نقش لاتروریسم در ایجاد هژمونی جهانی تروریسم سایبری دشمن

هنگامی که به گستره و عمق تسلط جهانی کشورهای آنگلوساکسون در نبردگاه سایبر دقت می‌شود، جدا از همه شقوق و نتایج حاصل، این سؤال مطرح می‌گردد که «چگونه متولیان فضای سایبر موفق شده‌اند در حدود صد سال، چنین تسلط بی‌بدیلی بر سراسر کشورها و ملل جهان به نفع خود ایجاد نمایند؟»

در واقع نه تنها در حوزه سایبر بلکه در تمامی حوزه‌ها نظیر زبان، سیاست، اقتصاد، رسانه، پیمان‌های نظامی، هنر و سینما و ... این تسلط جهانی آنگلوساکسون‌ها دیده می‌شود.

نقطه مشترک تمامی موارد فوق و دیگر مواردی که اگر بررسی شود، باز هم همین اشتراک را دارند، «قوانین یکسان و جهان شمول» است. در واقع غرب صهیونیستی با وضع قوانین جهانی و القای آنها به همه کشورهای جهان زمینه‌ای ایجاد نموده که اگر مخالف نظراتشان حرف زده شود، به مثابه مخالفت با تمامی جامعه جهانی است حال آنکه قوانین توسط ملل جهان وضع نشده بلکه توسط آمریکا و انگلیس در صد سال گذشته بنا گشته است.

یک نمونه اصلی و بسیار مهم قانون‌گذاری جهانی انگلیسی – آمریکایی، «سازمان ملل متحد» است که در واقع نه تنها مرجعی برای شنیده شدن صدای مردم جهان نیست بلکه در راستای اهداف آنگلوساکسون‌ها، دیگر کشورهای مخالف را محکوم کرده، علیه آنها قطعنامه تصویب می‌کند و حتی در شورای امنیت سازمان ملل برای آنها پرونده‌سازی می‌کند.

سازمان ملل متحد

نمونه پرونده هسته‌ای ایران در شورای امنیت سازمان ملل از این دست موارد است.

اما نکته حائز اهمیت این است که قوانین بظاهر ضد تروریستی جهان توسط کشورهایی بنا شده که خودشان تروریست بالذات هستند و در تاریخ جهان خصوصاً یک قرن اخیر، هر جنگی که شروع شده، یا مستقیماً یک طرف آن آمریکا و انگلیس بوده است و یا به نوعی در شروع آن و طولانی شدن مدت زمان جنگ نقش داشته‌اند.

بر اساس مکتب سوم امنیت که به مکتب «فرصت طلب» شهرت دارد و ویژه آمریکایی‌هاست، شیوه اقدام آنگلوساکسون‌ها بر این است که هر گاه تهدیدی علیه‌شان رخ دهد آن را به فرصت تبدیل می‌کنند. اما اشکال بزرگ این نگاه اینست که اگر تهدیدی در واقع وجود نداشته باشد، خودشان بصورت پشت پرده ایجاد تهدید نموده و سپس در ظاهر به مبارزه با آن می‌پردازند تا فرصت مد نظر را پدید آورند.

نمونه بارز این امر، حادثه یازده سپتامبر ۲۰۰۱ است که دولت آمریکا آن را طراحی و اجرا نمود ولی بعد حمله را به گردن طالبانی انداخت که خودش طراح و تغذیه‌کننده آن بوده و سپس با این بهانه به منطقه جنوب غرب آسیا و کشورهای افغانستان (۲۰۰۱) و عراق (۲۰۰۳) لشکرکشی نمود.

مصداق این رویه کلی در فضای سایبر جهانی نیز وجود دارد. تمامی قوانین جهانی سایبر، چه آن دسته که توسط آمریکا در سازمان ملل وضع شده و چه دسته‌ای که با فشار انگلیس در اتحادیه اروپا به تصویب رسیده، در امتداد چنین روندی است.

در نوع آنگلوساکسون، پنج سازمان موسوم به پنج چشم، هر گاه با اعتراضات شدید مردم و دیگر دولت‌ها مبنی بر جاسوسی بی حد و حصر و البته غیر قانونی روبرو شده‌اند، بلافاصله مسئله تهدیدات امنیتی و اقداماتا تروریستی علیه خودشان را مطرح کرده‌اند و به دنبال آن قانونی جدید در راستای بیشتر باز شدن دستشان برای ادامه جاسوسی جهانی مصوب نموده‌اند در حالی که نه تنها اقدام تروریستی بر ضدشان صورت نگرفته بلکه خودشان بزرگترین تهدید تروریستی علیه تمامی ملل جهان در فضای سایبر و اطلاعات جهان هستند.

از حقوق مسلم و مکتوب شهروندان کشورهای اروپای غربی و آمریکا اینست که حریم خصوصی‌شان باید توسط دولت و دیگر افراد حفظ شود. یعنی اشاره صریح بر اصل منع جاسوسی از شهروندان! اما هیچگاه این قانون نه تنها رعایت نشده بلکه صراحتاً توسط خود دولت‌ها نقض گشته است. این نقض قانون و اصطلاحاً «شیوه دور زدن قانون» تنها از طریق خودزنی‌ها و خود دسیسه‌چینی در حوزه تروریسم سایبری میسر شده است.

بعنوان نمونه، گزارش قانون جرایم سایبری مصوب ۱۹۹۱ اتحادیه اروپا بیان می‌دارد: «این گزارش تحت یک قرارداد با کمیسیون اروپایی آماده شد. با آنکه این مطالعه بطور خاص بر روی تروریسم رایانه‌ای متمرکز نبود، اما سهم عمده‌ای از آن به درک آسیب‌پذیری فناوری‌های اطلاعاتی نسبت به فعالیت‌های مجرمانه اختصاص داشت.»

یعنی با آنکه تا پیش از ۱۹۹۱ هیچ عملیاتی در چهارچوب سایبر تروریسم علیه اتحادیه اروپا شکل نگرفته بود و بالاترین سطح خرابکاری‌ها در حوزه هکتیویسم و توسط افراد غیر دولتی بوده است، اما از همان موقع به دنبال زمینه‌سازی تصویب قوانین ضد تروریسم بوده‌اند!

در اکتبر ۱۹۹۹ TSEU به این نتیجه رسید که جرایم فناوری‌های سطح بالا[1] باید در توافقات مربوط به تعریف و تصویب قوانین مشترک لحاظ شود. یک سال بعد شورای اروپایی طرح عملیات جامعی تدوین کرد که در آن بر اهمیت شبکه و مبارزه با تروریسم رایانه‌ای تأکید شده بود در حالیکه هنوز تا آن زمان گزارشی مبنی بر وجود عملیات‌های واقعی انجام شده تروریستی در حوزه سایبر علیه مواضع سایبری اروپا تنظیم نشده بود.

متن مصوب سال ۲۰۰۱ اتحادیه اروپا در حوزه امنیت سایبر اعلام می‌دارد: «مناطق عضو باید مطمئن شوند که طبقات داده‌های زیر حتماً نگهداری می‌شوند:

۱- نشان دادن منبع و مقصد یک ارتباط

۲- شناسایی تاریخ، زمان و دوره یک ارتباط

۳- شناسایی نوع ارتباط

۴- شناسایی وسیله ارتباطی

۵- شناسایی محل تجهیزات ارتباطی متحرک.»

شیوه توهم توطئه آگاهانه که منجر به طراحی دشمن فرضی شود، نهایتاً به این شکل زمینه قانون‌گذاری را مهیا کرده است که در سال ۲۰۰۱ بطور رسمی در متن قانون اتحادیه اروپا، بر خلاف قانون «حفظ حریم خصوصی شهروندان» قانون امنیتی مصوب گردد و همه کشورهای عضو ملزم به اجرای آن شوند.

با این روش نه تنها اعتراضی نسبت به نقض آشکار قوانین ملی کشورها از سوی شهروندان صورت نمی‌پذیرد بلکه با زمینه‌چینی روانی که توسط طراحی دشمن فرضی و تروریسم خیالی برای آنها شده است، مردم قبول می‌کنند که به جهت افزایش توان مقابله دولتشان با تروریسم سایبری، هر اقدامی حتی جاسوسی از خودشان در دستور کار قرار داشته باشد.

نقش بی‌بدیل لاتروریسم[۲] و قانون به شکلی که بیان شد در افزایش توان تسلط جهانی به کشورهای آنگلوساکسون یاری می‌رساند.

باز به عنوان نمونه، مورد دیگری از نقض قانون توسط اتحادیه اروپا ارائه می‌شود.

در بخشی از قانون مصوب اتحادیه اروپا در ۱۹ مارس ۱۹۹۸ بیان شده: «شورا، کشورهای عضو را به پیوستن به «گروه هشت»[۴] شبکه ۲۴ ساعته مبارزه جرم‌های فناوری سطح بالا دعوت می‌کند. در مذاکرات گروه هشت درباره جرم‌های فناوری سطح بالا دو دسته‌بندی مهم از تهدیدها مشخص شده‌اند:

۱- تهدید در برابر زیرساخت‌های رایانه‌ای که اختلال، ممانعت، تنزل رتبه یا ویران کردن اطلاعات موجود در رایانه‌ها، شبکه‌های رایانه‌ای را باعث می‌شود

۲- تهدیدهایی با همیاری رایانه (به این منظور که نوع خاصی از جرائم مثل سیاسی یا اقتصادی به کمک فضای سایبر تسهیل و اعمال گردد).»

عوامل اتحادیه اروپا خصوصاً انگلیس در حالی در سال ۲۰۰۹ (۱۳۸۸) با استفاده از فضای سایبر و ابزار رسانه، به تسهیل در امر وقوع کودتای مخملی در ایران و ایام فتنه ۸۸ بصورت تمام وقت و با تمام قوا و هزینه کمک کردند که یازده سال قبل از آن، هرگونه اقدام از این طریق را غیر قانونی انگاشته‌اند.

پس ملل جهان خصوصاً جمهوری‌اسلامی ایران، کاملاً با دولت‌های تروریستی مواجه است که برای تأمین امنیت خود حتی اقداک به ساخت تروریست‌های فرضی می‌کنند ولی برای از بین بردن امنیت دیگر کشورها نه تنها نقض قوانین خود مصوب را بد نمی‌دانند بلکه خودشان در نقش یک تروریست تمام عیار ظاهر می‌شوند.

مواردی که ارائه شد از دوایر قانونی اتحادیه اروپا در حوزه سایبر تروریسم است و نکته اینست که اتحادیه اروپا تحت لوای پنج چشم با حد پایین‌تری از خطرسازی برای دیگران اقدام می‌کند. در واقع موارد بیان شده، حد میانه تهدید است. تهدید اصلی در نبردگاه سایبر از سوی عوامل پنج چشم است که برای ایجاد تسلط کامل بر سراسر جهان، گستره آبی – حاکی زمین را میان خودشان تقسیم نموده و هر کدام به تحت نظر داشتن مداوم منطقه مشخص شده پرداخته‌اند.

هر چند که در مورد حدود تعیین شده هر کدام از این ۵ سازمان، میان کارشناسان اختلاف نظر وجود دارد اما همگی متفق القول باور دارند که پهنه جهان بواقع میان سیستم‌های جاسوسی سایبری پنج چشم تقسیم‌بندی شده است.

بطور خاص در منطقه جمهوری‌اسلامی ایران، کشور عمان میزبان یکی از پایگاه‌های اشلون در منطقه است و البته در بررسی‌های مستمر، وجود پایگاه اشلون در چند کشور دیگر از منطقه به اثبات رسیده است.

۱- High Tech

۲- Law Terrorism