جاسوسی در روابط دیپلوماتیک

(جاسوسی سنتی و سایبری)

تهیه و ترتیب: عبدالمنیر احمدی

1393

فهرست مطالب

مقدمه

حقوق دیپلماتیک و کنسولی تامین کننده روابط سیاسی خارجی کشور ها و حقوق مربوط به سفارت خانه ها و کارمندان آن است. و ظایف و صلاحیت های سفراء به طور کلی دراسناد بین المللی به ویژه کنوانسیون وین در مورد روابط دیپلماتیک به این موضوع پرداخته است. یکی از وظایف نماینده های دولت های فرستنده در دولت پذیرنده جمع آوری اطلاعات و ارایه راپور به دولت متبوع نماینده های دولت می باشد.

اما در روابط بین المللی دولت ها به طور غیر قانونی به جمع آوری اطلاعات مخفی و یا اطلاعات به شیوه های غیر قانونی می پردازند و و به اشکال مختلف جاسوسی می کنند که خود خلاف موازین حقوق بین المللی است.

جاسوسی هم در ساده ترین تعریف آن، عبارت است از عمل شخصی که با عناوین غیرواقعی و تقلب، اقدام به کسب اطلاعات، نقشه ها یا مدارک و اسناد مخفی و محرمانه کرده و اسرار نظامی، اقتصادی و سیاسی را تسلیم کشور بیگانه کند.

همچنین خیانت به کشور عبارت است از: سوء قصد علیه امنیت کشور به وسیله ایجاد ارتباط با کشور دیگری که دارای سلطه و استقلال است.

با در نظرداشت تعریف فوق، اهمیت جاسوسی در روابط دیپلماتیک کشور ها برای ما معلوم میشود و نیاز است تا دولت ها در برابر جاسوسان خارجی حمایت شوند.

من مطالب زیادی درین زمنیه نیافته و نیاز دیدم تا درین زمنیه به گونه دقیق و ریشه یی تحقیق نمایم و از منابع معتبر علمی و ویب سایت های مشهور انترنتی به عنوان منابع این تحقیق استفاده نموده ام.

درین رساله کوچک که حاوی سه فصل می باشد، ابتداء به کلیات و فصل دوم به جاسوسی در روابط دیپلوماتیک، متعاقباً در فصل سوم به جاسوسی سایبری میپردازیم.

فصل اول: کلیات

دیپلوماسی و روابط بین الملل، مفاهیمی چون جاسوسی و سایبر از عمده ترین مفاهیم کلی است که درین فصل به آن توجه شده است و به ترتیب در مباحث اول، دوم و سوم مورد مطالعه قرار میگیرد.

مبحث اول: مفهوم دیپلوماسی

واژه دیپلوماسی به معنی هدایت روابط بین افراد، گروهها و ملتها از جمله واژه‌های سیاسی مورد استفاده در عرصه مناسبات بین المللی است. دیپلوماسی (Diplomacy) در کاربرد رسمی خود عمدتاً به دیپلوماسی بین‌المللی که هدایت روابط بین المللی از طریق دیدار و گفت وگوهای دیپلمات های رسمی است اشاره دارد. در گذشته دیپلوماسی بین کشورها بیشتر به موضوعاتی همچون روابط شخصی و خانوادگی پادشاهان دو کشور با یکدیگر یا مسئله جنگ و صلح مربوط می شد، اما در شرایط کنونی جهان علاوه بر آنها موضوعاتی همچون روابط تجاری، مناسبات فرهنگی و علمی نیز در محور مباحثات دیپلماتیک بین کشورهای مختلف با یکدیگر و بین آنها با سازمانهای بین المللی قرار گرفته است.

دیپلوماسی در واقع مجری سیاست خارجی در چارچوب دکترین سیاست خارجی هر کشور است. دکترین سیاست خارجی یک کشور که معمولاً یک بیان کلی از سیاست خارجی آن محسوب می شود توسط رئیس حکومت یا وزیر امور خارجه اعلام می شود.

اهداف دکترین سیاست خارجی هر کشور ارائه اصول کلی برای هدایت سیاست خارجی و انجام دیپلوماسی است. این اصول به رهبری سیاسی یک کشور اجازه می دهد تا با وضعیت های مختلف پیش آمده به طور مناسب برخورد نماید و رفتار کشور در برابر سایر کشورها را توضیح دهد.

اجرای دیپلوماسی بر عهده گروهی که "هیأت دیپلوماتیک" نامیده می شود قرار دارد. این گروه نماینده رسمی کشور فرستنده آنها نزد کشور پذیرنده و میزبان تلقی می شوند. وظیفه هیأت دیپلوماتیک حفظ منافع دولت و شهروندان کشور فرستنده نزد دولت پذیرنده است. البته این امر در چارچوب مرزهای مجاز توسط حقوق بین الملل، انجام مذاکره با مقامات دولت طبق اصول مشخص شده توسط دولت فرستنده و از طریق سایر شیوه های قانونی که دولت پذیرنده آنها را به رسمیت شناخته صورت می گیرد.

هیأت دیپلوماتیک یک کشور نزد کشور دیگر تمامی فعالیت های خود را که برای تقویت روابط دوستانه بین دو کشور و نیز توسعه مناسبات سیاسی، اقتصادی، فرهنگی و علمی بین آنها انجام می دهد به دولت متبوع خود گزارش می کند. ریاست هیأت دیپلوماتیک یک کشور در کشور دیگر نیز بر عهده سفیر یا کنسول است.

یکی از نکات مهم در مناسبات دیپلماتیک بین کشورها با یکدیگر و یا بین آنها با سازمان های بین المللی به رسمیت شناخته شدن مصونیت دیپلماتیک برای سفیر و سایر اعضای کادر دیپلماتیک است. در این چارچوب دولت میزبان به سفیر یا کنسول به عنوان رئیس هیأت دیپلماتیک در یک کشور دیگر اجازه می دهد تا بخشی از خاک کشور او را که سفارتخانه یا کنسولگری نامیده می شود اداره کند. همچنین مکان، کارمندان و حتی خودروهای هیأت دیپلماتیک نیز در برابر بسیاری از قوانین کشور پذیرنده از مصونیت برخوردارند.

مصونیت دیپلماتیک یک نوع مصونیت قانونی است که کشورها به منظور تضمین انجام وظایف هیأت های دیپلماتیک بدون نگرانی از تحت تعقیب قرار گرفتن توسط کشور میزبان به آنها اعطا می کنند. اگرچه این نوع از مصونیت از سابقه دیرینه ای در حقوق بین المللی برخوردار است اما در سال 1961 با امضای کنوانسیون روابط دیپلماتیک وین به صورت اصول موضوعه حقوق بین الملل درآمده است.[1]

[1]. ر.ک به: ویب سایت: http://www.hamshahrionline.ir/details/28738

مبحث دوم: مفهوم جاسوسی

جاسوسی به معنی گماردن فرد یا وسیله ویا هرشی دیگر برای بدست آوردن اطلاعاتی که به نوعی برای صاحب آن ارزشمند بوده و تلاش میکند تاآن را حفظ کند می باشد قدمت جاسوسی بسیار طولانی بوده ویکی از روشهای بسیار کارآمد برای بدست آوردن ماهیتها و نظرات و اهداف غیر می باشد بطور مثال یک فردی دارای صندوقچه اي مخفی جهت نگهداری اسناد و مدارک و پول درون منزل و یا شرکت خود می باشد، سارقان با گماردن جاسوس(عامل داخلی) و یا تعقیب سوژه سعی بر به دست آوردن مشخصات صندوقچه، نوع قفل، محل اختفا ونوع کلید ونوع ضریب حفاظتی آن می باشند تا بعد از بدست آوردن اطلاعات لازمه دریک عملیات غافلگیرانه ویا ورود عدوانی ویا ورود پنهان با همکاری عامل داخلی به آن دستبرد زده و محتوای آن را بربایند.[1]

با این حال وقتی سخن از جاسوسی به میان می آید ذهن عامه مردم - که اطلاعات کمی از جزئیات این جرم دارند - بیشتر متوجه شبکه ها و سازمان‌های جاسوسی معروف کشورهای مختلف از جمله سیا در آمریکا، MI5و MI6 در انگلستان، موساد در اسرائیل و کا جی بی در اتحاد جماهیر شوروی سابق می شود.

برخی از این سازمان ها، مثل سیا ضمن استخدام جاسوس تا حد زیادی به شکل خودمختار از قوه اجراییه عمل کرده و گاهی حتی دست به عملیات هم می زنند. با این حال نباید تصور کرد که جاسوسی در سطح دنیا محدود به این سازمان‌ها می‌شود بلکه کشورهای مختلف و حتی افراد و سازمان های گوناگون دست به جاسوسی می زنند.

در دهه 80 میلادی که به دلیل رشد ارتکاب این جرم در این دهه آن را «دهه جاسوسی» نامیده اند، حدود 500 کتاب در مورد جاسوسی توسط مورخان، روزنامه نگاران، تحلیل گران نظامی، سیاستمداران و تا حد کمتری حقوق دانان و جرم شناسان نگاشته شده است.

1. تعریف جاسوسی

جاسوسی به عمل شخصی گفته می شود که با عناوین غیرواقعی و تقلب، اقدام به کسب اطلاعات، نقشه‌ها یا مدارک و اسناد مخفی و محرمانه کرده و اسرار نظامی، اقتصادی و سیاسی را تسلیم کشور بیگانه کند. همچنین خیانت به کشور عبارت است از: سوء قصد علیه امنیت کشور به وسیله ایجاد ارتباط با کشور دیگری که دارای سلطه و استقلال است.

2. اصطلاحات جاسوسی

أ. **عامل:** فردی است که از منبع یا منابع، اطلاعات را جمع آوری کرده و به استخدام یک سرویس اطلاعاتی در آمده ولی عضو رسمی آن سرویس نیست.ممکن است تعداد عوامل زیاد باشند که در سلسله مراتب یکدیگر قرار داشته و رده بالای آنها به عنوان سر عامل رده پایین تر درنظر گرفته می شوند. از عاملین ممکن است صرفاً در جهت جمع آوری اطلاعات استفاده نشود. بسته به نوع کارایی عامل‌ها پسوندهایی مانند نفوذی، فریب، نشان، مشاور و. . . به عامل اضافه می شود .

ب. **افسر یا رهبر سر شبکه:** عنصری است اطلاعاتی که هدایت و رهبری چندین شبکه جاسوسی مرتبط با هم را عهده دار است

ت. **مرکز یا ستاد:** محل تصمیم سازی و تصمیم گیری عملیات های یک سرویس جاسوسی است و به آخرین رده سلسله مراتب سازمان اطلاعاتی گفته می‌شود.

ث. **پوشش:** فعالیت جاسوسی به نحوی تغییر شکل داده و تحت شرایطی انجام می‌شود که کاملاً عادی و موجه به نظر آید و متناسب با محیط طبیعی استفاده کننده باشد؛ به‌عبارت دیگر اقدامات طرح ریزی شده‌ای که به فرد جاسوس اجازه می دهد عملی را که نمی تواند به طور آشکار انجام دهد بدون برانگیختن شک و گمان انجام دهد. به طور کلی و عام، پوشش به دو نوع قانونی(رسمی) و غیرقانونی(غیررسمی) تقسیم می‌شود:

1. **پوشش قانونی:** ورود عوامل جاسوسی به عنوان عناصر سیاسی یا دیپلماتیک دارای مصونیت به هدف مورد نظر جهت جاسوسی را بهره گیری از پوشش قانونی گویند. در اینگونه موارد عامل جاسوسی را مقیم قانونی و مکان فعالیتش در سفارتخانه، کنسولگری، دفاتر وابستگی و ... را ایستگاه قانونی می نامند.

[1]. ر.ک به: ویب سایت: http://kohnesarbazeirani.blogfa.com/post-68.aspx

2. **پوشش غیرقانونی:** ورود عامل جاسوسی بدون بهره مندی از مصونیت سیاسی یا دیپلماتیک را پوشش غیرقانونی نامند. در اینگونه موارد عامل جاسوسی را مقیم غیرقانونی و مکان فعالیتش مانند دفاتر شرکتی، نمایندگی‌ها، اماکن باستانی یا توریستی، هتل‌ها و. . . را ایستگاه غیرقانونی می نامند.

ج. **افسر یا رهبر عملیات:** شخصی است اطلاعاتی که عضو سازمان اطلاعاتی بوده و مسئولیت هدایت و رهبری عامل یا عاملین جاسوسی را عهده دار است.

ح. **شبکه جاسوسی:** به مجموع افسر یا افسران عملیات و عامل یا عواملی که درگیر عملیات جاسوسی مشخص هستند اطلاق می شود که بر حسب تعداد افسران عملیات یا عاملین جاسوسی متفاوت است.

3. انگیزه های جاسوسی

أ. **ایدئولوژیک:** هیچ جاسوسی در مقایسه با عاملی که دارای انگیزه های عقیدتی باشد به طور بالقوه چندان سودمند نیست. ایدئولوژی و مکتب انگیزه‌ای الزام آور و دائمی بوده و به عنوان پایدارترین انگیزه تلقی می شود. جاسوسی که متأثر از انگیزه‌های مثبت ایدئولوژیکی است به دلیل پایبندی به موضوعی خاص همچون حزب یا خط سیاسی، مذهب، کیش و آیین معین حاصل می‌شود. البته مکاتب و ایدئولوژی‌ها جنبه منفی را نیز می توانند دارا باشند چه بسا مکاتب در مواردی خاص، سرمنشأ خیانت‌ها می شوند. جاسوس مکتبی تنها هنگامی که نظام عقیدتی خود را در آستانه فروپاشی ببیند در مورد خود و آنچه می کند و کسانی که برایشان کار می کنند، دچار تردید می‌شود.

ب. **تطمیع:** پول ابزار سودمند هر سازمان جاسوسی است و هرگاه مدبرانه از آن استفاده شود. چه بسا موجب خرید اطلاعاتی بسیار ارزشمند شود. گرچه اطمینان به جاسوسان حریص همواره از سوی سرویس‌ها مورد تردید است ولی پول به‌عنوان انگیزه مستقل و مکمل، مورد استفاده سرویس‌ها قرار گرفته و می گیرد.

ت. **شیفتگی به فرهنگ بیگانه:** دسته ای از افراد بدون بررسی و کورکورانه تحت تأثیر فرهنگ بیگانه قرار گرفته و هیچ هدفی جز پیاده کردن ارزش هایی که به صورت نظری یا شعار از سوی آن فرهنگ‌ها القا می شود، ندارند.

ث. **عشقی، عاطفی:** در برخی فرهنگها، زمانها و موقعیت ها، عشق انحرافی، انگیزه‌ای بی همتا برای جاسوسی است و هرگاه از آن زیرکانه بهره گرفته شود دست کم به اندازه ترس مطلق، اثربخش و پرقدرت است اما تأثیر آن دوام بیشتری خواهد داشت. این انگیزه در افراد ساده لوح که اسیر عشق های واهی و خیالی شده اند و همچنین افرادی که فاقد تقید مذهبی هستند بسیار مؤثر است.

ج. **شانتاژ:** به بهره گیری از نقاط ضعف عامل در جهت اجبارش برای انجام فعالیت جاسوسی شانتاژ گویند. ترس، انگیزه پنهان افراد بسیاری است که به دیگر جاذبه های پرزرق و برق تن در نداده اند. ترس ابزار پرقدرت استخدام است به ویژه اگر با ظرافت و مدبرانه به کار گرفته شود. ترس اعم از نوع پیچیده یا آشکار آن یکی از قدیمی ترین شیوه‌های کار و به صرفه اقتصادی جهت جاسوسی است.

در بسیاری از سرویس های جاسوسی، مهم ترین سلاح، ترس است. ترس ماهیت افراد را دگرگون کرده و وجدان را بی اثر می سازد. اصل بهره وری عملیاتی از ترس، در این واقعیت نهفته است که ترس از توان عامل جاسوس، برای عمل نمی کاهد و در برخی از شرایط حتی عملا موجب کارکرد بهتر نیز می شود.

4. انواع جاسوسی

در یکی از دسته بندی‌های کلی براساس ماهیت وجودی، جاسوسی به چهار دسته اصلی تقسیم میشود:

أ. **جاسوسی سیاسی:** هدف جاسوسی سیاسی شناخت گروه ها و احزاب سیاسی و نیروهای مؤثر در کشور و فرقه های مذهبی و رهبران آنها، مبانی آنها و روابط اینگونه نهاد ها و ایجاد تفرقه بین آنها و فتنه انگیزی است. این نوع جاسوسی موفق شده و می شود تا امنیت کشوری را به طور جدی در معرض خطر قرار دهد که مصداق های آن در جهان کنونی کم نیست.

ب. **جاسوسی اقتصادی:** اطلاعات اقتصادی، دشمن را بر حصر اقتصادی صحیح توانمند می کند که امروز به عنوان حربه ای از سوی استکبار مورد استفاده قرار می گیرد و به تعبیری می توان ادعا کرد که مبارزه با اینگونه جاسوسی در جهان امروز کم اهمیت تر از مبارزه علیه جاسوسی نظامی نیست.

ت. **جاسوسی نظامی:** هدف تجسس نظامی به دست آوردن اطلاعات و معلومات مربوط به نیروهای مسلح در زمان صلح و جنگ است. دشمن می کوشد اطلاعات دفاعی کشور را در معرض دستبرد قرار دهد و اطلاعاتی درباره انواع اسلحه‌ها و میزان آن و تعداد نیروهای مسلح و شکل سازمان بندی آن و... به دست آورد که این نوع از جاسوسی در قوانین اکثر کشورها مورد توجه قرار گرفته است.

ث. **جاسوسی علمی و صنعتی:** یکی از جنبه هایی که دشمن علیه امنیت کشور از آن استفاده می کند، اطلاع از مصنوعات علمی و اختراعات و ابتکارات نظامی و غیرنظامی است. حفظ این اطلاعات از دستبرد اجانب از وسایل مهم دفاع از کشور است زیرا دشمن با دستیابی به این قبیل اطلاعات آن را ضد کشور و مصلحت‌جامعه به کار می برد.

گاهی مواقع مطالعه سازمان های جاسوسی و اهتمام آنان در تجسس در اختراعات مخصوص و اختراعات در صنعت نظامی تعجب برانگیز است. جاسوسی صنعتی حتی فراتر از دولت‌ها و گاه میان رقبای تجاری نیز مرسوم است.[1]

اما از نظر وسایل و ابز

5. وظایف و اهداف جاسوسان و سازمان های جاسوسی

وظیفه اصلی جاسوسان و سازمان های اطلاعاتی تامین امنیت کشور خود است. هدف سازمان های اطلاعاتی از فعالیت در کشورهای دیگر معمولا دنبال کردن مقاصد زیر است:

1) شناخت کامل و کافی در خصوص نقاط قوت و ضعف حکومت ها
2) شناسایی احزاب و تشکیلات سیاسی و... موافق و مخالف دولت
3) به دست آوردن اخبار و اطلاعات برنامه های مختلف دولت
4) به دست آوردن اطلاعات نظامی و تخمین قدرت دفاعی کشور (آمار نفرات، نوع و تعداد تجهیزات نظامی و...)
5) شناسایی فردی شخصیت های مهم
6) نفوذ در مراکز علمی و تحقیقاتی
7) شناسایی و چگونگی کار در مراکز مختلف اقتصادی، فرهنگی و...

جمع آوری و به دست آوردن اطلاعات فوق به دو روش عمده صورت می گیرد:

روش اول، که همیشه مورد توجه سازمان های اطلاعاتی بوده و بیشتر هم از آن استفاده می شود، به کارگیری از عوامل انسانی (جاسوس) است، جاسوسان به دو گروه نفوذی و استخدامی تقسیم می شوند. نفوذیان کسانی هستند که از ابتدا جاسوس بوده و دوره ها و آموزش های لازم را از قبل در مراکز خود کسب نموده اند، سپس به عناوین مختلف در هر کجا که لازم باشد نفوذ کرده و عملیات خود را آغاز می کنند. استخدامیان نیز اشخاصی هستند که در جایی که کار می کنند دسترسی به اطلاعات همکاران و اداره خود دارند، این افراد ویژگی ها و شرایط لازم برای جاسوس شدن را دارند و سازمان های جاسوسی با به خدمت گرفتن آن ها اخبار و اطلاعات لازم را دریافت می کنند.

روش دوم، جمع آوری اخبار، جاسوسی با استفاده از وسایل فنی و الکترونیکی است. با پیشرفت علم و ساخت وسایل پیچیده گوناگون و به کارگیری این ابزار در جهت جاسوسی ماموریت های گوناگونی انجام می شود. از جمله این ابزار و وسایل می توان به ماهواره، سیستم های شنود و استراق سمع، دوربین های فیلم برداری و عکاسی و... اشاره کرد.

البته سازمان های جاسوسی عمده ماموریت های خود را از طریق عوامل انسانی (جاسوس) انجام می دهند، اما در حقیقت جاسوس کیست؟

در جواب این سوال باید گفت: هر کسی اعم از هم وطن یا خارجی با هر شغلی نظیر دیپلمات، کارمند، خبرنگار، عکاس، فیلمبردار، توریست، پناهنده و... می تواند یک جاسوس باشد.

---

[1]. ر.ک به: صفحه انترنتی: http://fararu.com/fa/news/116595

عمده ترین راه های به دست آوردن اخبار و اطلاعات توسط جاسوسان با بهره گیری از شیوه های زیر است:

1) **نفوذ:** به معنی رخنه در هر اداره، ارگان و یا تشکیلاتی برای انجام مقاصد مختلف می باشد. جاسوسان معمولا پس از نفوذ و محکم کردن جاپای خود در آن محل ماموریت های متعددی را انجام می دهند، این ماموریت ها می تواند از کسب اخبار و اطلاعات تا انجام خرابکاری و ترور باشد.
2) **استراق سمع وسایل ارتباطی:** گاهی اوقات اخبار و اطلاعات طبقه بندی شده به صورت ناخود آگاه یا در اثر سهل انگاری توسط وسایل ارتباطی رد و بدل می شود، دشمن به راحتی با داشتن سیستم های نه چندان پیشرفته ای می تواند مکالمات را شنود کرده و آن ها را ضبط نماید.
3) **جاسوسی تلفنی:** بسیاری از مواقع جاسوسان حرفه ای ضمن تماس با اماکن و مراکز حساس خود را به عنوان نیروی خودی جا زده و پس از کسب اطمینان لازم از طرف مقابل با حرفه ای ترین روش ها کسب خبر نموده و حتی در برخی موارد اخبار و مسائلی را به دروغ و با نیت خصمانه القا می کنند.
4) **فیلمبرداری و عکسبرداری:** یکی از روش های جاسوسی است که جاسوس با استفاده از دوربین در فواصل گوناگون از هر چیزی که مورد نظر و توجه باشد فیلم و عکس تهیه کرده و در اختیار سازمان های خود قرار می دهد. بعضا هیچ گزارشی نمی تواند کار محتوای یک عکس را انجام دهد. دوربین های جاسوسی را در خودروها نیز می توان جاسازی کرد و هنگام عبور از نقطه مورد نظر عکسبرداری نمود. برخی از دوربین های جاسوسی بسیار کوچک است و در هر جایی مخفی می شود، حتی به شکل خودکار، انگشتر و... بوده و جاسوس در فرصت مناسب با کمک آن عکسبرداری می کند. جالب اینجاست که کیفیت عکس این دوربین ها بسیار بالا می باشد.
5) **میکروفن گذاری:** در مکان های مهم نظیر دفاتر اشخاص مهم سیاسی و فرماندهان نظامی، سالن اجلاس، سفارتخانه ها و... وجود یک میکروفن در حکم حضور یک جاسوس است. میکروفن گذاری از جمله اقدامات سازمان های جاسوسی بوده که با استفاده از عوامل نفوذی یا استخدامی در هر محلی که مورد نیاز باشد اقدام به نصب سیستم های شنود می کنند. میکروفن ها بیشتر اوقات به صورت حرفه ای کار گذاشته می شود، بعضی از مواقع نیز میکروفن را در اشیایی که باعث جلب توجه نشود مخفی یا جاسازی می کنند. این میکروفن ها به صورت سیم دار یا بی سیم کار کرده و بسیاری از آنها قادر به ضبط مکالمات هستند.

روش های ذکر شده جزء مهم ترین تاکتیک های جاسوسی بوده، البته بسیاری اصول دیگر نیز برای جاسوسی وجود دارد که عملا مورد استفاده جاسوسان است.

از جانب دیگر در وضعیتی که کشور ها با سوء استفاده از مصونیت های دیپلوماتیک به جاسوسی میپردازند و اطلاعات را به شیوه های غیر مشروع بدست میاورند جداً امنیت اطلاعات در خطر بوده و چالشهای فراروانی را ایجاد کرده و ازینجاست که ضرورت توجه به امنیت اطلاعات مطرح میشود.[1]

طریقه برخورد کشورها با جاسوسان متفاوت است گاهی جاسوس، به دلیل برخورداری از مصونیت دیپلماتیک، عنصر نامطلوب اعلام شده و اخراج می شود و گاهی وی دستگیر و بلافاصله مجازات شده و گاهی نیز با دادن اطلاعات غلط به او سعی در گمراه کردن کشور مورد نظر می‌شود.

برخی از کشورها نیز سعی می کنند جاسوس را به جای مجازات کردن، به یک جاسوس دوجانبه تبدیل کنند و از او بخواهند که به آنها اطلاعات بدهد و در مقابل، برای لو نرفتن او، گاهی اطلاعات به اصطلاح سوخته ای را نیز جهت ارائه به کشور دیگر در اختیار وی میگذارند. بدین ترتیب در حالی که کشور اول این فرد را جاسوس خود می داند وی در واقع برای کشور دوم جاسوسی می کند.[2]

جاسوسی از نقطه نظر شکلی به گونه های مختلف تقسیم میشود، اما با پدید آمدن انترنت، از نقطه نظر روشی و یا ابزاری، شیوه جدید جاسوسی تحت عنوان جاسوسی سایبری را بوجود آورد که آثار مخربی برای دولت ها و اطلاعات شان در پی داشت که طی مطالب بعدی به آن میپردازیم.

---

[1]. ر.ک به: صفحه انترنتی: http://ahaad.ir/s/9871
[2]. ر.ک به: صفحه انترنتی: http://fararu.com/fa/news/116595

مبحث سوم: مفهوم سایبر

سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. واژه های ترکیبی بسیاری از این کلمه سایبر بوجود آمده است: فضای سایبر(Cyberspace)، شهروند سایبر(Cybercitizen) ، پول سایبر(Cybercash) ، فرهنگ سایبر(Cyberculture) ، راهنمایی فضای سایبر(CyberCoach) ، تجارت سایبر (Cyberbussiness)، کانال سایبر (Cyberchannel) و....

واژه "فضای سایبر" را نخستین بار ویلیام گیبسون (William Gibson) نویسنده داستان علمی تخیلی در کتاب نورومنسر Neuromancer در سال 1984 به کار برده است.

اینترنت یکی از پیچیده ترین قسمت های سایبر است که توسعه آن در حال حاضر باعث تحولات شگرفی در زندگی انسانها شده است. روند رشد و پیشرفت اینترنت به معنای فضای سایبر آنقدر گسترده شده است که تقریبا اکثر انسانها به این تکنولوژی وابستگی پیدا کرده اند. در این نبشته کوچک بیشتر بر روی ابعاد مختلف فضای سایبر که بر روی مخاطب تاثیر گذاری های مختلفی دارد، بحث خواهیم کرد.

متاسفانه وقتی صحبت از اینترنت، سایبر و ویب میشود در ذهن بسیاری از مخاطبان، ویب سایت های اینترنتی نمود پرنگ و تنها بعد فضای مجازی تداعی می شود. سازندگان و توسعه دهندگان این شبکه قطعا پس از 30 سال، ایده های گوناگونی برای تاثیر گذری های چندجانبه و عمیق تر بر مخاطبان خود طراحی نموده اند.

همانطور که امروزه شاهد هستیم دیگر فضای سایبر یک فضای تک بعدی ویب سایتی نیست، امروز مخاطب بدون اینکه احساس کند در میان چندین وجه از اشکال سایبر دست و پا می زند می توان فضای سایبر را به مثابه دریاچه ای در نظر گرفت که ابعاد گوناگون آن مانند جزایر کوچک و بزرگی هستند که شناگران در این فضا هر از چندگاهی به یکی از این جزایر سر می زنند.

امروزه دیگر فعالیت در یک عرصه از فضای سایبر نمی تواند یک فعالیت اثر گذار و جامع باشد بلکه بسیاری از مراکز مهم و تاثیر گذار در تمام ابعاد این فضا با محتواهای مختلف در موضوعات مشترک فعال هستند.

أ. ویب سایت ها

پایه فعالیت مخاطب از سالیان اول ایجاد اینترنت ویب سایت ها بوده که هم اکنون نیز برای نسل اول کاربران شاید یکی از مهم ترین منابع دسترسی به محتوای سایبر باشند. گروه‌ها و موسسات مختلف در دنیا با ایجاد یک ویب سایت به مخاطبان خود در سراسر دنیا مطالب مورد نظر خویش را ارئه می کنند.

در این بعد از فضای سایبر نقش فعال در اثر گذاری را صاحبان سایت ها داشته و مخاطب به نوعی نقش منفعل محض را دارد . مخاطب می تواند مطالب ارائه شده را انتخاب و استفاده نماید اما نمی تواند در آن نقش آفرینی مستقیم و فعال داشته باشد. بنا بر اعلام صفحه انترنتی نت کرافت (NETCRAT.COM)، در اکتبر سال 2012 میلادی 620480777 ویب سایت[1] و در اکتوبر سال 2014 میلادی به تعداد 947029805 ویب سایت در دنیا وجود دارد.[2]

مخاطبان اصلی ویب سایت ها نسل اول کاربران هستند که شاید بیشترین آشنایی را با ویب سایت از قدیم الایام داشته اند همچنین به خاطر پویایی سریع ابعاد در فضای سایبر مخاطبان نسل اول کمتر با این تحولات به روز شده و به استفاده از ویب سایت قناعت می کنند. شاید اثر گذاری مطالب ویب سایت ها با توجه به اینکه نسبت به برخی دیگر از ابعاد فضای سایبر مفصل تر و شبیه تر به منابع مکتوب است تاثیر گذاری عمیق تر و بیشتری بر روی مخاطب داشته باشد.

---

[1]. سرویی که در سال 2012 توسط نت کرافت، قابل دریافت در پیوند آتی: http://news.netcraft.com/archives/2012/10/02/october-2012-web-server-survey.html

[2]. سروی سال 2014 توسط نب کرافت، قابل دریافت در پیوند: http://news.netcraft.com/archives/2014/11/19/november-2014-web-server-survey.html

ب. وبلاگ ها

استفاده از واژه وبلاگ و وبلاگ نویسی در سال 1994 آغاز و در سال 1999 میلادی اولین سرویس رایگان وبلاگ نویسی توسط (Pitas) ارائه و همان باعث رشد سریع این پدیده در جهان شد.

وبلاگها را میتوان محل ارائه نظرات کاربران خرده اینترنت دانست. افراد مختلف می توانند با اندک زمان و معمولا به صورت رایگان از سرویس های مختلف مادربلاگ های موجود استفاده کرده و صاحب یک وبلاگ شوند. وبلاگها برعکس ویب سایت ها محل فعالیت و حضور موثرتر کاربران هستند و شاید بازیگران خرده پای فضای سایبر آنچه مطلوب خودشان است را به رایگان در این فضا منتشر میکنند.

سطح تاثیر گذاری این وجه از فضای سایبر به مراتب کمتر از ویب سایت ها است اما برای صاحبان این تکنولوژی بهترین و به صرفه ترین محل برای جمع آوری مطلوبه، سلایق، گرایشات مخاطبان عظیم این شبکه است. وبلاگ ها انقلابی را در ویب 1 ایجاد کردند و فضای ویب را به شدت تحت تاثیر قرار دادند.

ت. اتاق های گفت و گو (چت روم ها)

اتاق های گفت و گو نیز مدت کوتاهی پس از ایجاد اینترنت راه اندازی شد و باعث گسترش بیش از اندازه ارتباطات انسانی در دنیا شد شاید پس از ایجاد این اتاق های مختلف در سرویس هایی مانند یاهو، پالتاک، گوگل و ... احاطه بر ارتباطات انسانی برای بسیاری از کشورها به شدت پایین آمد و در عوض این احاطه بر حرفها و گفت و گوهای مردم برای صاحبان فضای سایبر بسیار زیاد شد.

مهم ترین سرویس شناخته شده این اتاقهای گپ دیجیتالی را می توان در سرویس یاهو مسنجر (Yahoo messenger) یافت. اما اکثر مخاطبان با ورود به این اتاق ها زندگی دوم خویش را شروع می کنند در این زندگی فرد شاید ناخودآگاه دوست دارد برای فرد دیگری که او هم در اکثر موارد هویتش مشخص نیست، چیزی باشد که آرزوی آن را داشته است.

بارها و بارها از دوگانگی هویت کاربران در فضای مجازی سخن به میان آمده است. در این عرصه نیز کاربران فعالانه بر روی هم تاثیر می گذارند و شاید صاحبان فضای سایبر در این تاثیر گذاری ها تنها ساکت نشسته و نظاره گر عمل و عکس العمل های کاربران هستند. چت روم ها از سویی باب گفتگوی دو طرفه را باز کرده و ویب 1 به ویب 2 نزدیک کردند. ولی از طرف دیگر بسیاری از جرایم رایانه ای را هم به ارمغان آوردند.

ث. شبکه های اجتماعی مجازی

شبکه های اجتماعی مجازی را می توان یکی از مهم ترین جلوه های دگرگونی در ساختار فضای سایبر در نظر گرفت. شاید نتوان از سال۲۰۰۶ که شبکه فیس بوک به عنوان مهم ترین شبکه اجتماعی مجازی راه اندازی شد تا کنون که بیش از یک میلیارد عضو دارد هیچ شکبه دیگری را با این وسعت پیدا کرد.

نسل دوم کاربران اینترنت عمدتا مشتریان پر و پا قرص شبکه های اجتماعی هستند. در این شبکه ها مانند اتاق های گفت و گو با امکانات پیشرفته تر، افراد با ساختن معرفی نامه ای از خود و ارائه عکسی وارد دنیای اجتماعی مجازی می شوند. در این شبکه ها گروه بندی های مختلف با موضوعات خوب و بد دیده میشود اما سبک کار این وجه از فضای سایبر با ویب سایت ها کاملا متفاوت است. شما می تواند در یک ویب سایت یک خبر سیاسی مهم را بخوانید و یا یک گزارش کاملا مفصل را مطالعه نمایید و یا در وبلاگ خود خلاصه ای از آن را منتشر نمایید اما در صفحات شبکه های مجازی، افراد دیگر حوصله خواندن متن های مفصل را ندارند و لی چکیده بسیاری از حرفها و اخبار در یک یا دو جمله از سوی کاربران مختلف به صورت پیاپی منتشر می شود.

جملات و متن های کم حجم در ظاهر کم اهمیت و سطحی، با تکرارهای بیش از حد بر ذهن مخاطب نقش بسته می بندد.

این شبکه ها در ابتدا با هدف «ارتباطات» ایجاد شدند ولی در نهایت به عاملی در جهت پخش و کنترل «اطلاعات» منجر شدند.

در حال حاضر شبکه های اجتماعی مجازی فعالی همچون فیس بوک، توییتر، مای ساپیس، اورکات و... وجود دارند. یکی دیگر از نکات مهم تاثیر گذاری متقابل سایبر و مخاطبش در شبکه اجتماعی، این مسئله است که در ظاهرحجم زیادی از محتوای این شبکه های اجتماعی توسط مخاطبین و اعضا تولید می شود، اما جهت دهی موضوعات و حتی بالا بردن و جنجالی کردن این موضوعات

می تواند در دست صاحبان این شبکه ها باشد. خیلی از اوقات برخی از موضوعاتی که شاید بسیار عادی به نظر برسد در مقاطع زمانی به جنجال های شبکه ای یا در اصطلاح طوفانهای شبکه ای تبدیل می شوند.

همچنین صاحبان این شبکه ها در کشورهای هدف از این شبکه ها به عنوان بدیلی برای سایت های خبری و تحلیلی استفاده کرده و سعی در گسترش اخبار شفاهی و شایعات در مواقع بحرانی دارند. برای مثال صفحات مختلفی که در فیس بوک در ناآرامی های سوریه و یا لیبی با موضوع اخبار شفاهی راه اندازی شد که می تواند نمونه های خوبی باشد.

همچنین بسیاری از گروهها و مراکز مهم با ایجاد صفحه ای در این گونه شبکه های اجتماعی بخصوص فیس بوک با بالا بردن اعضا و تعداد لایک (نماد محبوبیت) سعی در نمایش قدرت تعداد مخاطبان خود دارند.

ج. بانک های اطلاعاتی دیجیتال

یکی دیگر از ابعاد فضای سایبر را می توان بانک های اطلاعات دیجیتال دانست که این بانک ها مخصوصا در قالب کتابخانه های دیجیتال ظهور و بروز دارند. شاید با شروع پدیده گوشی های هوشمند دست اندرکاران این فضا خیلی دوست داشته باشند تا مطالعه سایبری جایگزین مطالعه سنتی و مکتوب بشود. میزان رشد کتابخانه ها و بانکهای دیجیتال در سالهای اخیر، دسترسی سریع و آسان، ایجاد نرم افزارهای مختلف برای دانلود فایل ها به صورت سریع خود شیوه های تسهیل کننده مطالعه دیجیتال است.

مخاطبان بسیاریشاید در قدیم به علت عدم دسترسی به یک کتاب و یا یک گزارش موفق به خواندن آن نمی شدند اما در فضای سایبر با گذاردن یک لینک ساده از فایل دانلود کتاب و یا راه اندازی یک کتابخانه دیجیتال می توان بدون صرف بسیاری از هزینه های سنتی، یک کتابخانه 24 ساعته بدون تعطیلی داشت که افراد زیادی به راحتی از سراسر دنیا به ان مراجعه کرده و کتابهای مختلف را دریافت کنند.

اما در این وجه نیز شاید صاحبان فضای سایبر بدون چشم داشت این کار را انجام ندهند برای نمونه شاید در قدیم دسترسی به موضوعات و کتابهای مورد مطالعه مردم دنیا بسیار کار سخت و پرهزینه ای بود اما در کتابخانه ها و بانک های دیجیتال تعداد دانلود و ای پی های دانلود کننده به راحتی در اختیار صاحبان این فضا است و در آینده ای نه چندان دور صاحبان این فضا خواهند دانست که ذائقه مطالعاتی مردم دنیا به چه سمت و سویی خواهد رفت.

در این بانک های اطلاعاتی نیز مانند ویب سایت ها تاثیرات معمولا یک طرفه و از بانک دیجیتال به مخاطب است. مخاطبان این وجه از فضای سایبر نسبت به بقیه مخاطبان با سوادتر و از لحاظ اماری کمتر به نظر می رسند. سرمایه گذاری در این بعد از سایبر می تواند به پرورش نخبگان تحت کنترل هر دسته ای کمک شایانی بکند.

هر فرهنگ وتمدنی که بتواند جلوه های خود را که بیشتر در کتابهای آن فرهنگ تجلی دارد را به زبانهای مختلف ترجمه و بهتر و آسانتر در این بانکها قرار دهد می تواند نخبگان بیشتری از جهان را با فرهنگ خود آشناتر کند. این تاثیر گذاری بسیار طولانی و بر افراد محدودتری است اما به شدت عمیق و بر افراد تاثیرگذارتری می باشد.

ح. نشر دیجیتال

دنیای سایبر با پویایی و سرعت بالای خود تحولاتی شگرف در دنیای انتشارات نیز به وجود آورده است اگر در قدیم چاپ یک کتاب مدتها طول میکشد و بعد از آن انتقال آن از یک کشور به دیگر کشورها مستلزم زمان و هزینه بود، امروزه فضای سایبر با ایجاد کتابهای الکترونیک، نشریات دیجیتال و چند رسانه ای های مختلف سرعت نشر افکار و عقاید علمی و تدوین شده را چندین برابر کرده است.

بسیاری از گروههای کوچک و نخبه با کمترین هزینه برای دسترسی به اهداف خود از این گزینه در فضای سایبر استفاده می کنند. انتشار نظریات دیجیتالی که با یک کامپیوتر و داشتن محتوا نیاز به هزینه دیگری نیست. پخش انواع کلیپ ها و محتواهای صوتی و تصویری در فضای سایبر می تواند راه خوبی برای بقای این گروههای کوچک باشد. نشر دیجیتال از جنبه های بسیار مهم ویب 2 می باشد که میتوان گفت در کشور عقب مانده که اکثر مردم به انترنت دسترسی ندارند چندان مورد توجه نیست.

در این وجه میتوانیم شاهد رقابت گروههای مختلف برای تاثیر گذاری بر مخاطبان باشیم ممکن است در این بخش هزینه تولید محتوا مخصوصا در امر کتاب بالا باشد اما مشکل هزینه های چاپ ، انبار کردن و توزیع و حتی مشکل مجوزهای نشر به نوعی رفع شده است.

اما صاحبان سایبر در این موضوع نیز یکی از برندگان هستند، دیگر لازم نیست هزینه های کلان برای رصد و جمع آوری کتابهای منتشر شده صرف شود. نویسنده خود فایل اثر خود را در این فضا منتشر کرده و تعداد استقبال و نظرات دیگران هم پیرامون ان مشخص میشود.

خ. بازی های آنلاین

یکی دیگر از ابعاد فضای سایبر بازی های انلاین در این فضا است. بازی آلاین ها چندین خصوصیت نسبت به بازی های رایانه ای دارند اولا این بازی ها اکثرا رایگان هستند. کم حجم و فکری و نسبتا در یادگیری آسان هستند. بیشتر برای سنین بالا و نه کودکان طراحی می شوند.

بازی های فلش[1]، بازی های گروهی انلاین انواع بازی های اینترنتی هستند. بازی هایی مانند khanwars ، کلوب فوتبال و مافیا جز بازی های پرطرفدار اند. در بازی های انلاین مخاطبان بنا به جذابیت بازی به آن وابسته شده و سعی میکنند زمان بیشتری را در بازی بوده تا نسبت به رقبای خود برتری داشته باشند. همچنین برخی از بازی های آنلاین نیز با اهدافی کاملا متمایز از بازی های عادی منتشر می شود برای مثال می توان به بازی های انلانی منتشر شده بر روی سایت سیا اشاره کرد!

د. آموزشگاههای الکترونیک

آخرین وجه از فضای سایبر که در این گزارش به آن خواهیم پرداخت مبحث تازه ای با عنوان آموزشکده های الکترونیک است. در این نوع آموزش که کاملا در فضای مجازی انجام می شود به گروه وسیعی از مخاطبان اجازه دسترسی به دوره های آموزشی داده می شود. اما در همین فرایند آن دسته از مخاطبان که به این دوره ها علاقه داشته و از خود استعدادی بروز دهند مراتب ترقی را طی کرده و به مراحل بالاتر می رسند. با توجه به هزینه اندک این نوع آموزشگاهها در مقایسه با جذب انبوه استعدادها از سراسر دنیا، برای اکثر مراکز و نهادهای فعال برگزاری این دوره ها برای شناسایی و جذب نخبگان به صرفه می باشد.

با بررسی مختصر و کوتاه این ابعاد از فضای سایبر به این نتیجه مهم خواهیم رسید که فضای مجازی برای ماندن در مقام نخست تاثیر گذاری بر افراد وجوه مختلفی را طراحی کرده و سعی در ورود به حریم افراد به صورت کامل دارد به گونه ای که برخی از رسانه ها امروزه کارکرد چند بعدی خود را کامل کرده و از رادیو تا اپلیکیشن های آندروید را برای خود طراحی و استفاده می کنند.

ساده لوحانه است اگر برای تاثیر گذاری فقط به یک بعد این فضا توجه شود متاسفانه وقتی سخن از فعالیت در فضای مجازی می شود. بسیاری از افراد ویب سایت ها را مد نظر گرفته و برخی از نسل جدید ممکن است شبکه های اجتماعی را به یاد بیاورند.

فضای مجازی روز به روز توسعه می یابد و عرصه های خود را مانند تارهای عنکبوت گسترده تر می کند تا جایی که زندگی مجازی و حقیقی را یکسان نماید به نظر شما آن روز کنترل واقعی زندگی افراد در دستان کیست؟![2]

[1] - Flash Games

[2]. ر.ک به: ویب سایت: http://www.bcatc.ir/fa/87-student-s-basij/cyber/154

فصل دوم: جاسوسی و روابط بین الملل

مبحث اول: جاسوسی در روابط دیپلوماتیک

در روابط بین کشورها معمولا روابط رسمی دیپلماتیک بیانگر همکاری و تعامل رسمی میان دولت‌هاست و در چارچوب روابط رسمی دیپلماتیک، کشورها به دنبال تامین منافع خود هستند. معمولا دیپلمات‌ها، سفرا، کارداران و یا دیگر اعضای هیئت دیپلماتیک به عنوان نمایندگان سیاسی و رسمی یک دولت در کشور دیگر به فعالیت میپردازند. اقدامات این افراد رسمی و قانونی است و میتوانند به طور رسمی و علنی با مقامات کشور پذیرنده ملاقات و گفت و گو کنند. معمولا بخش‌هایی در سفارت خانه‌ها برای کسب خبر، جمع آوری اطلاعات و گزارش این اخبار به کشور فرستنده تعبیه میشود که همه اینها در قالب ها و برنامه های رسمی صورت میگیرد و جنبه قانونی دارد. کنوانسیون وین 1961 درباره روابط دیپلماتیک هم این حق را برای دیپلمات های رسمی قائل شده است که به طور رسمی و علنی به فعالیت بپردازند و به مراوده با مقامات رسمی کشورهای پذیرنده اقدام کنند.

اما بر این مسئله تاکید شده است که دیپلمات‌ها نباید از حیطه وظایف قانونی خود عدول کرده یا خارج شوند. به عبارت دیگر دیپلماتها باید آنچه که در قانون برای آن‌ها پیش بینی شده است اعم از آن چه قوانین داخلی کشورها پیش بینی کرده یا پروتکل‌های بین المللی که حدود و اختیارات دیپلمات‌ها را مشخص کرده را رعایت کنند.

اما از آن جا که کسب بعضی خبرها یا جمع آوری بخشی از اطلاعات به طور علنی و رسمی نمیتواند تامین کننده منافع کشورها باشد، کشورها معمولا در هیئت‌های دیپلماتیک خود، به طور غیررسمی و در کسوت دیپلمات گروه‌های اطلاعاتی و امنیتی تعبیه می کنند. این افراد اگرچه به عنوان دیپلمات معرفی شده اند اما کارشان خبرچینی و جمع آوری اطلاعات و ارتباط با مقامات رسمی، مقامات نظامی، سران احزاب و این قبیل افراد البته به صورت محرمانه و غیرعلنی است.

این مسئله طبیعی است و در بین هیئت‌های دیپلماتیک معمولا چنین افرادی معرفی میشوند. اما زمانی که شناسایی شوند و مشخص شود که کارشان غیرقانونی بوده و در واقع به امر جاسوسی می پرداختند، طبیعتا دولت پذیرنده آن‌ها را عنوان عنصر نامطلوب معرفی می کند و از دولت متبوع آنها می خواهد که این افراد را احضار کند. از آنجا که در همه هیئت های دیپلماتیک چنین افرادی وجود دارد زمانی که چنین اتفاقی بیفتد معمولا دولت مقابل هم ممکن است همین اقدام را انجام دهد و تعدادی افراد را به عنوان جاسوس معرفی کند و بخواهد که این افراد را مبادله کند یا مقابله به مثل انجام دهد. اما مسئله جاسوسی به همین مورد محدود نمی شود. فراتر از این هم دولت ها میتوانند در قالب افراد غیررسمی و غیردولتی، مثلا نمایندگان شرکتهایی که در کشورهای دیگر سرمایه گذاری میکنند یا حتی دانشجویانی که به امر تحصیل مشغول هستند، به جمع‌آوری اطلاعات و جاسوسی بپردازند. تا زمانی که این افراد شناسایی نشده‌اند می توانند به کار خودشان ادامه دهند. اما وقتی این افراد شناسایی میشوند، دولت میزبان میتواند آن‌ها را دستگیر و محاکمه کند. جاسوسی و قوانین مربوط به محاکمه جاسوسان در حقوق بین الملل، مسئله ای داخلی محسوب می شود و حقوق بین الملل وارد حیطه مسائل داخلی کشورها نمی شود. چگونگی برخورد با این افراد به صلاحدید کشورها و نوع نگاه آن‌ها به یکدیگر بستگی دارد. بنابراین روابط کشورها و مصالح سیاسی تعیین کننده چگونگی برخورد با جاسوسان است و همین مصالح سیاسی است که تعیین کننده امکان یا عدم امکان مبادله جاسوسان میان کشورها است. اهمیت منافع و مصالح سیاسی در ارتباط دولت‌ها با یکدیگر تا آنجاست که دولتی میتواند جاسوسی را شناسایی کند و از کنار او بگذرد و اجازه دهد به فعالیت خود ادامه دهد.[1] یا فردی که جاسوس نبوده را به عنوان جاسوس معرفی کند. و مثال ها عملی زیادی درین زمینه وجود دارد که به دور از حوصله این نوشته است.

امروزه نوع دیگری از جاسوسی که قبلا از آن یادآور شدیم در دنیا مدرن و دهکده جهانی بسیار تاثیر گذار و اغلب کشور قدرتمند به آن میپردازند جاسوسی سایبری بوده که مفصلاً در فصل آتی به آن اشاره میشود.

[1]. ر.ک به: ویب سایت: http://www.iranamerica.com/forum/showthread.php?t=19255

مبحث دوم: مدرن در روابط بین الملل

رسانه ها و به ویژه رسانه های اجتماعی با ورود به عرصه سیاست خارجی، تغییرات اساسی درمفاهیم، دامنه،کارکرد وشکل دیپلماسی راموجب شده اند وهمین امر تغییرات مهمی را در فرآیند سیاست گذاری، هدایت واجرای سیاست خارجی کشورها بوجود آورده است. روابط عمودی دردیپلماسی رسمی، باظهور رسانه های اجتماعی، متحول شده واکنون حفظ وتوسعه روابط افقی واقناع افکارعمومی وارتباط مستمر با نخبگان و بازیگران غیردولتی ضرورتی انکار نا پذیر بشمارمی رود.

در فضای سایبری، رسانه های اجتماعی که به عنوان ابزاری کارآمد برای معرفی وقبول افکار، فرهنگ، هنجار، ارزش واهداف مطلوب به دیگرملل تعریف می شود (قدرت نرم)، با حضور در عرصه دیپلماسی، ویژگی هایی چون ایجاد گسست درانحصار دولت بر شئون روابط خارجی، شکست انحصار ارتباطات رسمی سنتی، ایجاد موضوعات جدید و تغییرسریع و روزافزون روشها و درهم ریختگی عناصر فاصله، زمان و مکان را موجب شده اند. رسانه های اجتماعی با سرعت بی نظیر به رشد خود در همه شئون زندگی بشری ادامه میدهند. روابط بین المللی و دیپلماسی جهانی نیز از این شئون مستثنی نیست. اکنون اهداف سیاست خارجی تنها ازمسیر دیپلماسی رسمی و روابط انحصاری دولت ها با یکدیگر محقق نمی شوند. توجه به افکار عمومی واقناع آن به یکی از پایه های دیپلماسی های قدرتمند مبدل شده است.

رهبران کشورها با درک جدیدی ازقدرت افکارعمومی در پیشبرد اهداف سیاست خارجی، آن را یکی از ارکان دیپلماسی خود ساخته اند. دیپلماسی عمومی و رسانه ای در سایه چنین رویکردی از اقبال فزاینده ای برخوردارشده است. دوفضایی شدن جهان، درهم آمیختگی فضای سایبر با فضای واقعی، مدیریت دیپلماسی کشورها را در برابر وضعیتی قرارداده که کم توجهی به این دو فضایی شدن، تأثیر مستقیم درقدرت ملی آنان درعرصه بین المللی خواهد گذارد. دراین چارچوب توجه به رسانه های اجتماعی در حوزه دیپلماسی ازموضوعات اساسی سیاست خارجی می باشد.

باید بپذیریم که اکنون دیپلماتها بدون احاطه و شناخت دربکارگیری رسانه های اجتماعی، نخواهند توانست نقش وکارکردهای مناسب را ایفا کنند. شاید بتوان گفت موازنه درمحیط جدید بین المللی که درساختاری مشتمل برکشورهایی با قلمرو نفوذ پذیر و ترکیبی از قدرت نرم وسخت، سیاستی سنتی و دیجیتالی ویا سیاستی واقعی و دانش مدار تعریف می شود، حاصل ازفضایی آکنده از رخدادها و موقعیتهای ناشی ازگسترش روزافزون رسانه های اجتماعی باشد ودراین فضای به شدت رسانه ای قرنِ بیست ویکم، تنها دیپلماسی مجهز به رسانه های اجتماعی می تواند مؤثرترین وموفق ترین تعاملات را با مخاطبان خود داشته باشد. رسانه های اجتماعی به شکلی روزافزون و اجتناب ناپذیر نحوه هدایت واجرای سیاست خارجی را تغییرداده اند. اکنون قدرتِ جهانی یک کشور، در توانایی، ظرفیت واستعداد دیپلماسی رسانه ای درایجاد هویت ملی و ارائه تصویر مکمل بین المللی آن نهفته است.

درحال حاضر، کشورهای پیشرفته درامر دیپلماسی و سیاست های بین المللی به صورتی روزافزون از رسانه های اجتماعی در پیشبرد اهداف سیاست خارجی خود بهره گرفته ولی بیشترکشورها به دلیل محدودیت های فنی و انسانی ویا موانع قانونی، باسرعت کمتری دراین مسیر حرکت می کنند. وجود تفاوتها درنحوه بکارگیری رسانه های اجتماعی دردیپلماسی کشورها، می تواند همانند چالش دیجیتال میان جهان توسعه یافته و کمترتوسعه یافته، به شکاف در دیپلماسی دیجیتال ونهایتا ایجاد نابرابری شدید درتوان دیپلماسی این کشورها منجر شود. وزارت امورخارجه برای اینکه قادر باشد درعرصه دیپلماتیک از تأثیر و کار آمدی بیشتری برخوردار باشد، باید درزمینه استفاده از رسانه های اجتماعی تصمیمات اساسی اتخاذ نماید.

رسانه های اجتماعی راه های متنوعی را برای انتقال پیام به عموم در اختیارقرار میدهند، راه هایی که درگذشته در دسترس نبوده اند. کشورها و سازمانهای بین‌المللی به ارزیابی راه هایی که از طریق آن می توانند مأموریت های خود را با اتکا به بخشی از قدرت نرم افزایش دهند، ادامه می دهند، به عبارتی قانع کردن، به جای مجبور کردن. شاید بتوان گفت دیپلماسی متکی به رسانه های اجتماعی ازمزایایی برخوردار است، ازجمله حفظ و نگهداری از پایگاه‌های اینترنتی تعاملی نیازمند بودجه و پرسنل است. با قدرت گیری مردم به وسیله دسترسی به اشکال جدید رسانه و جریان وسیع تر اطلاعات، این پیوستگی مهم خواهد بود.

اکنون در عرصه دیپلماسی عمومی نوین، استفاده از رسانه های نوین (رسانه های اجتماعی) برای گوش فرادادن و تاثیرگذاری بر روی مخاطبان خارجی در دستورکار قرار گرفته است، چه این تأثیرگذاری از سوی دولت باشد وخواه ازسوی مردم باشد یک هدف را دنبال میکند و آن ایجاد محیطی عالی برای رسیدن به مقاصد اقتصادی، فرهنگی، سیاسی وامنیت ملی است. اما این دیپلماسی ویژگی های کلیدی به این شرح دارد:

- هرروزه، بازیگران بین المللی جدیدتری به صحنه می آیند و سازمان های مردم نهاد دراین میان به ویژه دارای اهمیت هستند.

- مکانیزم های استفاده شده توسط این بازیگران برای برقراری ارتباط باعموم درکشورهای خارجی، به سمت فناوری های جدید وجهانی حرکت کرده است

- این فناوری های جدید خطوط انعطاف ناپذیرگذشته میان حوزه های خبری داخلی وبین المللی را کمرنگ ساخته است

- دیپلماسی عمومی به جای بکارگیری مفاهیم کهنه تبلیغاتی ازمفاهیمی استفاده میکند که هم برگرفته از بازاریابی بوده و هم ریشه در نظریات ارتباطات شبکه ای دارند

- استفاده از واژگان جدید درزمینه وجهه و تصویر بین المللی یک کشورمانند قدرت نرم و برند یک کشور

- تأکید برتماس مردم با مردم برای روشنگری های دوجانبه و دراین میان بازیگر بین المللی نقش تسهیل کننده را ایفا میکند و رابطه سازی وظیفه اصلی دیپلماسی عمومی نوین است

برای استفاده مؤثر و کارآمد از رسانه های اجتماعی درعرصه دیپلماسی عمومی، ضروریات والزاماتی وجود دارد که مهمترین آنها چنین برشمرده می شود: اولا برای اینکه این دیپلماسی از حد اکثرکارایی برخوردار باشد، تأکید به نقش رهبران درترغیب به استفاده از این تکنولوژی لازم وضروری است. ثانیا برای توسعه دیپلماسی نوین تعاملی باید ساختار سیاسی را نیز مد نظر قرار داد. ثالثا درتوسعه مسئولیت پذیری کارگزاران ومدیریت استفاده از رسانه‌های اجتماعی توسط دیپلماسی عمومی، آموزش کارکنان دیپلماسی در این زمینه ضروری است. و رابعا وجود یک شبکه کارآ جهت بهره برداری از دیپلماسی عمومی، امری حیاتی است.

رسانه های اجتماعی در سال های اخیر پیامدهایی بر دستگاه دیپلماسی به لحاظ نرم افزاری و سخت افزاری به شرح ذیل ایجاد کرده اند:

- دگرگونی ساختاردیپلماسی؛ امکانات فناوری جدید، نشان می دهد که دیپلماسی بطور بنیادین تغییر ماهیت خواهد داد شاید تا در دهه پیش، ایده سفارت خانه های مجازی امری غریب بود ولی اکنون این امرمحقق شده و رسانه های اجتماعی به طور فزاینده ای موجب تماس میان شهروندان و دستگاه دیپلماسی شده اند
- تغییرنقش دیپلمات ها؛ نقش دیپلماتها به واسطه رسانه های اجتماعی دچار تغییر شده است پیش از این، دیپلمات‌ها اساسا به جمع آوری اطلاعات برای دولت متبوع خود مشغول بودند؛ ولی امروزه به دلیل انتشارآزاد وسریع درفضای سایبر، اطلاعات در اختیار همگان قرار دارد
- امکان افراط و تفریط دردیپلماسی؛ رسانه اجتماعی فی نفسه دارای ارزش خنثی است. این فناروی مقاصد و تمایلات کاربران را به خود میگیرد. گسترش روز افزون این رسانه، دولت‌ها را بیش از پیش با ظهور جنبش‌های بدون رهبر از سوی شهروندان مواجه میسازد.
- تمرکززدایی ازاجرای سیاست خارجی؛ سفارتخانه ها ودستگاه های سیاست خارجی حالتی سلسله مراتبی و چینشی طولی داشتند؛ اما امروز رسانه اجتماعی، واکنش سریع تر و ماهرانه سفراء درقبال وقایع درحال رویداد را ضروری ساخته است
- امکان تضعیف دیپلماسی سنتی؛ هرچند دیپلماسی دیجیتال، بافت و تفاوتی ظریف به پیام های صادره از دستگاه سیاست خارجی افزوده است ولی این احتمال قوی است که به شکلی فزاینده، روابط سنتی درمقابل، روابط دیجیتال تضعیف شوند
- شفاف سازی دیپلماسی؛ دیپلماسی دیجیتال تعاملات و فضای جدیدی را ایجاد کرده و در آینده روابط بین‌الملل مردمی تر خواهد شد؛ رسانه اجتماعی میتواند به ایجاد شفافیت بیشتر درعرصه روابط خارجی کمک کند.

یک جمع بندی اجمالی در باره وضعیت دستگاه دیپلماسی برخی کشورها در بهره گیری آنان از رسانه های اجتماعی حاکی است:

1- نقش و جایگاه رسانه های اجتماعی دردیپلماسی بیشتر کشورها به سرعت ارتقاء یافته است.
2- دستگاههای دیپلماسی همه کشورها، به فضای سایبر به عنوان مکمل فضای واقعی در اجرای سیاست های واقعی خود توجه دارند.
3- کشورهای غربی دراستفاده از رسانه های اجتماعی برای تحقق اهداف سیاست خارجی بیش از دیگر کشورها اهتمام به خرج داده و ازسرعت بسیار بیشتری در این زمینه برخوردارند.

4- دستگاه دیپلماسی شماری از کشور ها هنوزاقبال چندانی به رسانه های اجتماعی نداشته است.
5- متأسفانه تداوم وضعیت فوق وعدم تلاش دراصلاح آن، امکان چالش دیجیتال درحوزه دیپلماسی عمومی رادرعرصه بین المللی تشدید میکند.
6- عدم توجه دیپلماسی عمومی به فضای سایبر تهدید از دست دادن کاربران به ویژه کاربران نسل جوان که اهمیت فراوانی را برای زندگی در فضای مجازی واستفاده از رسانه های اجتماعی قائلند، تشدید می نماید.
7- بطورطبیعی استمرار وضعیت فوق می تواند به تضعیف دیپلماسی عمومی ودیپلماسی کلان کشور درعرصه بین المللی بیانجامد[1].

گذشته از جاسوسی به شیوه های سنتی و کسب اطلاعات از طریق رسانه های سنتی امروز نوع دیگر جاسوسی نیز مطرح است که عبارت از **جاسوسی سایبری** است و در محور توجه داشنمندان و مجالس سیاسی قرار گرفته است، این مطلب را طی بحث های آتی به بررسی میگریم.

اما قابل یاددهانی است که پیش از پرداختن به مبحث جاسوسی سایبری، نیاز است تا مفهوم دیپلماسی سایبری روشن شود و در پرتو دیپلماسی سایبری بحث جاسوسی سایبری قابل درک خواهد بود.

[1]. ر.ک به: صفحه انترنتی http://ahaad.ir/s/9871

فصل سوم: جاسوسی سایبری

مبحث اول: دیپلماسی سایبری یا سایبر دیپلماسی

در سایبر دیپلماسی مخاطبان چه داخلی و چه خارجی ، همه از اعضای جامعه اطلاعاتی هزاره سوم هستند و قصد دارد تا سیاست داخلی یا خارجی یک کشور را در حوزه های مختلف مربوط به خود ، درمحیطی متفاوت از نهاده های ساختار سنتی عرضه کند.

سایبر دیپلماسی (cyber diplomacy) مثل بسیاری از مفاهیم نوظهور دهکده جهانی، توجهات اندکی را در میان مسئولان کشور به خود اختصاص داده است. همانطوری که در فصل اول گفتیم، واژه دیپلماسی به معنی هدایت روابط بین افراد، گروه‌ها و ملت‌ها از جمله واژه‌های سیاسی مورد استفاده در عرصه مناسبات بین‌المللی است و دیپلماسی (Diplomacy) در کاربرد رسمی خود عمدتاً به دیپلماسی بین‌المللی که هدایت روابط بین المللی از طریق دیدار و گفت وگوهای دیپلمات های رسمی است اشاره دارد.

و اما ارتقای سطح اطلاع رسانی دولت ها در هزاره سوم، روش های متعددی به خود کسب کرده که یکی از آن ها، استفاده از نهاده های موجود در سایبر دیپلماسی می باشد. سایبر دیپلماسی در ساده ترین تعریف، استفاده از ابزارهای فناوری اطلاعات و ارتباطی روز، جهت تبیین، گسترش و ارتقای سطح اثر بخشی دستگاه دیپلماسی یک کشور در فضای مجازی می باشد. در سایبر دیپلماسی، مخاطبان چه داخلی و چه خارجی، همه از اعضای جامعه اطلاعاتی هزاره سوم هستند. بنابراین فعالانی که در این حوزه اشتغال دارند باید بدانند که مخاطب آن ها، یکی یا گروهی از اعضای خانواده تقریباً از یک و نیم میلیارد نفری کاربران فضای مجازی است.

توسعه سطح اطلاع رسانی دیجیتالی فعالیت های دولتی در ویب، ارتقای ضریب نفوذ دیپلماسی در رسانه های جهان، توسعه بدنه دولت الکترونیک در حوزه بین المللی، فعال شدن حوزه عملکرد دولت در فضای دیجیتالی داخلی و جهانی، تقویت ارگان های دیجیتالی خصوصی، تنظیم سیاست های دولت در زمینه گسترش e-commerce و e-banking در سطوح بین المللی از جمله فواید سایبر دیپلماسی است. سایبر دیپلماسی در واقع بخشی از بدنه دولت الکترونیک و جزئی از کلیت ساختار دولت مجازی در یک کشور است[1].

[1]. ر. ک به: وبب سایت: http://www.ictpress.ir

مبحث دوم: مفهوم جاسوسی سایبری

جاسوسی سایبری به معنای عام آن یعنی بدست آوردن اطلاعات سری بدون اجازه مالک آن؛ حال در معنی خاص این مالکیت می تواند در زمینه های مختلف تعریف و نیز به مالکیت های متفاوت تعمیم داده شود.

یعنی جاسوسی سایبری یا هنر یا تکنیک به دست آوردن اطلاعات سری بدون مجوز گرفتن از نگهدارنده اطلاعات (شخصی، حساس، اختصاصی یا نوع طبقه بندی شده) است. از اشخاص، رقیبان، حریفان، گروهها، دولتها، و دشمنیهای شخصی، اقتصادی، سیاسی یا نظامی صرفه استفاده کردن روشها در اینترنت، شبکه‌ها یا کامپیوترهای شخصی به خاطر استفاده از تکنیکهای کرک کردن و نرم‌افزار malicious شامل اسبهای تروژان وابزار جاسوسی. آن می‌تواند کاملاً ترکیب شده باشد درون خطی به واسطه میزهای تحریر کامپیوتر از متخصصان روی پایه‌ها در دور کشورها یا می‌تواند نفوذ کند در مکانی به وسیله جاسوسهای متعارف آموزش داده شده کامپیوتر و جاسوسها یا در سایر نمونه‌ها می‌تواند مجرم دستی بشود به وسیله هکرهای بدخواه غیر حرفه‌ای و برنامه نویسهای نرم‌افزار.

جاسوسی سایبری استفاده از این طور دسترسیها را در برابر اطلاعات سری و اطلاعات طبقه بندی شده یا کنترل کامپیوترهای اختصاصی یا کل شبکه‌ها برای یک مزیت استراتژیک و برای سیاسی، عملیات روانی و فعالیتهای براندازی فیزیکی وعملیات تخریبی درگیر کرده‌است. به تازگی، جاسوسی سایبری درگیر کاوش از فعالیتهای همگان روی سایتهای شبکه اجتماعی مانند Facebook و Twitter است.

این چنین عملیات، نظیر جاسوسی کردن غیر سایبری هستند، نوعاً غیر قانونی در قربانی کشور در صورتی که کاملاً حمایت شده به وسیله بزرگترین سطح دولت کشور حمله کننده. حالت اخلاقی همچنین وابسته‌است روی یک نظریه، مخصوصا یک گزینه از دولتهای درگیر. [1]

روشهای جاسوسی عموما با تغییرات تکنولوژی همگام است و هرچه فضای سایبر پیچیدگی بیشتری پیدا کند، این روشها نیز پیچیده تر می شوند. بستر کلی این جاسوسی ها همانطور که از نامش پیداست فضای اینترنت میباشد امّا این فضا باز خود به دو بخش شبکه های اداری و فردی تقسیم می‌شود.

دسترسی به مقصد مورد نظر از طریق فضای شبکه، با استفاده از تکنیک‌های کرک کردن و یا بدافزارهای مخرب امکان پذیر می باشد. بدافزارهای مخرب تقسیم بندی‌های مختلف دارند که با توجه به نوع سیستم مقصد، گونه ای خاص از آنها استفاده می شود؛ و دامنه آن ها از ویروس‌ها تا کرم ها و تروژان ها را شامل می‌شود.

در این نبشته یکی از مهمترین قسمت های جاسوسی سایبری جاسوسی سایبری سیاسی (political cyber spying) را بطور اجمالی به بررسی میگیریم:

در ابتدا شاید نیاز باشد به تعریف واژه "espionage" که از آن در فضای سایبر به جاسوسی تعبیر میشود بپردازیم. معنی لغتنامه ای این کلمه "استفاده از جاسوسان به منظور جمع‌آوری اطلاعاتی درباره آنچه یک کشور و یا یک شرکت در حال انجام دادن آن است و یا قصد انجام دادن آن را دارد"، میباشد.

جاسوسی و انجام عملیات های پنهان دو واژه‌ای هستند که در دیکشنری "MERRIAM-WEBSTER" مرزی نزدیک به هم دارند و تمایز آن ها تنها زمانی مشخص میشود که به زمینه کاری آنها بیشتر دقت شود. این یعنی؛ هنگامی که دولتمردان غربی از نقطه نظر بین‌المللی بدان نگاه کنند، معنای جاسوسی و انجام عملیات پنهان که دو جایگزین فارسی برای "espionage" و "covert action" میباشند؛ یکی است. امّا هنگامی که با نگاه ملی بدان مینگرنند این دو کلمه برای آنها دو معنای کاملا متضاد را در سیاست هایشان بدنبال دارد.

عملیات پنهان بنابر تعریف سی‌آی‌ای به عملیات‌هایی گفته می شود که به وسیله آنها بتوان شرایط اقتصادی، سیاسی و نظامی را درسایر کشورها تغییر داد و به نفع خود تمام کرد.

---

[1]. ر.ک به: سایت: http://fa.wikipedia.org/wiki/%D8%AC%D8%A7%D8%B3%D9%88%D8%B3%DB%8C_%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C

چنایچه یاد آور شدیم امروزه اسرار تجاری و اقتصادی براي دولتها و سازمان های جاسوسی، از اسرار نظامي اهمیت بیشتری یافته است. به همین جهت جاسوسي اقتصادي روز به روز شدت گرفته و روش هاي تازه‌ای برای کسب اخبار و اطلاعات مفید به کار گرفته می‌شود.

در این راه کسب اطلاع از توانمندی‌های دشمن کم اهمیت تر از اطلاع از نیروهای دشمن نیست، بلکه کسب اطلاعات پیرامون تجهیزات و ابزار موجود در کارخانجات صنعتی کشورهای دشمن، اهمیت بیشتری از کسب اطلاع از تعداد و نوع و کیفیت کار تانك‌های دشمن پیدا کرده است. از این نظر میتوان گفت سازمان‌های جاسوسی مأموریت دارند که آنچه را کشورها با جنگ نتوانستند به آن برسند، با عملیات جاسوسی به انجام برسانند.

"شفایوز" مؤلف کتاب «دوستان جاسوس» به ایجاد بخش جاسوسی توسط شرکت موتورولای آمریکا اشاره کرده و مینویسد: این شرکت تحت عنوان های مختلف، مشغول جمع آوری اطلاعات فنی و اقتصادی از کشورها و کمپانی های رقیب است. در این راستا شرکت های زیمنس و داسا و مجموعه رانیمیتال و هوخست و بایر و فیبا در آلمان از اهداف مهم دستگاه‌های جاسوسی آمریکا و اروپا هستند.
در گزارشی که بخش ضدجاسوسی سازمان اطلاعاتی فرانسه منتشر کرده، آمده است: آمریکایی ها جاسوسی اقتصادی را هدف اول خود قرار داده اند.
اما حملات جاسوسی سایبری اقتصادی را می توان به 2 بخش کلّی تقسیم کرد؛ یکی حمله به زیر ساخت های صنعتی که بخش اعظمی از اقتصاد کشورها را تشکیل می دهند و دیگری حمله به منابع تجاری و اقتصادی که می توان بانکها و شرکتهای تجاری را مهمترین آن‌ها دانست.

بطور مثال "استاکس نت" نوعی کرم پیچیده کمپیوتری است که در سال 2010 از طریق حفره‌های امنیتی موجود در ویندوز مایکروسافت شیوع پیدا کرد و تجهیزات و نرم افزارهای صنعتی شرکت زیمنس را هدف قرار داد. این اولین باری نبود که سیستم های صنعتی مورد حمله قرار می گرفت ولی اولین بدافزاری بود که به جاسوسی از سیستم‌های صنعتی می پرداخت و سعی در تخریب آن ها داشت و بدین منظور حاوی فایل های آلوده‌ای بود که قابل برنامه ریزی بودند.

سیمانتک در گزارش خود در مورد این بدافزار اعلام کرد که 60% رایانه هایی که بدین بدافزار آلوده شده اند در ایران قرار دارند. آزمایشگاه کاسپراسکای اعلام کرد که این حمله "تنها می تواند به وسیله حمایت های دولتی و از سوی کشور و یا کشورهایی صورت گرفته باشد".

مبحث سوم: روش های جاسوسی سایبری

سایبر برای هر شخص یا گروهی که با آن به تعامل می پردازد به شکلی متفاوت نمود می یابد

شهرها و محیط و ماحول این جهان، که توسط مهندسین خلق شده و همه از آن استفاده میکنند، برای هر شخص یا گروهی که با آن به تعامل می پردازد به شکلی متفاوت نمود می یابد. فضای سایبری برای ارتش کشور، یک حوزه جنگ و مبارزه است؛ برای یک دانشجو، مکانی است برای تعامل با دیگر همسالانش؛ و برای یک شرکت تجاری، مکانی است برای کسب درآمد، و این فهرست به همین ترتیب ادامه می یابد. بحث و گفتگو در مورد یک موضوع مرتبط، یعنی امنیت سایبری، نیز همین ویژگی ها را داراست. چگونگی دستیابی به امنیت، یا حتی تعریف آن، نیز به مشترکان و کاربران بستگی دارد. جاسوسی دیجیتال، برای اکثر افراد در دنیای امنیت سایبری، یک موضوع جنجالی و مهم است. آیتم های خبری اندکی چنین جنبش و پویایی نظیر گزارشی که در ماه فوریه توسط شرکت من، ماندیانت، در مورد واحد 61398 منتشر شد، در این دنیای مجازی ایجاد کرده اند. این گزارش تاریخچه هفت ساله جاسوسی های دیجیتال توسط واحد 61398 علیه حداقل 141 شرکت غربی را افشا کرد. ماندیانت، جاسوسی های سایبری چینی را ردیابی کرد و به یک ساختمان اداری 12 طبقه در خارج از شانگهای رسید.

مسلماً هر نوع اقدام به جاسوسی، موضوعی جدی و مهم است، اما برخی از افراد تفاوت جاسوسی در جهان سایبری را با جاسوسی در جهان فیزیکی درک نمی کنند. عده اندکی به این موضوع واقف هستند که همان ابزارهای لازم برای انجام جاسوسی های دیجیتال، می تواند به متجاوزان اجازه دهد که یک گام به جلو برداشته و ویرانگری های دیجیتال نیز به بار آورند. زمانی که دشمن به یک سیستم کمپیوتری نفوذ می کند، میزان خسارتی که وارد می کند یا نمی کند، کاملاً به قصد و نیت خودش بستگی دارد. این که چنین اقداماتی را باید جنگ تلقی کرد یا خیر بیشتر یک تصمیم گیری سیاسی است، اما امکان تبدیل جاسوسی به ویرانگری موضوعی است که اغلب نادیده گرفته می شود.

مبحث چهارم: تفاوت میان جاسوسی سایبری و جنگ سایبری

منتقدان در اظهار این که جاسوسی تنها یک مرحله پایین تر از یک حمله دیجیتال تمام عیار (که می تواند اقدام به جنگ تفسیر شود) می باشد، درنگ نمی کنند. به عنوان مثال، «بروس اشنایر» ، به گزارش های فعالیت های سایبری چین چنین پاسخ داد: «این یک جنگ سایبری نیست. این در واقع هیچ نوع جنگی نیست. این جاسوسی است، و درک تفاوت آن با جنگ مهم است. گذاشتن نام جنگ بر روی آن، تنها به ترس های ما دامن زده و هیزمی برای آتش تسلیحات جنگ سایبری می شود.»

درک عمومی از دفاع، جاسوسی و جنگ دیجیتال باید بهبود یابد. افرادی با پیشینه نظامی، از سه اصطلاح جهت تشریح فعالیت های سایبری استفاده می کنند: دفاع از شبکه های کامپیوتری (CND) ، سوء استفاده و استخراج از شبکه های کامپیوتری(CNE) ، و حمله به شبکه های کامپیوتری(CNA) . CND که وظیفه محافظت از اطلاعات دیجیتال در برابر هکرها را بر عهده دارد، میان همگان یک امر خوب تلقی می گردد. CNE و CNA مسئله سازتر هستند چون شامل انجام اقداماتی تهاجمی علیه یک هدف مشخص می باشند

متخصصان غربی در حوزه امنیت، CNE را به عنوان جاسوسی دیجیتال، و CNA را به عنوان تغییر دادن، مختل کردن، یا تخریب سیستم های کامپیوتری، چه به صورت مجازی و چه به صورت فیزیکی، در نظر می گیرند. به عنوان نمونه هایی از CNE می توان به نفوذ به شبکه های کامپیوتری برای سرقت اسرار تجاری یا دیگر داده های حساس، کنترل بر تایپ کردن اشخاص و سرقت رمز های عبور آن ها، یا ربودن اطلاعات هنگام ویب گردی آن ها در اینترنت، اشاره کرد. تغییر رکوردها و سوابق پایگاه داده یا حذف کردن داده ها نمونه ای از CNA مجازی بوده و استفاده از کامپیوترها برای خسارت زدن یا ویران کردن تجهیزات یا وارد کردن صدمات دیگر در جهان واقعی، نمونه هایی از CNA فیزیکی می باشد.

اصطلاح «جنگ سایبری» معمولاً به استفاده از یک سلاح دیجیتال برای وارد کردن صدمات فیزیکی اطلاق می گردد. یکی از نمونه های این مورد که مورد، حمله استاکس نت علیه تأسیسات هسته ای ایران بوده است. برخی افراد اصطلاح «جنگ سایبری» را بسیار آزادانه و بی قید و بند مورد استفاده قرار می دهند، یا بسیاری از انواع اقدامات دیجیتال را تا زمانی که به عملیات نظامی جهان واقعی مرتبط باشند، جنگ سایبری می پندارند. همانند زمانی که هکرهای روسی، ویب سایت های گرجستان را در طول جنگ سال 2008 میان دو کشور تخریب نمودند.

دشمنی که قادر به جاسوسی باشد، قادر به خسارت زدن هم هست، و این تنها به قصد و نیت اش بستگی دارد. در نتیجه، بسته به هدفی که مورد حمله قرار می گیرد، جاسوسی سایبری می تواند به سرعت به یک جنگ سایبری مبدل شود، جنگی که در آن از تسلیحات دیجیتال برای اعمال خسارات فیزیکی استفاده می گردد. پرسشی که مطرح میشود این است که آیا متجاوز تصمیم می گیرد جاسوسی کند، یا دست به تخریب و ویرانگری هم میزند؟

این الگوی حمله را در نظر بگیرید. متجاوز در ابتدا اقدام به شناسایی هدف مورد نظر کرده تا نقاط ضعف آن را بررسی کرده و راه هایی برای سرقت یا دستکاری داده ها بیابد. سپس، محتویات و مطالبی که به شکل سلاح درآمده اند (مثلاً سندی با کدهای مخرب و ویروسی، یا لینکی به یک وب سایت مخرب) را از طریق یک پیام ایمیل ارسال می نماید. گیرنده ایمیل پیوست های آن را باز کرده یا روی لینک کلیک می کند، و این کار موجب می شود که کامپیوتر وی تبدیل به قربانی متجاوز گردد. متجاوز اکنون می تواند کامپیوتر قربانی را کنترل کرده و آزادانه اهداف خود را دنبال نماید.

این همان لحظه کلیدی است: آیا متجاوز تصمیم می گیرد جاسوسی کند، یا دست به تخریب و ویرانگری بزند؟ در اکثر موارد، پاسخ همواره جاسوسی کردن بوده است. متجاوزان معمولاً بیشترین استفاده را از دسترسی به هدف و سرقت بی سر و صدای داده ها می برند. این مورد هم در خصوص جرائم سایبری با انگیزه های مالی و هم جاسوسی دیجیتال صدق می کند. پنهانی بودن و مداوم بودن این نوع جاسوسی هاست که ارزش دارد. سارقان دیجیتال حرفه ای نمی خواهند با تخریب داده ها یا ایجاد آثار فیزیکی، حضور خود را اعلام نمایند.

تعداد اندکی از موارد، که معمولاً توسط افرادی موسوم به هکتیویست ها انجام می شوند، شامل تخریب داده ها نیز هستند. اکثر ناظران چنین اقداماتی را همانند خرابکاری می دانند. متجاوز می خواهد قربانی را آشفته و خجالت زده کند، بنابراین به هدف مذکور نفوذ کرده، داده ها را به سرقت می برد، با نابود کردن فایل های کلیدی کامپیوترهای آن را از کار می اندازد، و سپس اخبار پیروزی ها و دستاوردهای خود را روی اینترنت منتشر می سازد. این مدل بسیار با دنیای CNE و CNA متفاوت است.

سه پرونده اخیر نشان می دهند که برخی افراد خارج از جوامع هکتیویست ها نیز به دنبال تخریب و ویرانگری هستند. در ماه اوت سال 2012، شرکت نفت دولتی عربستان سعودی، که با نام شرکت آرامکو عربستان نیز مشهور است، از یک تخریب دیجیتال آسیب دید. به گفته «عبدالله السعدان» ، یکی از معاونین شرکت، متجاوزین خارجی فایل هایی کلیدی را از بیش از 30.000 کامپیوتر پاک کردند. سرلشکر «منصور التركی»، سخنگوی وزارت کشور عربستان، اظهار داشت که «این حمله نتوانست به هدف نهایی خود، که متوقف ساختن جریان نفت عربستان بود، دست پیدا کند.» چند سال بعد، راس گاز، شرکتی با سهام مشترک متعلق به پترولیوم قطر و اکسون موبیل، و یکی از بزرگ ترین تأمین کنندگان گاز طبیعی مایع، گزارش داد که از یک حمله مشابه آسیب دیده است.

در تازه ترین مورد که در ماه مارچ سال 2013 به وقوع پیوست، حملات مخرب دیجیتالی بیش از 48 هزار کامپیوتر را در کره جنوبی تحت تأثیر قرار داد. سه ایستگاه تلویزیونی و سه بانک گزارش دادند که فایل های حیاتی سیستم ها توسط نرم افزارهای مخرب مورد حمله قرار گرفته اند و آثار این حملات، مشابه صدمات وارده به شرکت آرامکو عربستان و راس گاز بوده است. مقامات کره جنوبی این حملات را به کره شمالی نسبت دادند.

مهم است که در این زمینه، میان حملات دیجیتال که به طور موقت شبکه ها را مختل کرده، و حملاتی که داده ها را پاک می کنند، تمایز قائل شویم. نوع اول حملات با عنوان DDoS یا حملات «حمله توزیع شده محروم سازی از سرویس» (Distributed Denial of Service) شناخته می شود. در این روش متجاوزان، کامپیوترهای هدف را با ترافیک شبکه ای جعلی، غرق کرده و توانایی قربانی برای ارتباط با اینترنت و همچنین توانایی سایرین برای بازدید از شبکه های مورد حمله را کاهش می دهند. خسارت های ناشی از چنین حملاتی به محض این که متجاوز حمله را متوقف سازد، یا یک شرکت امنیتی به کمک قربانی بیاید، پایان می یابد. این نوع حمله روشی از حمله محروم سازی از سرویس(Denial of Service attack) (یا به اختصار DoS است که در آن حمله کننده با تعداد زیادی از کامپیوترها و شبکه هایی که در اختیار دارد، حمله را صورت می دهد. در این روش تمام رایانه ها یکی از روش های حمله را که در ذیل ذکر شده اند را همزمان با هم انجام می دهند که ممکن است در برخی موارد خسارات جبران ناپذیری را به بار آورد.

حملات پاک کردن داده ها، مخرب تر هستند. هنگامی که یک متجاوز داده ها را نابود می سازد، به طور کلی مطالب را از هارد درایو هدف پاک می کند. اگر هیچ کپی دیگری از داده ها وجود نداشته باشد، آن ها برای همیشه از دست می روند. اگر سیستم آسیب دیده، یک عملیات تجاری بسیار مهم را اجرا کند، آن عملیات تا وقتی که کامپیوتر بازسازی یا فرمت شود دچار اختلال خواهد شد. به عنوان مثال، متجاوزی که به محاسبات کنترل کننده یک دستگاه رزونانس مقناطیسی یا روباتی که قطعات خودرو را پرس می کند، حمله می نماید، می تواند به شکلی موثر تجارت و کسب وکار را متوقف سازد.

این موضوع را باید به یاد داشت که در فضای سایبری، توانایی سرقت، معادل با توانایی نابودسازی است. در تمامی این سه پرونده (شرکت آرامکو عربستان، راس گاز، و کره جنوبی) ، متجاوزین احتمالاً به شکلی یکسان عمل کردند. متهاجمان احتمالاً خیلی راحت می توانستند تصمیم بگیرند که روزها، هفته ها، یا ماه ها به جاسوسی از این شرکت ها بپردازند. اگر بازرسان موفق می شدند متجاوزان را شناسایی کرده و متهاجمان را بیرون کنند، برخی مفسران ادعا می کردند که این حمله هم یک مورد دیگر از جاسوسی های بی ضرر بوده است. هر چه باشد، متجاوزان هنگامی که آزادانه در شبکه های قربانی پرسه می زدند، نگاهی هم به داده ها انداخته اند. با این حال، حقیقت این است که در فضای سایبری، توانایی سرقت، معادل با توانایی نابودسازی است. هر نمونه ای از بهره برداری از شبکه های کامپیوتری، یک پرونده بالقوه از حمله به شبکه های کامپیوتری است.

مبحث پنجم: راهکارهای که باید برای مقابله با جاسوسان سایبری

پرداختن به این مسئله نیازمند در نظر گرفتن چند مرحله است. اول اینکه سیاست گذاران باید نگرش های بی قید و آسانگیرانه خود نسبت به «جاسوسیِ صِرف» را به شکلی مناسب بازبینی کنند. درست است، برخی از متجاوزان احتمالاً اعمال خود را به جاسوسی محدود کرده و تصمیم می گیرند خسارتی وارد نکنند؛ اما همه چنین لطفی نخواهند کرد. دوم این که، سازمان هایی که هدف حمله قرار می گیرند باید بدانند که متجاوزان به طور معمول به شبکه های آن ها نفوذ می کنند. هر کسی که یک شبکه را راه اندازی می کند، باید یک ذهنیت شکارچی وار را هم در خود ایجاد کند، و سعی کند عملیاتی انجام دهد که متجاوزین را پیش از این که تصمیم بگیرند داده ها را سرقت کرده یا نابود نمایند، ردیابی و شناسایی کند. سوم این که، سازمان ها باید با همنوعان خود، شرکت های تأمین کننده موارد ایمنی که قابل اعتماد و درستکار هستند، و نهادهای دولتی همکاری کنند تا اطلاعات مربوط به تهدیدها را به قالب هایی استاندارد شده و دستگاه خوان نظیر قالب OpenIOC از ماندیانت، یا بیان ساختار یافته اطلاعات تهدیدی از MITRE تغییر دهند.

هنگامی که یک سازمان از تهدیدها آگاه شود، می تواند از شرکتی نظیر ماندیانت بخواهد که به جستجوی متجاوزان پرداخته و پس از یافتن آن ها، بیرونشان کند. ماندیانت از ترکیبی از ابزارها و اطلاعات برای ارزیابی مدارک و شواهد به دست آمده از شبکه ها، کامپیوترها و برنامه های کاربردی استفاده می کند تا تهدیدهای نهان را کشف کرده و به قربانیان کمک کند که شبکه خود را به یک وضعیت قابل اعتماد بازگردانند.

باید با جاسوسان سایبری مقابله جدی کرد، سازمان ها زمانی که بتوانند متجاوزین را سریعاً در شبکه های خود شناسایی کرده و پیش از این که دشمن مأموریت خود را (هر چه که هست) تکمیل نماید، او را از بین ببرند، پیروز خواهند بود. دیگر بیش از نمی توانیم پشت این طرز فکر که فعالیت های متجاوزانه را می توان تحمل کرد چون هدفشان صرفاً جاسوسی است، پنهان شویم.[1]

نتیجه

در نهایت به این نتیجه می رسیم که جاسوسی عملاً در روابط بین کشور وجود دارد و نمایندگان سیاسی کشور ها با سوء استفاده از مصونیت ها و صلاحیت های اعطا شده مطابق کنوانسیون وین در مورد روابط دیپلماتیک به این امر غیر قانونی می پردازند.

کشور ها برای مبارزه با این پدیده قوانین داخلی تصویب نمایند و از طرف دیگر درامر تشخیص عناصر مطلوب دقت به خرچ دهند.

در سطح بین المللی نیاز است تا به این مسئله تلاش های جمعی صورت گیرد و معاهداتی به توافق کشور ها ایجاد شود.

[1]. ر.ک به: ویب سایت: http://www.irdiplomacy.ir/fa/page/1916099

منابع و مأخذ

أ. کتاب ها

1. صدر، دکتر جواد، حقوق دیپلماتیک و کنسولی، چاپ سیزدهم، تهران: انتشارات دانشگاه تهران، 1392.
2. ذوالعین، پرویز، حقوق دیپلماتیک، چاپ دوم، تهران: انتشارات وزارت امور خارجه، 1384
3. خالوزاده، سعید، حقوق دیپلماتیک و کنسولی، تهران: انتشارات (سمت)، 1392
4. ساجدی، احمد، سازمان های جاسوسی جهان، تهران: انتشارات محراب قلم،

ب. ویب سایت ها:

1. ویب سایت: http://www.magiran.com
2. ویب سایت: http://en.wikipedia.org/wiki/Stuxnet
3. ویب سایت: http://www.washingtonpost.com/world
4. ویب سایت: http://www.hamshahrionline.ir/details/28738
5. ویب سایت: http://kohnesarbazeirani.blogfa.com/post-68.aspx
6. ویب سایت: http://fararu.com/fa/news/116595
7. ویب سایت: http://ahaad.ir/s/9871
8. ویب سایت: http://news.netcraft.com/archives/2012/10/02/october-2012-web-server-survey.html
9. ویب سایت: http://www.bcatc.ir/fa/87-student-s-basij/cyber/154
10. ویب سایت: http://www.iranamerica.com/forum/showthread.php?t=19255
11. ویب سایت: http://www.ictpress.ir
12. ویب سایت: http://fa.wikipedia.org/wiki/%D8%AC%D8%A7%D8%B3%D9%88%D8%B3%DB%8C_%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C
13. ویب سایت: http://www.irdiplomacy.ir/fa/page/1916099