فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال چهارم / شماره اول (شماره پیاپی ۱۳) / بهار ۱۴۰۴
وبگاه مجله: https://sanad.iau.ir/journal/cyberlaw
ISSN: 2821-126X

Cyber attacks of the Mojahedin Khalq Organization and the International Law on the Use of Force (with an emphasis on Albania's international responsibility)

Ehsan sadeghipoor
Department of Law, ST.C., Islamic Azad University, Tehran, Iran
Mahmoud Ganj Bakhsh
Department of Economics and Islamic Banking, Faculty of Economics, Kharazmi University, Tehran, Iran (Corresponding Author)
Email: Ganjbakhsh@khu.ac.ir
Kourosh Jafarpour
Department of Private Law, ST.C., Islamic Azad University, Tehran, Iran

DOI:

Keywords:
Cyber Attack, Mojahedin Khalq Organization, Self Defence, Islamic Republic of Iran, Albania

Abstract

The capabilities that the cyberspace has brought to human society have caused a number of non-governmental actors to abuse this potential for their political purposes. In fact, the Mojahedin Khalq after being expelled from Iraq and transferred to Albania, which caused them to move away from Iran's borders and severely restrict them from carrying out terrorist operations inside the country (Iran), they focused most on cyber actions and espionage activities. Arguably, defense against non-state actors is at least sometimes legal. However, due to the emergence of new types of terrorism such as cyber terrorism, which may endanger international peace and security at once, international law has been unable to establish new rules appropriate to the cyber space. The question raised in this research is how the possibility of resorting to self-defence on the part of the Islamic Republic of Iran against the cyber terrorism attacks of the Mojahedin Khalq (hypocrites) is justified and following that, what is the legal status of Albania according to the rules of international responsibility law? In this regard, in order to answer this problem, a descriptive-analytical research method has been used using library tools. Therefore, after the investigation, the present study concludes that if a cyber attack on critical infrastructures that has comparable damages to conventional weapons, gives the affected government the possibility of resorting to self-defence. It is very clear that this will not mean ignoring the international responsibility of the government that has supported or sheltered terrorist groups.

فصلنامه علمی
مطالعات حقوقی فضای مجازی

صفحات مقاله ۱ الی ۱۱

حملات سایبری سازمان مجاهدین خلق و حقوق بین‌الملل توسل به زور (با تأکید بر مسؤلیت بین المللی آلبانی)

احسان صادقی پور

گروه حقوق بین الملل عمومی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران

محمود گنج بخش

گروه اقتصاد و بانکداری اسلامی، دانشکده اقتصاد، دانشگاه خوارزمی، تهران، ایران

(نویسنده مسئول) پست الکترونیک: Ganjbakhsh@khu.ac.ir

کوروش جعفرپور

گروه حقوق خصوصی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران

تاریخ دریافت : ۱۰ شهریور ماه ۱۴۰۳ تاریخ پذیرش: ۵ دی ماه ۱۴۰۳

چکیده

ظرفیت هایی که فضای سایبر برای جامعه بشری به ارمغان آورده است باعث گردیده تعدادی از بازیگران غیردولتی از این پتانسیل برای مقاصد سیا سی خود سوء ا ستفاده نمایند. به‌واقع مجاهدین‌خلق پس از اخراج از عراق و انتقال به آلبانی که موجب دور شدن آن‌ها از مرزهای ایران و محدودیت شـدید آن‌ها برای انجام عملیات‌های تروریسـتی در داخل کشـور (ایران) شـد، بیشـترین تمرکز خود را به روی اقدامات سـایبری و فعالیت‌های جاسوسی قرار دادند. مبرهن است دفاع در برابر بازیگران غیردولتی حداقل در برخی مواقع قانونی است. اما به لحاظ ظهور گونه های جدید تروریسم مثل تروریسم سایبری که ممکن است به یک باره صلح و امنیت بین المللی به مخاطره بیفتد موجب گردیده است که حقوق بین الملل از و ضع قواعد جدید متنا سب با فضای سایبری عاجز بماند. سؤالی که در این تحقیق مطرح می‌گردد این ا ست که امکان تو سل به دفاع مشروع از سوی جمهوری‌اسلامی‌ایران در برابر حملات تروریسم سایبری مجاهدین‌خلق (منافقین) چگونه توجیه می‌شود و به دنبال آن بر اساس قواعد حقوق مسؤلیت بین‌المللی آلبانی چه وضعیت حقوقی دارد؟ در این راستا جهت پاسخگویی به این مسأله از روش تحقیق توصیفی-تحلیلی با ا ستفاده از ابزار کتابخانه‌ای بهره گرفته شده است. بنابراین پس از بررسی، پژوهش حاضر نتیجه می‌گیرد چنانچه حمله سایبری به زیرساخت های حیاتی که خسارات قابل قیاس با سلاح‌های متعارف داشته باشد، امکان توسل به دفاع مشروع را به دولت زیان‌دیده می‌دهد. پر واضح است این امر به معنای نادیده گرفته شدن م سؤلیت بین‌المللی دولتی که از گروه های تروریـستی حمایت کرده و یا به آن ها پناه داده ا ست، نخواهد بود.

واژگان کلیدی: حمله سایبری، سازمان مجاهدین خلق، دفاع مشروع، جمهوری اسلامی ایران، آلبانی

مقدمه

تحول و پیشرفت فناوری‌های اطلاعاتی و ارتباطی به گروه‌های تروریستی این امکان را داده است تا به سرعت و به راحتی از یک مکان به مکان دیگر انتقال یابند. این تغییرات سبب شده است تا اقدامات تروریستی طی دهه های اخیر وسعت جغرافیایی بیشتری یابد و با افزایش چشمگیر، ترس و وحشت حاصل از این اقدامات در میان عامه مردم رسوخ کند. در سال‌های اخیر تروریسم از حالت سنتی خارج شده و اشکال مدرن آن تحت عنوان موج تروریسم جدید در حال گسترش است. تروریسم سایبری از جدیدترین مصادیق آن می‌باشد که از تلاقی اعمال تروریستی و فضای سایبر[1] پا به عرصه وجود نهاده است. به عبارتی تروریسم سایبری، با وجود نوظهور بودن به مراتب خطرناک تر از تروریسم سنتی است و تهدیدات آن برای امنیت ملی کشورها به خطری بالقوه تبدیل شده است. لذا این پژوهش بر این نظریه استوار است که علی رغم عدم اجماع بر سر مفهوم تروریسم، جامعه بین المللی درباره مبارزه با تروریسم متفق القول بوده است و بدین سبب تلاش‌های بسیاری برای مبارزه با این پدیده انجام داده است. طی سال‌های اخیر با گسترش چشمگیر حملات مسلحانه تروریستی خصوصاً پس از ۱۱ سپتامبر ۲۰۰۱ عملکرد دولت‌ها و رویه‌ی بین‌المللی حاکی از پذیرش حق دفاع مشروع کشورها علیه حملات تروریستی از جانب بازیگران غیردولتی می‌باشد. بدین وسیله از نظر سنتی حمله مسلحانه فقط به حملاتی که از جانب دولت‌ها صورت می‌گرفت اطلاق می‌شد اما به رسمیت شناختن این که اعمال کنشگران غیردولتی می‌تواند منجر به یک حمله مسلحانه شود، یقیناً تحولی انقلابی در حقوق بین الملل است. مسأله مورد بحث در این مقاله، این است که امکان توسل به دفاع مشروع از سوی جمهوری اسلامی ایران در برابر حملات تروریسم سایبری مجاهدین خلق (منافقین) چگونه توجیه می‌شود و به دنبال آن بر اساس قواعد حقوق مسؤلیت بین المللی آلبانی چه وضعیت حقوقی دارد؟

پس با توجه به آنچه در ماده ۵۱ منشور ملل متحد آمده است، ضرورت دارد تا حملات سایبری مجاهدین خلق پیرامون مفهوم حمله مسلحانه به عنوان یک عنصر اساسی در بحث دفاع مشروع مورد تأمل و بررسی قرار بگیرد. امری که به نظر می‌رسد در خصوص حملات سایبری گروه تروریستی مزبور فعلاً به نقطه لازم نرسیده است. لکن چنانچه در آینده شدت حملات به حد مفهوم حمله مسلحانه برسد، این حق برای جمهوری اسلامی ایران مسلم خواهد شد. از طرف دیگر این مسأله به معنای نادیده گرفتن مواضع حقوقی–سیاسی ایران در محافل بین‌المللی و مذاکره با دولت آلبانی برای استرداد سران مجاهدین خلق نخواهد بود موضوعی که در خصوص مسؤلیت بین المللی دولت آلبانی حداقل تا ۲۰ ژوئن ۲۰۲۳ جهت جلب رضایت ایران کاملاً مشهود است. این پژوهش به واکاوی ماهیت حملات سایبری سازمان مجاهدین خلق از منظر حقوق بین الملل می‌پردازد. بر این اساس ابتدا گزارشی از حملات سایبری این گروه و ترویسم سایبری ارائه می‌شود، سپس حملات سایبری از منظر قاعده منع توسل به زور مورد تحلیل قرار می‌گیرد. همچنین به طور ویژه، حملات سایبری مجاهدین خلق (منافقین) از نگاه ماده ۵۱ منشور ملل متحد مورد ارزیابی قرار می‌گیرد و در نهایت موضوع مسؤلیت بین‌المللی کشور آلبانی در این رابطه مورد تحلیل قرار می‌گیرد.

۱. مجاهدین خلق و حملات سایبری به جمهوری اسلامی ایران (شرح واقعیات)

در دو سال اخیر این گروه تروریستی به واسطه فاصله سرزمینی قابل توجه، با رخنه در خلاءهای محیط سایبر در پی حملات سایبری به زیرساخت‌های دولتی برآمده است. در اولین اقدام سایبری هک صدا و سیمای جمهوری اسلامی در تاریخ ۷ بهمن ۱۴۰۰ را مرتکب شدند. گروهی سایبری وابسته به سازمان مجاهدین خلق مسؤلیت این اقدام را بر عهده گرفتند که در پی آن چند شبکه ی تلویزیونی قطع شد (صدای ایران،

[1] . Cyber Space

۱۴۰۰: ۱). در تصدیق این حمله یکی از مدیران صدا و سیما در این زمینه بیان کردند که احتمالاً سرورهای صدا و سیما مورد حمله هکری قرار گرفته است (اقتصاد نیوز، ۱۴۰۰: ۱). در دومین اقدام در روز دوشنبه ۲۳ اسفند ۱۴۰۰ این گروه اعلام کرد چندین سامانه و سایت وزارت فرهنگ و ارشاد اسلامی را از دسترس خارج کرده و اسناد آن را در اختیار خود گرفته است (نو اندیش، ۱۴۰۰: ۱). حدود دو ماه بعد روز دوشنبه ۵ اردیبهشت ۱۴۰۱ این گروه هکری از اقدام جدید خود علیه سایت‌ها و سامانه‌های وزارت جهاد کشاورزی جمهوری اسلامی خبر داد (جامعه ۲۴، ۱۴۰۱: ۱). در ۱۲ خرداد ۱۴۰۱ سایت شهرداری و دوربین‌های کنترلی شهرداری تهران را هک کردند. خبرگزاری رسمی ایران نیز در این باره نوشت که براساس پیگیری‌های صورت گرفته، بخشی از شبکه دوربین‌های نظارتی شهرداری و همچنین زیرساخت‌های خدماتی همچون سایت تهران من، سایت شهرداری تهران و نیز بخشی از سامانه‌های داخلی همچون اتوماسیون داخلی و دیگر سامانه‌های ارتباطی کارکنان شهرداری تهران مختل شده است (انصاف، ۱۴۰۱: ۱). هک وب سایت‌های وزارت خارجه جمهوری اسلامی ایران در ۱۷ اردیبهشت ۱۴۰۲ و دسترسی به اسناد و مدارکی بنا به ادعای گروه (فارس، ۱۴۰۲: ۱). در همه‌ی این موارد گروه هکری وابسته به سازمان مجاهدین خلق مسؤلیت حملات سایبری را برعهده گرفتند. در واقع مقامات آلبانی حدود یک دهه پیش با سوء استفاده‌های سیاسی از قواعد حقوق بین‌الملل موافقت کردند که به این گروه به دلایل به ظاهر بشردوستانه سرپناه بدهند اما به شرطی که این گروه از مشارکت در برخی فعالیت‌های سیاسی خودداری کند و اگر سوء ظن استفاده این گروه از خاک آلبانی برای انجام حملات سایبری یا طرح ریزی و تأمین مالی فعالیت‌های تروریستی اثبات شود، احتمالاً موقعیت آن ها به خطر می افتد. چنین فعالیت‌هایی نه تنها توافقنامه را نقض می‌کند، بلکه تهدیدی آشکار برای امنیت ملی آلبانی است. به دنبال اثبات این موضوع در خرداد ۱۴۰۲ پلیس ایالتی شهر دورس آلبانی با حکم قضایی و با هدف مبارزه با تروریسم و پیشگیری از حملات سایبری وارد محوطه مقر این سازمان تروریستی شد.

۲. تروریسم سایبری

تروریسم نوین از قابلیت‌ها و امکانات دنیای مدرن بهره می‌برد. به طوری که گروه مزبور در یک منطقه از جهان برنامه ریزی عملیات را بر عهده می‌گیرد اما در هزاران کیلومتر دورتر عمل تروریستی به منصه ظهور می‌رسد. به عبارتی فناوری‌های نوین، هدف گیری تروریستی را آسان‌تر و مقابله با آن را مشکل تر ساخته است. در حال حاضر ما شاهد موج پنجم تروریسم یا همان تروریسم سایبری هستیم. چرا که فناوری سایبری با از بین بردن مرزها، تهدیدات خطرناک و نوینی را برای تمدن بشری به ارمغان آورد (فرشاسعید و همکاران، ۱۴۰۱: ۱۷۲).

از آن جا که بحث تروریسم سایبری به دلیل نوظهور بودن فضای سایبر جدید است و همانند تروریسم سال‌ها موضوع تحقیق و مطالعه نبوده است، نمی‌توان انتظار داشت به آن اندازه تعاریف و تحلیل‌های گوناگون موجود باشد. به عبارتی در مورد تعریف پدیده تروریسم سایبری به مانند تروریسم اجماع تعریف بین کارشناسان این حوزه وجود ندارد و همچنان واژه ای بحث برانگیز است (فضائلی، ۱۴۰۲: ۱۱۵). اصطلاح تروریسم سایبری را اولین بار محقق ارشد موسسه امنیت و اطلاعات کالیفرنیا باری کالین،[1] به کار برد (رزمخواه، ۱۴۰۲: ۵). از نظر وی سایبر تروریسم: سوءاستفاده عمدی از یک سیستم، شبکه یا مؤلفه اطلاعاتی رایانه ای برای تحقق هدفی که مؤید یا تسهیل کننده اقدام تروریستی باشد (Collin, 1997: 15-18) یا دوروتی دنینگ[2] استاد علوم رایانه ای در سال ۲۰۰۱ تروریسم سایبری را چنین تعریف می نماید: حملات غیرقانونی و تهدید علیه رایانه‌ها، شبکه و اطلاعات به منظور ارعاب مردم و حاکمیت برای پیشبرد اهداف سیاسی و اجتماعی می‌باشد (امیرلی و

[1] . Barry Collin
[2] . Dorothy E. Denning

ثقفی، ۱۳۹۸: ۳۹۵). نبرد در محیط سایبر به دلیل ارزان بودن حملات، مجهول ماندن هویت حمله کنندگان، مشکلات موجود در بحث انتساب و مبهم بودن قواعد قابل اعمال در فضای سایبر در مقایسه با جنگ های سنتی از استقبال بیشتری برخوردار است. فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می توان اقدامات خطرناکی را در مدت زمان کم و با سرعت بالایی انجام داد. هر فرد برای انجام حمله سایبری تنها به ارتباط اینترنتی، یک رایانه و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. البته، انجام حملات سایبری شدیدتر مستلزم صرف هزینه‌های بالاتری است. بنابراین فضای سایبری و فناوری‌های مرتبط با آن یکی از مهمترین منابع قدرت در هزاره سوم می‌باشند (Li & Liu, 2021: 8184). حمله ویروس استاکس نت به تأسیسات هسته ایران نمونه بارزی از حمله سایبری است. استاکس نت به عنوان کرم صنعتی با هدف حمله سایبری به زیر ساخت‌های حیاتی صنعت ایران و آسیب رسانی به تأسیسات هسته ای نطنز طراحی و منتشر شده بود. مورد دیگر، براساس گزارش‌ها القاعده اطلاعات خود درباره هدف‌هایش را از راه اینترنت بدست می‌آورد و از همان راه نیز رمزگذاری می‌کرد.

در سپتامبر ۲۰۰۲، گزارش ها نشان می‌دهند که سلول‌های القاعده در آمریکا برای ارتباط با سلول‌های این گروه در مناطق دیگر، از تلفن اینترنتی بهره می‌برده اند. این رویدادها نشان می‌دهند که اینترنت به یک ابزار جنگ مجازی برای تروریست‌ها تبدیل شده است. بدین گونه تروریست سایبری می تواند با از کار انداختن امکانات فنی، رایانه‌ها را که زندگی اجتماعی، و اقتصادی مردم وابسته با آن است، در مقیاس وسیع تری بر آن‌ها زیان رسانیده و در سطح گسترده‌تری کشتار راه بیندازد و نیز از طریق تهدید به حمله بیشتر، از طرف‌های مقابل خود امتیاز بگیرد. به هر حال، امروزه دنیای رایانه، دنیایی است که هر لحظه مورد تهدید تروریست‌ها است و احتمال حملات آتی هر چه بیشتر مردم را دچار وحشت می‌کند. در واقع این برآیند از این واقعیت نشأت می‌گیرد که حملات تروریسم سایبری علاوه بر زیرساخت‌های مالی، می‌تواند پایه‌های مربوط به اماکن حساس دولتی و یا حیاتی را شامل شود در نتیجه این امر منجر به فجایع گسترده انسانی و یا زیست محیطی شود (Hansen et.al., 2007: 4).در تعریف تروریسم، مشخص است که ضرورتی ندارد که خشونت فیزیکی باشد. خشونت در هر شکل آن می‌تواند موجبات تحقق اقدامات تروریستی را فراهم آورد. باید گفت که حتی وقوع خشونت هم نیاز نیست، زیرا صرف تهدید به خشونت هم اقدام را تروریستی می‌کند. تروریست با استفاده از خشونت سعی دارد تا دلهره بی پایانی را در جامعه ایجاد کند و دامنه آن را علاوه بر قربانیان مستقیم خود به خیل عظیمی از بینندگان نیز تعمیم دهد. بنابراین مفهوم خشونت امری نسبی است که ممکن است شدت آن متناسب با زمان و مکان کم یا زیاد شود.

۳. حملات سایبری و ممنوعیت تهدید و توسل به زور در حقوق بین‌الملل

ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلالی می‌تواند تأثیرات و پیامدهای به مراتب بیشتری از جنگ در فضای واقعی در پی داشته باشد. در نتیجه دولت‌ها و موجودیت های غیردولتی برای رسیدن به اهداف سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی به قدرت سایبری متوسل می‌شوند. از سوی دیگر از آن جا که فضای سایبر فضایی مبتنی بر بی نامی است و حملات در این فضا بسیار ارزان تر و سریع تر از روش های سنتی و انتساب در حملات سایبری امری دشوار است، از این میدان نبرد استقبال زیادی شده و دلیلی شده برای دولت‌ها که به این نتیجه برسند که استفاده از سلاح‌های سایبری به جای استفاده از سلاح های سنتی می‌تواند امتیاز زیادی به ارمغان بیاورد (اسمعیل زاده ملاباشی و همکاران، ۱۳۹۶: ۵۴۰). پر واضح است منشور ملل متحد در بند ۴ ماده ۲ تصریح می‌دارد: کلیه اعضا در روابط بین‌المللی خود از کاربرد یا تهدید به کاربرد زور علیه تمامیت سرزمینی یا استقلال سیاسی هر دولت دیگر و نیز از هر عملی که به نحوی از انحاء مغایر با اهداف ملل متحد باشد، خودداری خواهند کرد. مسأله ای که مطرح می‌شود این است که آیا حمله سایبری می‌تواند نقض بند ۴

ماده ۲ منشور تلقی شود؟ بند ۴ ماده ۲ منشور ملل متحد بدون آن که تعریفی از زور ارائه دهد، ممنوعیت تهدید و توسل به زور را اعلام می‌کند، ممنوعیتی که در عین ابهام، بی‌پروا است و طبیعت پیچیده‌ی آن مهیای تحلیل‌های مختلف است. رویکرد عمومی آن است که هر گونه توسل به زور با بند ۴ ماده ۲ منشور ملل متحد مغایرت خواهد داشت مگر تحت استثنائاتی (فلک و همکاران، ۱۳۸۷: ۲۰-۱۹). منشور عبارت توسل به زور را به کار برده است. بنابراین می‌توان گفت لفظ مسلحانه به معنی تجهیز به یک سلاح یا درگیری با استفاده از یک سلاح است (Garner, 2009: 123). سلاح نیز ابزار مورد استفاده یا طراحی شده برای استفاده جهت صدمه زدن به دیگری یا قتل وی است. تقریباً تمامی اشیاء می‌توانند به عنوان سلاح به کار روند؛ در صورتی که قصد دارنده‌ی آن خصمانه باشد. دیوان بین‌المللی دادگستری در نظر مشورتی خود در خصوص مشروعیت تهدید یا استفاده از سلاح‌های هسته‌ای، تصریح می کند که بند ۴ ماده ۲، و همچنین مواد ۵۱ و ۴۲ منشور ملل متحد به سلاح خاصی اشاره نکرده اند. آن‌ها بر هر گونه توسل به زور، صرف نظر از سلاح مورد استفاده اعمال می‌شوند (ICJ Reports, 1996: para39).

بعبارتی رأی مذکور تاییدی است غیرمستقیم بر این مسأله که عملیات سایبری می‌تواند از مصادیق توسل به زور تلقی شود (Melzer, 2011: 21-24). به طور خاص، سخت افزار، نرم افزار و کدهای حمله از طریق شبکه رایانه، سلاح هایی هستند که می‌توانند از طریق انتقال جریان داده‌ها به ایراد خسارت منجر شوند (شایگان و صفوی کوهساره، ۱۳۹۷: ۴۲۶). بنابراین، لزومی ندارد تسلیحات مذکور برای اهداف تهاجمی ساخته شده باشند و یا دارای آثار انفجاری باشند (ICJ Reports, 1986: para228). در سال ۱۹۴۵ منشور ملل متحد نه تنها جنگ تجاوزکارانه، بلکه هرگونه تهدید یا استفاده از زور را نیز منع می‌کند. بنابراین منشور ملل متحد جهت توسل به زور دو ساز و کار را به رسمیت شناخته است، اول امنیت جمعی بر مبنای ماده ۳۹ و مواد بعد از آن دوم دفاع مشروع فردی یا جمعی بر مبنای ماده ۵۱. با این استدلال اگرچه جهان شمولی شناسایی و پذیرش منع توسل به زور و اهمیت نظری و عملی آن موجب شده آن را در زمره قواعد آمره حقوق بین‌الملل به شمار آورند اما در بعضی از موارد استفاده از زور می‌تواند مشروع باشد و بدیهی است هدف دفاع مشروع صرفاً دفع تجاوز دشمن است.

۱,۳ امکان سنجی توسل به دفاع مشروع جمهوری اسلامی ایران در برابر حملات تروریسم سایبری سازمان مجاهدین خلق

با تصویب قطعنامه ۱۳۶۸، شورای امنیت با استناد به ماده ۵۱ منشور ملل متحد بر حق ذاتی دفاع مشروع فردی و جمعی دولت‌ها در مقابل تروریست تأکید نمود. به عبارتی شورای امنیت مسیر را برای این گفتار که ماده ۵۱ منشور، علاوه بر این که حاکم بر روابط میان دولت است، بر روابط میان دولت‌ها و کنشگران غیردولتی نیز حاکم است، هموار کرد. در حقیقت منشأ حمله از منظر منشور موضوعیت ندارد (Martínez Sponda, 2023: 72). این جمله بندی به اندازه کافی عام تدوین شده است تا اجازه استناد به دفاع مشروع، در برابر حمله مسلحانه، از جانب موجودیت‌های غیردولتی را نیز می‌دهد. حتی رویه دولت‌ها نیز در تحول است رویه همراه با اعتقاد حقوقی دولت‌ها از این نظر پشتیبانی می‌کند که کنشگران غیردولتی نیز مرتکب حمله مسلحانه می‌شوند و بدین ترتیب در مقابل آن حق دفاع مشروع به وجود می‌آید، که چنین روندی می تواند منجر به شکل گیری قاعده عرفی بین‌المللی باشد. در برخی مواقع بازیگران غیردولتی با استفاده از امکاناتی که محیط سایبر در اختیار آن‌ها قرار داده بدون این که گلوله ای شلیک شود اعمالی را مرتکب می‌شوند که خسارات ناشی از آن بسیار بالاتر از خسارات جنگ‌های مسلحانه است. بنابراین پرسشی که مطرح می شود این است که کشور قربانی توسل به زور سایبری در صورت تلقی چنین حمله‌ای به عنوان یک حمله مسلحانه، می‌تواند به دفاع مشروع متوسل شود؟ به طور کلی به نظر می‌رسد که با توجه به تکامل جنگ افزارها و منطق مستتر در بند ۴ ماده ۲ منشور،

محدودیتی برای گسترش ممنوعیت موجود در آن به منظور در برگرفتن موارد نوین استفاده از زور نمی‌گردد چون این مقرره به صراحت به نیروی مسلح یا نظامی اشاره نمی‌کند (Segura-serrano, 2006: 224-225). اما نکته قابل توجه در خصوص نبرد سایبری این است که برخی حملات در فضای سایبر را باید در درجه ای پایین‌تر از جنگ قلمداد کرد چرا که از شدت کمتری برخوردارند (Cornish et.al. 2010: 10). در آوریل ۲۰۰۷ تعدادی از تارنماهای مهم نهادهای دولتی کشور استونی مانند تارنمای ریاست جمهوری، پارلمان، وزارتخانه‌ها، احزاب سیاسی، رسانه‌های خبری و دو بانک مهم این کشور مورد حمله سایبری قرار گرفتند و در این میان، اتهام متوجه روسیه شد. اما ناتو اعلام کرد در این بازه زمانی، حملات سایبری را یک کار نظامی مسلم نمی‌شناسد تا ماده (۵) پیمان ناتو درباره دفاع دسته جمعی مورد استناد قرار گیرد یا در درگیری میان روسیه و گرجستان در سال ۲۰۰۸، تأثیرات حمله سایبری بسیار محدود بوده و حتی از لحاظ زمانی نیز این حملات به اندازه ای طول نکشیدند که بخواهند تشکیل یک حمله مسلحانه بدهند (قاسمی و نامدار، ۱۳۹۷: ۲۱۲). در این جا هر حمله سایبری علیه شبکه رایانه ای هر ساختاری را نمی‌توان حمله مسلحانه سایبری دانست، به عبارتی در این جا مقوله زیرساخت های حیاتی نقش بسیار اساسی دارد، چرا که این ساختارها باید زیرساخت‌های بنیادین باشند (میرعباسی و کورکی نژاد قرایی، ۱۳۹۷: ۲۷۳). می‌توان مصادیق زیرساخت‌های حیاتی را به دسته‌های ذیل تقسیم نمود: جمعیت، انرژی، بانک مرکزی، ارتباطات، خدمات (از جمله خدماتی مالی، توزیع غذا و مراقبت های بهداشتی) حمل و نقل، تأسیسات هسته ای، ساختمان‌های دولتی، سدها، دارایی‌ها و اماکن تجاری، پایگاه ها و تأسیسات نظامی (نعمت پور و همکاران، ۱۴۰۰: ۱۷۲). در خصوص موضوع مقاله مستنداتی در دست است که نشان می‌دهد سازمان مجاهدین خلق از خاک کشور آلبانی در دو سال اخیر اقدام به حملات سایبری علیه سازمان‌های دولتی و غیردولتی ایران کرده است مثل هک دوربین‌ها و وب سایت‌های شهرداری، شبکه‌های صدا و سیما، وب سایت‌های وزرات امور خارجه و نهاد ریاست جمهوری. ضمن پذیرش مسؤلیت این حملات از سوی این گروه، طبق گفته منابع آلبانیایی پلیس این کشور سرورهایی از محل استقرار مجاهدین خلق کشف کرده‌اند که نشان می‌دهد که از طریق این تجهیزات کامپیوتری مرتکب حمله سایبری می‌شدند. این حقیقت که حملات سایبری فاقد شدت لازم نقض بند ۴ ماده ۲ تعبیر نمی‌شوند، به معنای مشروعیت آن‌ها نیست. حمله به سیستم کنترل حمل و نقل هوایی و یا اختلال در نیروگاه‌های اتمی می‌توان با اطمینان بیان نمود که خسارات مادی و تلفات جانی منتج از آن قابل پیش بینی بوده اما در مورد حمله به وب سایت‌های صدا و سیما یا چند وزارت خانه قدری ابهام وجود دارد. چرا که مطابق دکترین نتیجه محور فلسفه اصلی دفاع مشروع جلوگیری از ورود خسارت‌های مالی و جانی به یک کشور است. لکن جمهوری اسلامی ایران گزینه های حقوقی و سیاسی مختلفی را پیش رو دارد که می تواند برای دفاع از خود در برابر چنین حملاتی در آینده به این تدابیر متوسل شود. مواضع سیاسی ایران در این خصوص قاعدتاً بر تدابیر و راهکارهای حقوقی نیز تاثیرگذار هستند.

۴. مسؤلیت بین‌المللی دولت آلبانی در چارچوب طرح کمیسیون حقوق بین‌الملل ۲۰۰۱

پر واضح است که طبق قواعد مسؤلیت بین‌المللی طرح کمیسیون حقوق بین‌الملل، هر عمل متخلفانه بین‌المللی دولت، مستلزم مسؤلیت بین المللی آن دولت است. مسؤلیت ناشی از عمل، چه به صورت فعل و چه به صورت ترک فعل، زمانی محرز است ۱. طبق حقوق بین‌الملل قابل انتساب به آن دولت باشد. ۲. موجب نقض تعهدات بین‌المللی دولت باشد. این طرح در واقع انعکاس حقوق بین‌الملل عرفی است و بنابراین برای همه دولت‌ها الزام آور است (ابراهیم گل، ۱۳۹۶: ۳۰). نکته قابل توجه این است که این الزام در خصوص بازیگران دولتی مجری است بدین ترتیب اصولاً رفتار یا اعمال اشخاص خصوصی اعم از حقیقی یا حقوقی را نمی توان به عنوان عمل خلاف بین‌المللی محسوب و به کشور منتسب نمود و او را مسؤل شناخت. این قاعده را می توان از مفهوم مخالف ماده ۵ طرح مواد راجع به مسؤلیت به دست آورد. با این حال، ممکن است در

مواردی اعمال و رفتار اشخاص خصوصی در قلمرو یک کشور، موجبات مسؤلیت بین‌المللی آن کشور را فراهم نماید. از جمله این که اگر رفتار اشخاص ناشی از عدم پیش بینی و پیشگیری از وقوع تخلف و یا عدم کفایت کنترل، کوتاهی یا عدم مراقبت لازم در این امر از سوی ارکان دولتی باشد. بدین ترتیب مسأله مسؤلیت بین‌المللی دولت‌ها ناشی از حملات سایبری بازیگران غیردولتی با چالش اساسی مواجه است. در حقیقت، فقدان مرز در فضای سایبری سبب شده است شناسایی منشأ حمله سایبری با دشواری‌هایی مواجه شود اما بسیاری از کارشناسان بر این عقیده هستند که با اختصاص وقت و منابع کافی مسأله انتساب موثق حملات سایبری قابل حل است حداقل هنگامی که حملات با مقیاس بالا علیه زیرساخت‌های حیاتی صورت گیرد (فرشاسعید و همکاران، ۱۴۰۰: ۲۱). بنابراین در تطبیق با موضوع مقاله می‌توان گفت که کشور آلبانی مطابق توافق ۲۰۱۴ به مجاهدین خلق با دلایل به ظاهر بشردوستانه پناهندگی اعطا کرده است در واقع سرزمین خود را در اختیار تروریسم گذاشته، و نه فقط حمایت کرده بلکه حداقل تا همین اواخر به آن‌ها سهل گرفته است. به عبارتی پناهندگی ابزاری برای مجاهدین خلق تبدیل شده است، چرا که از وضعیت پناهندگی سوء استفاده کرده و به اقدامات تروریستی از کشور میزبان دست زده اند. در مواردی که اعطای پناهندگی به مرتکبین اعمال تروریستی توسط یک دولت و همچنین از پوشش پناهندگی برای اقدام تروریستی در دولت متبوع یا سایر دولت‌ها استفاده شود، چنانچه دولت اعطا کننده، از این فعالیت ها مطلع باشد، یا حمایت و هدایت کننده این گونه اعمال باشد، و یا دستور آن ها را داده باشد، مسؤلیت بین المللی دولت اعطا کننده قابل تصور است. چنانچه شورای امنیت سازمان ملل از همه دولت‌ها درخواست کرد که حلقه امنیت را برای کسانی که در برنامه ریزی، سرمایه گذاری، حمایت و ارتکاب اعمال تروریستی دست دارند، تنگ کنند (آذری آغاجری، ۱۳۸۸: ۱۱۸۷). از جمله این که در قطعنامه ۱۳۷۳ مقرر کرده است که دولت‌ها باید از پناه دادن به کسانی که اعمال تروریست‌ها را پشتیبانی مالی و غیرمالی می‌کنند خودداری ورزند و نیز مانع استفاده از قلمرو خود بر ضد شهروندان خود یا سایر کشورها توسط کسانی شوند که اقدامات تروریستی را حمایت مالی و پشتیبانی می‌کنند (S/RES/1373, 2001). با توجه به استدلالات گفته شده، آلبانی مسؤل حملات سایبری مجاهدین خلق تلقی می‌شود زیرا، علی رغم تعهدات بین‌المللی و نیز قطعنامه های مکرر شورای امنیت مبنی بر عدم حمایت از تروریسم، به گروه تروریستی پناه داده است. هنگامی که مسؤلیت بین‌المللی محرز گردید، کشور مسؤل، مکلف به جبران و ترمیم خسارات وارده است.

بنابراین، نتیجه اساسی مسؤلیت، تعهد به جبران خسارت کامل است. ماده ۳۱ (بند ۱) طرح مواد راجع به مسؤلیت مبین اصل مذکور است. دیوان دائمی دادگستری بین‌المللی نیز در قضیه کارخانه کورزف در رأی خود، الزام به جبران خسارات را برای طرف مسؤل در قبال نقض هر تعهد بین‌المللی شناخته است. طبق ماده ۳۷ طرح مواد راجع به مسؤلیت: ۱) کشوری که مسؤل عمل متخلفانه بین‌المللی شناخته شده، موظف است به منظور جبران خسارت ناشی از این عمل خلاف، رضایت کشور زیان دیده را جلب نماید. جبران خسارت به این روش می‌تواند به شکل تأیید زیر پا گذاشتن پایبندی، ابراز تأسف، معذرت خواهی رسمی یا دیگر اشکال مناسب صورت پذیرد (بیاتی و ایمانی، ۱۴۰۱: ۱۲۳). پر واضح است مطابق قواعد حقوق بین‌الملل آلبانی باید از جمهوری اسلامی ایران جبران خسارت نموده و با انجام اقداماتی رضایت خاطرش را جلب نماید. بالاخره رسانه های آلبانی اخیراً اعلام کردند که پلیس این کشور به مقر سازمان مجاهدین خلق در این کشور حمله کرده است؛ حمله به مقر این گروه پس از آن روی داد که احتمال حضور تعدادی از مظنونین به حملات سایبری در مقر آن‌ها گزارش شد. به دنبال این موضوع نخست وزیر آلبانی، از گروه مزبور خواست تا اگر به دنبال جنگ با ایران هستند، خاک این کشور را ترک کنند. با این جمله تأکید کردند که آلبانی هیچ قصدی برای جنگ با ایران ندارد و پذیرای سوءاستفاده کنندگان از این میهمان نوازی نیست. بدین ترتیب به نظر می‌رسد در عمل اقدام آلبانی را می توان نوعی جبران خسارت (جلب رضایت ایران) تلقی کرد. کلام آخر این که اگر قرار است در آینده دارای جهانی با ثبات امنیتی بالا در حوزه سایبری

باشیم، برای فرار از مسؤلیت دولت‌ها باید جلوی چنین بهانه‌هایی گرفته شود و تأکید بر مسؤلیت دولت‌هایی شود که حملات سایبری از داخل قلمرو آن‌ها هدایت می‌گردد.

نتیجه‌گیری

اینترنت هم‌زمان با ایجاد میلیون‌ها شغل جدید تهدیدات جدی را نیز با خود به همراه آورده است. بازخورد این تهدیدها در قالب و عناوین متعددی ظهور یافته که حمله سایبری سازمان مجاهدین خلق علیه سازمان های دولتی و غیردولتی ایران جزء چالش برانگیزترین این نوع تهدیدها بوده است. بدون تردید وقوع چنین حملاتی تبعات خاص خود را به همراه داشته که بررسی ابعاد حقوقی آن از منظر حقوق بین‌الملل برای کشورها ضروری می‌نماید. ایران به دلیل این که هدف چنین حمله‌ای قرار گرفته مستثنی از این قاعده نیست و باید به بررسی ابعاد حقوقی این پدیده پرداخت تا بتواند تدابیر مناسبی در قبال چالش فرارو اتخاذ کرده و در برابر وقوع چنین حملاتی در آینده پیشگیری و از خود دفاع نماید. صرف نظر از آرمانگرایی های متخصصین حقوق بین الملل در حال حاضر رویه بین‌المللی حکایت از مشروعیت توسل به دفاع مشروع در برابر حملات تروریستی گروه‌های غیردولتی از سرزمین یک کشور ناتوان یا کشوری که حکومت آن در برابر اعمال گروه‌های غیردولتی حالت انفعالی داشته است، دارد. اگرچه در نبود نظام حقوقی کارآمد در خصوص فضای سایبری تردیدی نیست، لیکن آنچه مهم جلوه می کند، تلاش برای وام گرفتن اصول و قواعدی حقوقی از دیگر نظام‌های موجود حقوق بین‌الملل و سنجش میزان مشابهت آن‌ها با فضای سایبری است. و بیان کردیم یک حمله سایبری با توجه به نتایج و آثار آن یعنی شدت آسیب و تخریب ایجاد شده و البته وجود رابطه علت و معلولی بین حمله سایبری و خسارات به وجود آمده ارزیابی می‌گردد و در این چارچوب می‌تواند حمله مسلحانه تلقی شده و حق دفاع مشروع را در پی داشته باشد. این که حملات سایبری مجاهدین خلق با توجه به نوع تأثیری که گذاشته نقض اصل ممنوعیت توسل به زور تلقی می‌شود، ظاهراً متقن نبوده چرا که حملات سایبری این گروه در حد حملات پراکنده به وبگاه‌های اینترنتی چند سازمان دولتی یا غیردولتی است. بنابراین حملات سایبری این گروه فعلاً در حدی نیست که در چارچوب مفهوم حمله مسلحانه بگنجد از طرف دیگر بنا به اظهارات مقامات رسمی ایران حمله مزبور هیچ گونه خسارات فیزیکی به همراه نداشته و از این رو نقض ممنوعیت توسل به زور در حقوق بین‌الملل تلقی نمی‌شود. البته سکوت رسمی، عدم پیگیری مسأله فوق در مجامع بین المللی و واکنش انفعالی جمهوری اسلامی ایران در قبال این حمله بررسی گزینه های موجود را عملاً عقیم می‌کند. به هر حال حملات سایبری معضلی جهانی است بنابراین راهبردی که دولت‌ها می‌توانند برای معضل حملات سایبری داشته باشند این است که در سطح بین المللی همکاری های خودشان را در این حوزه افزایش دهند و با تدوین یک معاهده جامع بین‌المللی درباره حملات سایبری کنترل این حوزه خطرناک را بدست بگیرند. به نظر می رسد اکثر حقوقدانانی که در حوزه سایبری می‌نگارند، دست کم از کنار آن به سادگی گذشته اند که جنس حملات سایبری، امکان وقوع آن از سوی بازیگران غیردولتی و نحوه عملکرد آن کاملاً از حملات کلاسیک متفاوت بوده که بررسی دقیق این مسائل می‌تواند دال بر نیاز به تدوین قواعد و نظامات جدیدی برای مدیریت این حملات در جامعه بین‌المللی باشد.

منابع

۱. ابراهیم‌گل، علیرضا. (۱۳۹۶). مسؤلیت بین‌المللی دولت: متن و شرح مواد کمیسیون حقوق بین‌الملل، چاپ نهم، تهران، انتشارات شهردانش.

۲. آذری آغاجری، بهزاد. (۱۳۸۸). «مسؤلیت بین‌المللی دولت‌ها در قبال اعمال خشونت‌آمیز اشخاص حقیقی در چارچوب تروریسم»، فصلنامه سیاست خارجی، دوره ۲۳، شماره ۴، ۱۱۹۸-۱۱۶۵.

۳. اسمعیل‌زاده ملاباشی، پرستو، عبداللهی، محسن، زمانی، سیدقاسم. (۱۳۹۶). «حملات سایبری و اصول حقوق بین الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)»، فصلنامه مطالعات حقوق عمومی، دوره ۴۷، شماره ۲، ۵۵۹-۵۳۷.

۴. اقتصاد نیوز. (۱۴۰۰). اتفاق بی‌سابقه؛ حمله هکری منافقین به صدا و سیما، پایگاه خبری اقتصاد نیوز، در: https://www.eghtesadnews.com/%D8%A8%D8%AE%D8%B4%D8%A7%D8%A%D8%A8%D8%A7%D8%B1-%D8%B3%DB%8C%D8%A7%D8%B3%DB%8C-57/472081-%D8%A7%D8%AA%D9%81%D8%A7%D9%82-

۵. امیرلی، حسین، ثقفی، کامیار. (۱۳۹۸). «ارائه مدل مفهومی ارزیابی تهدیدات تروریسم سایبری»، فصلنامه امنیت ملی، دوره۹، شماره ۳۳، ۴۲۴-۳۸۹.

۶. انصاف. (۱۴۰۱). سایت و شبکه دوربین شهرداری تهران هک شد، پایگاه خبری و تحلیلی انصاف نیوز، در: http://www.ensafnews.com/349452/%D8%B3%D8%A7%DB%8C%D8%AA-%D9%88-

۷. بیاتی، محمدحسن، ایمانی، اصغر. (۱۴۰۱). «مسؤلیت بین‌المللی دولت‌ها در قبال حمایت از تروریسم»، فصلنامه راهبرد سیاسی، دوره ۶، شماره ۴، ۱۳۰-۱۱۱.

۸. جامعه ۲۴. (۱۴۰۱). سایت‌های وزارت کشاورزی هک شد، پایگاه خبری جامعه ۲۴، در: https://jameh24.com/fa/news/37176/%D8%B3%D8%A7%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8

۹. رزمخواه، نجمه. (۱۴۰۲). «نقدی بر پیش‌نویس قانون اتحادیه اروپا در همسان‌سازی قوانین حاکم بر هوش مصنوعی، از منظر مقابله با تروریسم سایبری»، فصلنامه مطالعات حقوق عمومی، ۲۷-۱.

۱۰. شایگان، فریده، صفوی کوهساره، سیدحامد. (۱۳۹۷). «عملیات سایبری به مثابه توسل به زور»، فصلنامه مطالعات حقوق عمومی، دوره ۴۸، شماره ۲، ۴۴۱-۴۱۹.

۱۱. صدای ایران. (۱۴۰۰). ماجرای هک شدن صدا و سیما چیست؟، پایگاه خبری صدای ایران، در : https://sedayiran.com/fa/news/271584/%D9%85%D8%A7%D8%AC%D8%B1%D8%A7%

۱۲. فارس. (۱۴۰۲). دستیابی به اسناد و بانک‌های اطلاعاتی و هک سرورهای وزارت خارجه تکذیب شد، خبرگزاری فارس، در: https://farsnews.ir/news/14020217000971/%D8%AF%D8%B3%D8%AA%DB%8C%D8%A7%D8%A8%DB%8C-%D8%A8%D9%87-%D8%A7%D8%B3%D9%86%D8%A7%D8%AF

۱۳. فرشاسعید، پرویز، جلالی، محمود، گودرزی، مهناز. (۱۴۰۰). «ضرورت تدوین کنوانسیون بین‌المللی حملات سایبری»، فصلنامه مطالعات حقوقی، دوره ۱۳، شماره ۱، ۲۳۰-۲۰۵.

۱۴. فرشاسعید، پرویز، جلالی، محمود، گودرزی، مهناز. (۱۴۰۱). «ضرورت همکاری دولت‌ها در تقویت امنیت سایبری»، فصلنامه مطالعات بین‌المللی، دوره ۱۹، شماره۲، ۱۷۸-۱۶۳.

۱۵. فضائلی، مصطفی (۱۴۰۲). «رابطه میان تروریسم و مخاصمات مسلحانه؛ با نگاهی به وضعیت افغانستان»، فصلنامه تحقیقات حقوقی، دوره ۲۶، شماره ۱۰۲، ۱۱۳-۱۴۰.

۱۶. فلک، دیتر، باث، میشل، فیشر، هورست، پیترگاسر، هانس، گرین وود، کریستوفر، هینشل فان هینگ، ولف، ایپن، نات، اوتر، استفان، ژوزف پارش، کارل، رابوس، والتر، ولفروم، رودیگر. (۱۳۸۷). حقوق بشردوستانه در مخاصمات مسلحانه، ترجمه سید قاسم زمانی، نادر ساعد، حسین شریفی طرازکوهی، هاجر سیاه رستمی، فاطمه کیهانلو، میرشهبیز شافع، محمد جعفر ساعد، کتایون حسین نژاد، چاپ اول، تهران، موسسه مطالعات و پژوهش های حقوقی شهردانش.

۱۷. قاسمی، غلامعلی، نامدار، سعید. (۱۳۹۷). «بررسی مفهوم دفاع مشروع در پرتو حملات سایبری با تأکید بر حمله استاکس نت به تأسیسات هسته ای ایران»، مجله مطالعات حقوقی، دوره ۱۰، شماره ۱، ۲۳۵-۱۹۹.

۱۸. میرعباسی، سیدباقر، کورکی‌نژاد قرایی، مجید. (۱۳۹۷). «قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در ماده ۵۱ منشور سازمان ملل متحد»، فصلنامه مطالعات حقوق عمومی، دوره ۴۸، شماره ۲، ۲۸۰-۲۶۱.

۱۹. نعمت پور، اردشیر، تقی زاده انصاری، مصطفی، ببری گنبدی، سکینه. (۱۴۰۰). «مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین‌الملل»، فصلنامه مطالعات بین‌المللی، دوره ۱۸، شماره ۳، ۱۶۵-۱۸۵.

۲۰. نواندیش. (۱۴۰۰). حمله سایبری به سایت وزارت ارشاد و نمایش تصاویر گروهک منافقین، پایگاه خبری- تحلیلی نواندیش، در: https://noandish.com/fa/news/138788/%D8%AD%D9%85%D9%84%D9%8

21. Collin, Barry. (1997). the future of Cyberterrorism: Where the Physical and Virtual Worlds Converge, 11th Annual International Symposium on Criminal Justice Issues.

22. Cornish, Paul, Livingstone, David, Clemente, Dave, Yorke, Claire. (2010). On Cyber Warfare, A Chatham House Report. 1-49.

23. Garner, B. (2009). black\s law dictionary, USA: Thomson West, 9th Ed.

24. Hansen, James v, Lowry, Paul Benjamin, Rayman D, Meservy, McDonald, Daniel M. (2007). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection, Decision Support System. Vol.43 (4).

25. ICJ Reports. (1986). Military and Paramilitary Activities in and Against Nicaragua (Nicaragua V United states). At: https://www.icj-cij.org/node/100900.

26. ICJ Reports. (1996). on the Legality of the Threat or use of Nuclear weapons. At: Reportshttps://www.refworld.org/cases,ICJ,4b2913d62.html.

27. Li, Yuchong, Liu, Qinghui. (2021). a comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments, Energy Reports. 7, 8176-8186.

28. Martínez Esponda, Pedro. (2023). Norm-instability as a Strategy in International Lawmaking: The Case of Self-defence against Non-state Actors, The Many Paths of Change in International Law. 69-88.

29. Melzer, Nils. (2011). Cyberwarfare and international Law, UNIDIR. 1-38.

30. Segura-serrano, Antonio. (2006). internet regulation and the role of international law, max Planck yearbook of United Nations law. Vol. 10, pp.191-272.

31. S/RES/1373. (2001). at: http://www.un.org/en/ga/searvh/view_doc.asp?symbol= S/RES/1373&282001%29.