امداد و ياري پروردگار
* فداكاري و توانايي عبور از خود

نقاط ضعف و كاستي‌ها

* محدوديت‌هاي دسترسي به اينترنت و فناوري
* كمبود منابع مالي براي استفاده از ابزارهاي پيشرفته
* حملات سايبري و تهديدات امنيتي
* عدم يكپارچگي و هماهنگي در استفاده از فضاي سايبري
* مشكلات در توليد و مديريت محتواي ديجيتال
* محدوديت در دسترسي به پلتفرم‌ها و رسانه‌هاي جهاني
* عدم درك كامل از اصول امنيت سايبري

ضرورت‌هاي تأسيس قرارگاه سايبري

اهداف و مأموريت‌هاي قرارگاه سايبري

الزامات تأسيس قرارگاه سايبري

* الزامات فني
* الزامات انساني
* الزامات امنيتي
* الزامات مديريتي
* الزامات فرهنگي
* الزامات مالي و منابع

مراحل تأسيس قرارگاه سايبري

تجميع انگيزه‌ها از طريق همدلي ايمان‌محور

* برگزاري نشست‌هاي اوليه و ايجاد گفتمان نياز به قرارگاه متمركز
* برگزاري گردهمايي مشترك نمايندگان تمامي گروه‌هاي مقاومت

همسوسازي ديدگاه‌ها از طريق همفكري پژوهش‌محور

* تشكيل گروه‌ها و كميته‌هاي همكاري علمي در راستاي طراحي ساختار قرارگاه
* طراحي راهبردها و برنامه‌هاي عملياتي در چارچوب ساختار قرارگاه

شتابدهي فعاليت‌ها از طريق همكاري برنامه‌محور

* توزيع مناسب برنامه‌ها بر اساس تقسيم كار جهاني گروه‌هاي فعّال جهادي
* مستندسازي و تجميع مستمر آمار و گزارش فعاليت‌ها، بازبيني و اصلاح