Volume 14, Issue 53, Autumn 2021
Received: 2021/08/05
Date of acceptance: 2022/03/03
Pages: 243-263

فصلنامه علمی تحقیقات حقوقی بین‌المللی
International Legal Research Scientific Quarterly

دوره چهاردهم/ شماره ۵۳/ پاییز ۱۴۰۰
تاریخ دریافت: ۱۴۰۰/۰۵/۱۴
تاریخ پذیرش: ۱۴۰۰/۱۲/۱۲
صفحه: ۲۴۳ الی ۲۶۳

سامانه: alr.iauctb.ac.ir doi 10.30495/ALR.2022.1937260.2133

Article Type: Research

نوع مقاله: پژوهشی

نقش اتحادیه بین‌المللی مخابرات در برقراری امنیت سایبری

الناز کتانچی[۱]، بابک پورقهرمانی[۲]

چکیده

زمینه و هدف: اتحادیه بین‌المللیِ مخابرات از طریق اعتمادسازی و امنیت در استفاده از فناوری اطلاعات و ارتباطات، توسعه و پیاده‌سازی استانداردها در امنیت سایبری در سطح بین‌المللی و با کمک به کشورهای عضو برای تقویت ظرفیت امنیت سایبری برای به اشتراک‌گذاری مؤثر اطلاعات، یافتن راه‌حل‌ها، پاسخ به تهدیدهای سایبری، توسعه و اجرای استراتژی‌ها و قابلیت‌های ملی و همکاری‌های منطقه‌ای و بین‌المللی از طریق کنفرانس و قطعنامه اقدام نموده است.

روش: پژوهش حاضر به روش توصیفی- تحلیلی می‌باشد.

یافته‌ها و نتایج: یافته‌ها نشان می‌دهد؛ اتحادیه بین‌المللی مخابرات، به ویژه در اجلاس جهانی جامعه اطلاعاتی آن در خصوص ایجاد امنیت سایبری تصمیمات ارزشمندی از جمله ایجاد برنامه راهبردی پنج‌گانه توسعه مدل‌های قانون‌گذاری گرفته است که تا به امروز به عنوان برنامهٔ کاری با ویژگی‌های منحصربه‌فرد، بالأخص ارائه‌دهنده ابزار توسعه مبارزه با جرایم سایبری شمرده می‌شود و قطعنامه‌های صادره به ویژه قطعنامه حفاظت از کودکان آنلاین و تأکید بر ایجاد فضای امن آنلاین نیز بر اهمیت نقش سازمان مذکور در این حوزه افزوده است. نتیجهٔ حاصل از پژوهش نشان می‌دهد که اتحادیه بین‌المللی مخابرات برای ایجاد امنیت سایبری بایستی با تغییر رویکرد حقوقی خود از طریق تدوین یک کنوانسیون مستقل در ایجاد امنیت سایبری که از قدرت الزام‌آوری کافی نیز برخوردار باشد، به کشورها این امکان را بدهد تا با یاری جستن از ظرفیت‌های کنوانسیون، قوانین خود را یکسان نموده و آسیب‌پذیری زیرساخت‌های اطلاعاتی خود را کاهش دهند؛ بنابراین این پژوهش با هدف تبیین تصمیمات و اقدامات اتحادیه بین‌المللی مخابرات به عنوان سازمان بین‌المللی فعال در زمینه ایجاد امنیت سایبری، نگاشته شده است.

کلیدواژه‌ها: اتحادیه بین‌المللی مخابرات، فضای سایبری، امنیت سایبری، اجلاس جهانی جامعه اطلاعاتی، اقدامات.

* استناددهی (APA): کتانچی، الناز؛ پورقهرمانی، بابک. (۱۴۰۰). نقش اتحادیه بین‌المللی مخابرات در برقراری امنیت سایبری. *تحقیقات حقوقی بین‌المللی*، ۱۴(۵۳)، ۲۶۳-۲۴۳.
http://alr.iauctb.ac.ir/article_687637.html

۱. دانشجوی دکتری تخصصی حقوق بین‌الملل عمومی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.
رایانامه: e.katanchi20@gmail.com
۲. دانشیار گروه حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران (نویسنده مسئول).
رایانامه: b.pourghahramani@yahoo.com

CC BY-NC-SA

مقدمه

فضای سایبر[1] محیطی هست که به‌سرعت در حال رشد است و باید آن را جزء لاینفک زیستِ فردی و جمعی انسان‌ها دانست. این فضا در عین کاربردی و مثبت بودن، چالش‌ها و تهدیداتی را می‌تواند ایجاد نماید که نباید آنها را نادیده گرفت. دنیا باید به‌طور جمعی و خصوصاً از طریق سازمان‌های بین‌المللی، ضمن شناسایی این چالش‌ها، ابتکارات لازم را برای مقابله با آنها تنظیم و عملی نماید؛بنابراین می‌توان گفت که نظام کنونی حاکم بر جرایم سایبری تا حدود زیادی متکی بر همکاری بین‌المللی است. لذا با برجسته‌تر شدن نقش سازمان‌های بین‌المللی در عرصه جهانی، آنها نیز همچون کشورها از این فضا بهره می‌برند و البته موازی با آن به فعالیت در این حوزه می‌پردازند. همچنان که نهادهای بین‌المللی و منطقه‌ای نیز همچون حقوق داخلی به تنظیم قوانین و مقررات و تعریف چهارچوب‌های قانونی و حقوقی در قالب تدابیر حقوقی به عنوان یکی از طرق ایجاد امنیت در فضای سایبری می‌پردازند. برجسته‌ترین نهاد بین‌المللی که در این راستا فعالیت‌های مؤثری را داشته است؛ سازمان ملل متحد می‌باشد که با ایجاد نهادهای فرعی و تخصصی گام مهمی را در ایجاد امنیت در فضای سایبری برداشته است یا شورای اروپا با تصویب کنوانسیون ۲۰۰۱ بوداپست[2] با موضوع جرایم رایانه‌ای بر مهم بودن امنیت در فضای سایبری تأکید داشته است (تقی‌زاد، ۱۳۹۶: ۱۰۵).

در این میان یکی از سازمان‌های بین‌المللی که وابسته به سازمان ملل متحد است و در دو دهه اخیر نقش پررنگی را در خصوص ایجاد رویدادهای امنیتی در فضای سایبری داشته است؛ اتحادیه بین‌المللی مخابرات[3] می‌باشد. این اتحادیه که وظیفه قانون‌گذاری و نیز مدیریت فضای فرکانسی، تدوین استانداردهای تبادل داده و اطلاعات و همچنین کمک به رشد و توسعه ارتباطات در سراسر جهان را بر عهده دارد. با برگزاری «اجلاس جهانی جامعه اطلاعاتی»[4] در سال‌های ۲۰۰۳ و ۲۰۰۵ برای اولین بار توجه جدی بر فضای سایبری و موضوعات مطرح در آن از سوی این سازمان بین‌المللی، اجلاس جهانی جامعه اطلاعاتی و دولت‌های عضو مطرح شده است و در سال ۲۰۰۷ برنامه کاری امنیت جهانی سایبری از سوی اجلاس جامعه جهانی اطلاعات تعریف شد که تا به امروز نیز به عنوان برنامه کاری با ویژگی‌های منحصربه‌فرد و مؤثر در این زمینه شناخته شده است. همچنین قطعنامه‌هایی نیز در خصوص مبارزه با جرایم سایبری از سوی اتحادیه بین‌المللی مخابرات در سال‌های اخیر به تصویب رسیده است که نشانگر همکاری و معاضدت سازمان بین‌المللی مخابرات و دولت‌های عضو در راستای کاهش جرایم سایبری و قاعده‌مند کردن قوانین و مقررات در بهره‌مندی از فضای سایبری با ضریب امنیتی (Gabrial, 2019: 1-4) بالا می‌باشد.

---

1. Cyberspace
2. Council of Europe Cybercrime Convention, 2001
3. International Telecommunication Union
4. World Summit on the Information Society

بنابراین تبیین مطالب بالا نگارنده را بر آن داشته است تا با نگاهی بر اقدامات اتحادیه بین‌المللی مخابرات نقش آن را در ایجاد امنیت سایبری و خلأهای حقوقی موجود را در این زمینه مورد مطالعه قرار دهد و برای ارائه راهکار به این سؤال پاسخ دهد که آیا اتحادیه به تشکیل کارگروه‌های تخصصی (فنی- حقوقی) در زمینه ایجاد امنیت سایبری تا به اکنون اقدام نموده است؟

اما در وهله نخست نگاهی اجمالی بر مفهوم امنیت سایبری و شقوق آن و شرح مختصری از تاریخچه تشکیل اتحادیه بین‌المللی مخابرات و ارکان آن لازم می‌نماید؛ چراکه برای شرح هر موضوعی ضرورت بیان مفاهیم اصلی و اولیه در آن حوزه امری بدیهی به شمار می‌آید.

۱. مفهوم امنیت سایبری

امنیت به حداقل رساندن خطر یا تهدید است که این خطرها نه‌فقط از نوع سنتی و نظامی هستند بلکه تهدیدات جدید غیرنظامی را نیز در برمی‌گیرند. تهدیدات جدید غیرنظامی امروزه علاوه بر صحنه واقعی به عرصه مجازی هم سوق یافته است و گستردگی بی‌اندازه آن موجب توجه جدی به حوزه امنیت در فضای سایبری گردیده است. از این‌رو تعریفی که از امنیت در فضای سایبری یا امنیت سایبری می‌گردد، می‌تواند مجموعه ابزارها، سیاست‌ها، مفاهیم امنیتی، دستورالعمل‌ها، رویکردهای مدیریت، آموزش بهترین شیوه‌ها، اطمینان و فناوری‌هایی که می‌تواند برای محافظت از محیط‌زیست سایبری و سازمان‌ها و دارایی‌های کاربر لازم است را، در بربگیرد.

در تعریفی عام گفته شده است که: امنیت عبارت است از مکانیزم‌های پیشگیری یا کاهش احتمال وقوع رخدادهای خطرناک و جلوگیری از تمرکز قدرت در هر نقطه از شبکه و احیای شبکه در حین وقوع رخدادهای ناخوشایند (وقتی‌که رخدادهای خطرناک حادث می‌شوند) هر عاملی که به‌طور بالقوه بتواند منجر به وقوع رخدادی خطرناک شود یک تهدید امنیتی به شمار می‌آید (نامخواه، ۱۳۹۰: ۳۴).

بنابراین حفاظت از سیستم‌های اطلاعات از سرقت یا صدمه به سخت‌افزار، نرم‌افزار و اطلاعات نرم‌افزاری و محافظت در برابر حمله محروم‌سازی از سرویس[1] (اختلال) و بات نت‌ها[2] (گمراهی) به عنوان پارامترهایی است که امنیت سایبری را تأمین می‌نماید.

از این‌رو، امنیت سایبری را می‌توان به عنوان راه حل‌های پیشنهادی (شامل قوانین، دستورالعمل‌ها، حراست‌های فناوری و غیره) برای تهدیدات ناشی از هک و به خطر انداختن سیستم‌های رایانه‌ای تعریف کرد (Brunot, 2018: 3).

1. Denial of Service (DoS)
2. Botnet

۲. شقوق امنیت سایبری

شقوق امنیت سایبری را می‌توان هم از منظر حقوق و هم در پارادایم فضای سایبری بررسی کرد:

۲-۱. امنیت سایبری در حقوق

امنیت سایبری در حقوق دارای دو مفهوم مضیق و موسع است. در مفهوم مضیق، منظور اتخاذ تدابیر فنی و پیشگیرانه برای تأمین امنیت شبکه‌ها و اطلاعات است. در این مفهوم، اقدامات غیرفنی، جایگاهی نداشته و اشخاص، موضوع مستقیم تدابیر امنیتی نیست، همچنان که تأمین امنیت فراتر از محیط سایبری را در برنمی‌گیرد. این مفهوم منطبق بر امنیتی است که اهل فن در علوم رایانه و اینترنت آن را طراحی و تبیین می‌کنند؛ اما در مفهوم موسع، دو قسم از تدابیر برای تأمین امنیت در فضای سایبری را می‌توان سراغ گرفت: تدابیر مستقیم یا اصلی که درواقع تدابیری هستند که به شکل قانونی و فنی برای تأمین امنیت داده‌ها، اطلاعات و سیستم‌ها و شبکه‌های رایانه به‌کار می‌رود و تدابیر واسطه‌ای که این تدابیر در پی تنظیم مقررات مناسب برای فضای سایبری است تا به واسطه‌ی آن هدف اصلی یعنی امنیت فضای واقعی تأمین شود (Gasser, 1988).

۲-۲. امنیت سایبری در پارادایم فضای سایبری

امنیت در پارادایم فضای سایبری تابع دو عنصر کلیدی انسان و فضای سایبری است. انسان و جامعه در مقابل فضای سایبری جهانی با ویژگی‌های خود فضای تهدیدزایی را شکل داده است. تهدیدات فضای سایبری، ضرورت حفاظت از انسان، جامعه و حاکمیت را در برمی‌گیرد. درواقع این تهدیدات نیازمند سه سطح امنیت است.

۲-۲-۱. امنیت در حوزه زیرساخت و شریان‌های اطلاعاتی

فرصت جدید ایجادشده برای حرفه‌ها و کشورها در فضای اتوماسیون تبادل همکاری، تجارت الکترونیکی، تولید هدفمند منجر به تولید، ذخیره‌سازی و بهره‌مندی از اطلاعات حساس و حیاتی شده است و وابستگی به شبکه‌های پرسرعت و پردازشگرهای قدرتمند روزبه‌روز افزایش می‌یابد که سیستم‌ها را در معرض مخاطراتی از آتش و طوفان تا بزهکاری و تروریسم سایبری قرار داده که نیاز به مدیریت و نظارت دارد (محسنی و صوفی زمرد، ۱۳۹۶: ۱۶۴).

۲-۲-۲. امنیت در حوزه فرد و اجتماع

در این حوزه با توجه به تفاوت در کارکرد انسان و حقوق او در ایدئولوژی اسلامی با ایدئولوژی غرب چالش‌هایی را ایجاد می‌نماید. ابعاد این چالش در بعد فردی و اجتماعی ضرورت طرح‌ریزی برای امنیت فرهنگی و امنیت اخلاقی و دینی را ایجاب می‌کند.

۲-۲-۳. امنیت در حوزه ملی و حاکمیتی

تهدیدات در حوزه ملی و حاکمیتی، مجموعه تهدیداتی است که حیاتی‌ترین منافع و حاکمیتی یک نظام را به چالش می‌کشاند. این حوزه از تهدیدات بخش در حوزه زیرساخت و شریان‌های اطلاعاتی قرار داشته بخشی در حوزه امنیت سیاسی و اقتصادی است (محسنی و صوفی‌زمرد، ۱۳۹۶: ۱۶۵).

اکنون با توجه به اینکه یک تعریف اجمالی از مفهوم امنیت سایبری و شقوق امنیت سایبری ارائه گردید؛ به بیان تاریخچه تشکیل و فعالیت، اقدامات و تصمیمات بین‌المللی از سوی اتحادیه بین‌المللی ارتباطات که در راستای ایجاد امنیت در فضای سایبری صورت گرفته است، می‌پردازیم.

۳. تاریخچه تشکیل و فعالیت اتحادیه بین‌المللی مخابرات

اتحادیه بین‌المللی مخابرات یک سازمان وابسته به سازمان ملل متحد در ابتدا با عنوان اتحادیه تلگراف بین‌المللی در سال ۱۸۶۵ در پاریس تأسیس شد. سپس نام آن در سال ۱۹۳۲ در کنفرانس مادرید به اتحادیه بین‌المللی مخابرات تغییر یافت. این نام از اول ژانویه ۱۹۳۴ به‌کار برده شد تا منعکس‌کننده دامنه مسئولیت‌های اتحادیه باشد[۱] و اتحادیه از سال ۱۹۴۷، کنفرانس‌های سالیانه و مستقل خود را برگزار می‌کند. در ۱۵ نوامبر ۱۹۴۷، با تصویب موافقت‌نامه فی‌مابین اتحادیه و سازمان ملل متحد توسط مجمع عمومی ملل متحد، اتحادیه بین‌المللی مخابرات، به عنوان آژانس تخصصی ملل متحد به رسمیت شناخته شد[۲]. اتحادیه بین‌المللی ارتباطات، مسئول تنظیم مقررات بین‌المللی و مدیریت طیف فرکانس رادیویی و منابع مداری می‌باشد. اتحادیه بیش از ۴۰ سال است که به وسیله کنفرانس‌های ارتباطات رادیویی جهانی به تنظیم مقررات طیف و استفاده مدارها به وسیله ایستگاه‌های خدمات ارتباطات رادیویی فضایی می‌پردازد. دولت‌های عضو اتحادیه، رژیم حقوقی را ایجاد کردند که به قالب اساسنامه، کنوانسیون و مقررات رادیویی اتحادیه مدون شده است. این اسناد بر مبنای اصول استفاده مؤثر و کارآمد از منابع طیفی و مداری و دسترسی عادلانه به آن منابع[۳] استوار شده و دربرگیرنده اصول مهم و مقررات تفضیلی خاصی است که عبارت است از:

- تخصیص طیف فرکانس‌ها جهت سرویس‌های مختلف ارتباطات رادیویی؛

---

۱. در این زمان، مسئولیت‌های اتحادیه بین‌المللی مخابرات، شامل تمامی اشکال ارتباطات با سیم و بی‌سیم شد.

2. http://www.itu.net/en/history/pages/ITUsHistory.aspx.Last Visited at: 11 Dec 2019.

۳. این اصول که در شماره ۱۹۶ اساسنامه اتحادیه (ماده ۴۴) مندرج است، مقرر می‌دارد که: «در استفاده از باندهای فرکانس برای خدمات رادیویی، دولت‌های عضو باید توجه داشته باشند که فرکانس‌های رادیویی و هر مدار مرتبط، از جمله مدار ثابت ماهواره‌ای از منابع طبیعی محدود هستند و اینکه آنها باید به صورت عقلانی، مؤثر و اقتصادی و مطابق با مفاد مقررات رادیویی به‌طوری‌که کشورها یا گروه کشورها بتوانند دسترسی عادلانه‌ای به آن مدارها و فرکانس‌ها داشته باشند و با در نظر گرفتن نیازهای خاص کشورهای در حال توسعه و موقعیت جغرافیایی کشورهای خاص مورد استفاده قرار گیرند».

http://www.itu.int/inunews/manager/display.asp?lang=en&year=2009&issue=02&ipage

– رعایت حقوق و تعهدات دولت‌های عضو در حصول دسترسی به منابع طیفی یا مداری.

به رسمیت شناخته شدن این حقوق، به وسیله ثبت علائم فرکانسی و موقعیت‌های مداری (اعم از مواردی که مورد استفاده قرار گرفته یا جهت استفاده در نظر گرفته شده است) در دفتر ثبت بین‌المللی فرکانس اتحادیه (جباری و حاتمی، ۱۳۹۳: ۱۵۰ – ۱۴۹).

با پرتاب اولین قمر مصنوعی با نام «اسپوتنیک۱[۱]» به فضا در چهارم اکتبر ۱۹۵۷، عصر فضا و ارتباطات رادیویی فضایی[۲] آغاز شد. در سال ۱۹۵۹، کمیته مشورتی بین‌المللی رادیویی، گروه مطالعاتی را برای بررسی و جمع‌آوری داده‌ها و اطلاعات درباره ارتباطات رادیویی فضایی تشکیل داد[۳]. علاوه بر این، کنفرانس اداری رادیویی اتحادیه (کنفرانس رادیویی)[۴]، بازنگری در جداول تخصیص فرکانس و اختصاص فرکانس‌های خاصی را به ارتباطات رادیویی فضایی در دستور کار خود قرار داد.

کنفرانس فوق‌العاده رادیویی در سال ۱۹۶۳ در ژنو برای تخصیص فرکانس‌ها به سرویس‌های فضایی گوناگون[۵] برگزار شد. این کنفرانس، اولین گردهمایی بین‌المللی بود که با رویکرد و دستور جلسه‌ای کاملا فضایی تشکیل می‌شد. در این کنفرانس، علاوه بر تغییر اساسی کلیه قوانین و مقررات رادیویی، باندهای فرکانسی خاصی برای سرویس فضایی گوناگون از جمله هواشناسی، مخابراتی، دورسنجی و ...، تعیین و اولین قوانین برای استفاده از مدار ثابت زمین تصویب شد. همچنین در این کنفرانس، حق مساوی همه ملت‌ها در استفاده از باندهای فرکانسی تخصیص یافته مورد شناسایی و تائید قرار گرفت (رضی‌پور و گلرو، ۱۳۸۸: ۱۳).

اتحادیه در سال ۱۹۷۱ کنفرانس جهانی اداری رادیویی را برگزار کرد و قوانین تخصیص فرکانس‌ها را مورد بازبینی قرار داد. کنوانسیون بین‌المللی مخابرات راه دور در سال ۱۹۸۲ در نایروبی[۶] منعقد شد. درواقع این کنوانسیون، جانشین کنوانسیون بین‌المللی مخابرات راه دور[۷] شد که در تاریخ ۲۵ اکتبر ۱۹۷۳ در ملاکاتور مولینوس (اسپانیا) منعقد شده بود[۱].

1.Sputnik-1

2.http://www.itu.int/en/history/pages/ITUsHistory.asp.Last Visited at: 24 Dec 2019.

3.CCIR – Ixth Plenary Assembly (Los Angeles, 1959). Available at: http:// www.itu.int/en /history/ Pages/ Listof ITUConferencesAssembliesAndEvents.aspx. Last Visited at: 11 Dec 2019.

4.The Administratve Radio Conference (Radio Conference), (Geneva, 1959). Available at: http://www.itu.int/ en/history/Pages/ListOFITUConferences Assemblies AndEvents.aspx:1.ast Visited at: 07 Dec 2019.

5.(FARC-63) Extraordinary Administrative Radio Conference to Allocate Frequency Bnds for Space Radiocommunication Purposes –Space Radiocommunication Conference (Geneva, 1963). Available at: http://www.itu.int/en/history/Pages/ListOFITUConferencesAssembliesAndEvents.aspx.Last Visited at: 06 Feb 2016.

6. The Plenipotentiary Conference, (Nairobi, 1982). Available at: http://www.itu.int/en/history/Pagest/ListOFITU ConferencesAssembliesAndEvents.aspx. Last Visited at: 13 Feb 2020.

۷. قانون کنوانسیون بین‌المللی ارتباطات دور، مشتمل بر یک مقدمه، ۸۲ ماده، یک فرمول نهایی و سه ضمیمه و یک پروتکل نهایی، ۶ پروتکل الحاقی و ۴۸ قطعنامه، سه توصیه و سه خواسته که در تاریخ ۱۳۵۵/۱۰/۸ برابر ۲۵ اکتبر ۱۹۷۳ در ملاکاتور مولینوس (اسپانیا) تنظیم و از ←

دو کنفرانس دیگر علاوه بر کنفرانس‌های قبلی در سال‌های ۱۹۸۵[۲] و ۱۹۸۸[۳] در ژنو برگزار شد که به‌طور خاص به موضوعات فضایی «استفاده از مدار ماهواره‌ای ثابت زمین[۴] و برنامه‌ریزی سرویس‌های فضایی جهت بهره‌برداری از آن» می‌پرداخت (جباری و تاج‌آبادی، ۱۳۹۱: ۱۱۲).

در سال ۱۹۸۹ و در جریان سیزدهمین اجلاس تام‌الاختیار سران کشورهای عضو[۵]، مقررات مربوط به تصویب اساسنامه و اصلاح کنوانسیون اتحادیه بین‌المللی مخابرات، به ترتیب تصویب و اصلاح شد. در این کنفرانس اهمیت ارائه کمک‌های فنی به کشورهای درحال‌توسعه در همان وضعیتی که این کشورها به‌طور سنتی به فعالیت‌های استانداردسازی و مدیریت طیف می‌پردازند، تأکید شد.

در سال ۱۹۹۲ نیز کنفرانس دیگری در ژنو[۶] برگزار شد. این کنفرانس، در راستای انطباق بیشتر با شرایط پیچیده و رقابتی روزافزون، تغییراتی را در اتحادیه داد. درنتیجه این سازمان‌دهی مجدد، اتحادیه، متناسب با سه حوزه اصلی فعالیت‌های خود و نیز همسو با اهداف نهایی خود (رشد و توسعه ارتباطات و شبکه‌های جهانی و کمک به توسعه زیرساخت‌های ارتباطی) به سه بخش تقسیم شد[۷]. اکنون ۱۹۳ کشور و ۷۰۰ نهاد خصوصی از سرتاسر جهان عضو این اتحادیه هستند و دارای دوازده اداره مختلف در سطوح منطقه‌ای می‌باشد. این اتحادیه که مقر آن در ژنو می‌باشد[۸].

بنابراین، می‌توان گفت اتحادیهٔ بین‌المللی مخابرات، سازمانی بین‌المللی است که دولت‌ها و بخش خصوصی از طریق آن شبکه‌ها و خدمات ارتباطات جهانی را هماهنگ می‌کنند و نقش کلیدی را در استانداردسازی و توسعه صنعت ارتباطات و البته موضوعات امنیت سایبری را از سال ۲۰۰۷ تاکنون ایفا می‌نماید که در قسمت‌های بعدی شرح آنها خواهد آمد.

↩طرف هیئت نمایندگی ایران به امضا رسیده است، در تاریخ ۱۳۵۵/۱۰/۸ به تصویب مجلس شورای اسلامی رسید و اجازه تسلیم اسناد تصویب آن داده شد.

1.The Plenipotentiary Conference, (Malaga Torremolinos, 1973). Available at: http://www.itu.int/en/history/Pages/listOFITUConferencesAssembliesAndEvents.aspx.Last Visited at: 10 Feb 2020.

2. World Administrative Radio Conference on the Use of the Geostationary – Satellite Orbit and the Planning of the Space Service UTILIZNG IT (1 ST SESSION) (Geneva, 1985). Available at: http://www.itu. Int/ en/history/pages/ListOFITUConferencesAssembliesAndEvents,aspx. Last Visited at: 06 Feb 2020.

3. World Administrative Radio Conference on the Use of the Geostationary – Satellite Orbit and the Planning of the Space Service UTILIZNG IT (1 ST SESSION) (Geneva, 1988). Available at: http://www.itu. Int/ en/history/pages/ListOFITUConferencesAssembliesAndEvents,aspx. Last Visited at: 06 Feb 2020.

۴. مدار ماهواره هم‌زمانی که مدار چرخش و جهت آن بر روی صفحه‌ای است که از خط استوای زمین می‌گذرد (راهنمای اصطلاحات و واژه رادیویی، ۱۳۸۹).

5.The Plenipotentiary Conference, (Nice, 1989). Available at: http://witu.int/en/history/Pages/ListOFITU.ConferencesAssembliesAndEvents.asp, Last Visited at: 06 Feb 2020.

6. Additional Plenipotentiary Conference, (Geneva, 1992). Available at: http://www.itu.int/en/history/Pages/ListOFITUConferencesAssembliesAndEvents.aspx. Last Visited at: 22 Jan 2020

7.http://www.itu.int/en/history/Pages/ITUsHistory.aspx.

8.http://www.itu.int/en/Pages/default.aspx

۴. اقدامات اتحادیه بین‌المللی مخابرات در امنیت سایبری

جدای از اقدامات ملی تلاش‌های بین‌المللی در راستای پرداختن به مشکلات و تهدیدات در فضای سایبری در مقایسه با رویکردهای ملی از لحاظ دسترسی به منابع محدودتر می‌باشند. درواقع اغلب سازمان‌های بین‌المللی فعال در حوزهٔ سایبری، مبتنی بر معاهدات چندجانبه و تحت تأثیر دولت‌های تأسیس کننده آنان می‌باشند که می‌توان سازمان ملل متحد، اتحادیه بین‌المللی مخابرات، شورای اروپا در سطح جهانی و اتحادیه اروپا، ناتو، اتحادیه آفریقا، سازمان کشورهای آمریکایی، سازمان همکاری‌های شانگهای، آسه آن و سازمان همکاری‌های اقتصادی آسیا اقیانوسیه در سطح منطقه‌ای نام برد. درحالی‌که اغلب امور حوزه سایبری توسط دولت‌ها سازمان‌دهی می‌شود، سازمان‌های بین‌المللی به بهبود وضع و ارتقای راهبردهای جهانی، ایجاد ساختارها، نهادها و سیاست‌های مناسب منطقه‌ای و بین‌المللی در راستای پیشگیری از سوءاستفاده از فناوری‌ها، ارتقای توانایی مقابله با اتفاقات سایبری و اجرای حقوق مخاصمات مسلحانه می‌پردازند (تقی‌زاد، ۱۳۹۵: ۶۷).

از جمله اقدامات اتحادیه بین‌المللی مخابرات برگزاری اجلاس جهانی جامعه اطلاعاتی و نتیجه حاصل از این اجلاس برنامه کاری جهانی امنیت سایبری و قطعنامه‌ها می‌باشند که در ذیل به شرح آنها پرداخته می‌شود.

۴-۱. اجلاس جهانی جامعه اطلاعاتی[1] و نتایج حاصل از آن

مقدمات برگزاری این اجلاس جهانی از سال ۱۹۹۸ به‌وسیله اتحادیه بین‌المللی مخابرات و با حمایت دبیرکل وقت سازمان ملل متحد پایه‌ریزی شد. با توجه به اهمیت تاریخی این اجلاس، مجمع عمومی سازمان ملل متحد، طی قطعنامه مصوب ۲۱ دسامبر ۲۰۰۱، از سران تمام کشورهای دنیا خواست تا برای این مشارکت فعال در این نشست حضور یابند.

کمیته تدارک اجلاس جهانی سران، درباره جامعه اطلاعاتی، سه گردهمایی مقدماتی با شرکت نمایندگان دولت‌ها، بخش خصوصی و جامعه مدنی از ژوئیه ۲۰۰۲ تا سپتامبر ۲۰۰۳ تشکیل داد. به موازات این گردهمایی‌های تدارکاتی بین‌المللی، چند کنفرانس تدارکاتی منطقه‌ای در فاصله بهار ۲۰۰۲ تا بهار ۲۰۰۳ در پنج قاره با حضور نمایندگان دولت‌ها، بخش خصوصی و جامعه مدنی مناطق برگزارکننده، جهت بحث و بررسی درباره دستور کار اجلاس جهانی برگزار شد.

نخستین پیش‌نویس «اعلامیه اصول» و «برنامه عمل» در دومین گردهمایی تدارکاتی بین‌المللی درباره اجلاس جهانی سران تهیه و تدوین شد (علی‌آبادی، بی‌تا: ۱۴۱ – ۱۴۰).

بعد از آن، اتحادیه بین‌المللی مخابرات به‌عنوان اصلی‌ترین نهاد در برگزاری «اجلاس جهانی جامعه اطلاعاتی» می‌باشد که طی دو دوره، یک‌بار در ژنو در سال ۲۰۰۳ و بار دیگر در تونس در

1.World Summit on the Information Society

سال ۲۰۰۵ برگزار گردید. در این اجلاس دولت‌ها، سیاست‌گذاران و کارشناسان امر از سرتاسر نقاط دنیا، ایده‌ها و تجربیات خود را در مورد بهترین نحوه بررسی و پرداختن به موضوعات پیش‌آمده در خصوص توسعه یک جامعه اطلاعاتی جهانی از جمله توسعه قوانین و استانداردهای سازگار به اشتراک گذاشتند. نتایج و دستاوردهای حاصله از این دو اجلاس، در چهار سند تحت عناوین «اعلامیه اصول ژنو»، «برنامه اجرایی ژنو»، «تعهدات تونس» و «برنامه کاری تونس برای جامعه اطلاعاتی» گنجانده شده است. از میان اسناد فوق «برنامه اجرایی ژنو» بر اهمیت اقدامات در راستای مبارزه علیه جرایم سایبری و ایجاد امنیت سایبری تأکید می‌نماید. به این صورت که در برنامه آینده آمده است:

مسیر اجرایی شماره ۵ برنامه اجرایی ژنو[1]:

الف) ایجاد اعتماد و امنیت در استفاده از فناوری ارتباطات و اطلاعات که اعتماد و امنیت جزء ارکان اصلی جامعه اطلاعاتی می‌باشند.

ب) دولت‌ها، همسو با همکاری با بخش خصوصی، باید از طرقی مثل تدوین خطوط راهنمایی که تلاش‌های جاری در این حوزه‌ها را در نظر دارد، مد نظر قرار دادن قوانینی که اجازه انجام تحقیقات و تعقیب مؤثر درباره سوءاستفاده از فناوری‌های ارتباطات را می‌دهد، ارتقای سطح همکاری‌های مؤثر متقابل، تقویت پشتیبانی نهادها در سطح بین‌المللی به منظور پیشگیری، شناسایی و بازیابی توانایی در برابر چنین اتفاقاتی و ترغیب برای آموزش و افزایش آگاهی در خصوص جرایم سایبری و سوءاستفاده از فناوری‌های ارتباطات و اطلاعات؛ شناسایی، پیشگیری و عکس‌العمل‌های لازم را انجام دهند».

همین‌طور در دورهٔ دوم «اجلاس جهانی جامعه اطلاعاتی» که در سال ۲۰۰۵ در تونس برگزار گردید، به مسئله جرایم سایبری پرداخته شد. «برنامه کاری تونس برای جامعه اطلاعاتی» در بند ۴۰ خود بر نیاز به همکاری‌های بین‌المللی در مبارزه علیه جرایم سایبری تأکید نمود و در این خصوص، به رویکردهای قانون‌گذاری موجود، ازجمله قطعنامه‌های مجمع عمومی سازمان ملل متحد (۵۶/۱۲۱ و ۵۵/۶۳) و کنوانسیون جرایم سایبری شورای اروپا ۲۰۰۱ اشاره می‌نماید (Marion, 2010). در این بند آمده است: «ما بر اهمیت پیگرد جرایم رایانه‌ای به انضمام جرایمی که در یک حوزه قضایی صورت گرفته، ولی بر دیگر حوزه‌ها تأثیر می‌گذاردند، تأکید می‌کنیم. ضرورت تأثیر راهکارها یا ابزارهای مؤثر و کارآمد در سطوح ملی و منطقه‌ای برای افزایش همکاری بین‌المللی در میان مقامات ذی‌صلاح و پلیس تخصصی جرایم رایانه‌ای را تأکید می‌نماییم. ما از دولت‌ها درخواست می‌نماییم در همکاری با سایر گروه‌های ذی‌نفع و سرمایه‌گذاری برای تدوین و تصویب قوانین لازم برای توسعه و پیشرفت تحقیق و پیگرد جرایم

1.Geneva Action plan – Action Line C5
http://groups.itu.int/stocktaking/About/WSISActionLines/C5.Cybersecurity.aspx

رایانه‌ای با توجه به چهارچوب‌های موجود برای مثال قطعنامه‌های شماره ۵۵/۶۳ و ۵۶/۱۲۱ مجمع عمومی سازمان ملل متحد در رابطه با مبارزه با سوءاستفاده از فناوری اطلاعات و پروژه‌های منطقه‌ای در این زمینه اقدام نماید» (Gercke, 2012: 130).

علاوه بر، برگزاری دو دوره اجلاس مذکور در متن، در سال‌های اخیر نیز اجلاس جهانی جامعه اطلاعاتی نشست‌هایی داشته است[۱].

درواقع به عنوان نتیجه حاصله از برگزاری اجلاس‌های جهانی جامعه اطلاعاتی و برنامه کاری جهانی امنیت سایبری، اتحادیه بین‌المللی ارتباطات تنها نهاد تسهیل‌کننده اجرای «پنجمین مسیر اجرایی از برنامه اجرایی ژنو» در خصوص ایجاد اطمینان و امنیت در استفاده از فناوری ارتباطاتی و اطلاعاتی شناخته شد[۲]. در دومین جلسه در خصوص مسیر اجرایی پنجم اجلاس جهانی جامعه اطلاعاتی در سال ۲۰۰۷ دبیر کل اتحادیه بین‌المللی ارتباطات، بر اهمیت همکاری بین‌المللی در راستای مبارزه با جرایم سایبری تأکید و اجرای «برنامهٔ کاری جهانی امنیت سایبری اتحادیه بین‌المللی ارتباطات» را خواستار شد. اهمیت این برنامه کاری بدین‌جهت است که از ۷ هدف کلیدی بر اساس ۵ رکن راهبردی- شامل بسط راهبردهای توسعه مدل‌های قانون‌گذاری جرایم سایبری، حائز اهمیت در این حوزه تشکیل شده است.

ارکان پنج‌گانه برنامه کاری جهانی امنیت سایبری عبارتند از:

۱. حوزه کاری یک؛ تدابیر حقوقی و قانونی[۳]

در حوزه کاری یک، این موضوع مطرح شده است که دبیرکل اتحادیه بین‌المللی مخابرات باید همکاری را بین بازیگران مختلف ارتقا بخشد تا ابزارهای حقوقی مؤثر در ایجاد اعتماد و امنیت در استفاده از فناوری اطلاعات و ارتباطات، استفاده مؤثر از توصیه‌های اتحادیه بین‌المللی مخابرات و سایر استانداردها مطابق با موافقت‌نامه‌های بین‌المللی فعلی شناسایی و مشخص شود.

در مورد چگونگی دستیابی به توافق‌های موجود در این زمینه به‌عنوان مثال، کنوانسیون سایبری شورای اروپا در زمینه جرایم سایبری و کنوانسیون پیشگیری از تروریسم سال ۲۰۰۵ می‌باشد. کنوانسیون مربوط به جرایم سایبری را اگرچه به رسمیت شناخته‌اند؛ اما کنوانسیون جرایم سایبری نمی‌تواند به عنوان تنها راه حل برای همه کشورها پیشنهاد شود. اگرچه وضعیت کنوانسیون را به

---

۱. اجلاس جامعه جهانی اطلاعاتی در سال ۲۰۱۵ با هدف توسعه موارد کاربرد فناوری اطلاعات و ارتباطات و راه‌اندازی کسب‌وکارهای الکترونیکی آنلاین نشستی را برگزار نموده است. در سال ۲۰۱۶ با موضوع «سیاست رسمی کشورها در قبال جامعه اطلاعاتی» به کار خود ادامه داده است. در سال ۲۰۱۷ نیز نشستی با شعار «جوامع اطلاعاتی و دانش‌بنیان در جهت اهداف توسعه پایدار» برگزار نموده است. در سال ۲۰۱۸ هیچ نشستی نداشته است.

2. Report by the Secretary-General. ITU COUNCIL CONTRIBUTION TO THE 2016 UNITED NATIONS HIGH-LEVEL POLITICAL FORUM ON SUSTAINABLE DEVELOPMENT, Document C16/INF/13.
//sustainabledevelopment.un.org/content/documents/10422International%20Telecommunication%20Union%20Council%20.pdf

3. Work Area one, “Legal measures”

عنوان نمونه اقدامات قانونی تحقق یافته به عنوان یک ابتکار منطقه‌ای متعلق به کشورهای امضاکننده، مطابق با وضعیتی که به آن تعلق می‌گیرد، تصدیق کند[1].

۲. حوزه کاری دو؛ تدابیر فنی و شکلی[2]

حوزه کاری دو، بر اقدامات اصلی برای رفع آسیب‌پذیری در محصولات نرم‌افزاری، از جمله برنامه‌های اعتباربخشی، پروتکل‌ها و استانداردها متمرکز شده است. بحث و گفتگو در مورد چگونگی ایجاد کار موجود در این زمینه از جمله، معیارهای مشترک و کار اتحادیه بین‌المللی مخابرات و سایر سازمان‌های استانداردسازی انجام شده است. در مورد پیشنهادات اجماع وجود نداشته است که اتحادیه بین‌المللی مخابرات بتواند امکاناتی را برای چارچوب اعتبار سنجی امنیت در سطح جهانی بپذیرد[3].

۳. حوزه کاری سه؛ ساختارهای سازمانی[4]

حوزه کاری سه، روی یک چارچوب بالقوه برای ارزیابی آمادگی امنیت سایبری متمرکز شده است. یکی از اعضا پیشنهاد کرد که اتحادیه بین‌المللی مخابرات بتواند «فهرست آمادگی سایبری»[5] را بر اساس یک چارچوب ساختارهای سازمانی پیشنهادی تهیه کند، از جمله:

- یک رهبر ملی برای هماهنگی در امنیت سایبری یا شورای ملی امنیت سایبری؛
- یک تیم واکنش اضطراری رایانه[6] ملی که نماینده حفاظت از زیرساخت‌های امنیتی در یک دولت است یا یک کانون ملی برای هماهنگی[7].

۴. حوزه کاری چهارم؛ ظرفیت‌سازی[8]

پیشنهادات ارائه شده در حوزه کاری چهارم مبنی بر اینکه:

- دبیرکل همچنان از برگزاری و ره‌آوردهای کنفرانس‌های منطقه‌ای امنیت سایبری از سوی اتحادیه بین‌المللی مخابرات که سازمان‌های دولتی و خصوصی را برای رفع چالش‌های مهم مربوط به امنیت سایبری گرد هم می‌آورند، حمایت نماید.

---

1. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf, p. 6, Last Visited at: 15 Jul 2020.
2. Work Area two, "Technical and procedural measures"
3. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf, p.9, Last Visited at: 15 Jul 2020.
4. Work Area three, "Organizational structures"
5. GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY. STRATEGIC ENGAGMENT IN CYBERSECURTIY: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf, p.13
6. Computer emergency response team (CERT)
7. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf, p. 12, Last Visited at: 15 Jul 2020.
8. Work Area four, "Capacity building"

– دبیرکل برای تقویت برنامه‌های درسی علوم رایانه و مهندسی ارتباط از راه دور اطمینان حاصل کند که درواقع امنیت را به عنوان بخشی از محور اصلی مطالعه در برمی‌گیرد[1].

۵. منطقه کاری پنجم؛ همکاری بین‌المللی[2]

در مورد توصیه‌های منطقه کاری پنجم، اجماع عمومی حاصل شد و هیچ مخالفتی اعلام نشده است[3] و تأکید گردید که باید با سایر حوزه‌های کاری از جمله تمدید دستورالعمل برنامه جهانی امنیت سایبری که از طریق اتحادیه بین‌المللی مخابرات به روش‌های عملی پشتیبانی می‌شود، هماهنگی وجود داشته باشد[4].

همچنین اهداف هفتگانه بر اساس ۵ رکن مذکور به شرح زیر می‌باشند:

۱) گسترش راهبردها به منظور ایجاد یک مدل قانون‌گذاری جرایم سایبری که در سطح جهانی قابل اجرا باشد و با تدابیر قانون‌گذاری منطقه‌ای و ملی موجود قابل تبادل اطلاعات باشد؛

۲) گسترش راهبردها به منظور سیاست‌گذاری و ایجاد ساختارهای سازمانی ملی و منطقه‌ای مناسب برای مقابله با جرایم سایبری؛

۳) توسعه راهبردها برای وضع یک معیار حداقلی امنیتی مورد پذیرش در سطح جهانی و طرح‌های اعتبارگذاری در ارتباط با برنامه‌های نرم‌افزاری و سیستم‌ها؛

۴) توسعه راهبردها برای ایجاد یک چهارچوب جهانی نظارت، هشدار و عکس‌العمل نسبت به اتفاقات برای تضمین هماهنگی‌های فرامرزی بین اقدامات ابتکاری موجود؛

۵) توسعه راهبردها برای ایجاد و تائید یک سیستم هویتی دیجیتال جهانی و جامع و ایجاد ساختارهای سازمانی ضروری برای تضمین شناسایی اعتبارنامه‌های دیجیتال اشخاص حقیقی فراتر از مرزهای جغرافیایی؛

۶) توسعه یک راهبرد جهانی به منظور تسهیل ایجاد ظرفیت‌های انسانی و ساختاری برای بالا بردن سطح علم و آگاهی در زمینه‌های فوق؛

۷) ارائه توصیه در مورد چهارچوب بالقوه و احتمالی در خصوص یک راهبرد چند محوری جهانی در راستای همکاری، گفتمان و هماهنگی جهانی در همه زمینه‌های فوق الذکر[5].

در همین راستای یک گروه کارشناسی و متخصص برای ارائه و اجرای راهبردهای مربوط به «برنامه کاری جهانی امنیت سایبری» ایجاد شد. به منظور تحلیل و توسعه اقدامات و راهبردها با توجه به اهداف هفتگانه فوق، دبیرکل اتحادیه یک گروه تخصصی پیشرفته را متشکل از

1. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf, p. 13, Last Visited at: 15 Jul 2020.
2. Work Area five, "International cooperation"
3. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf, p. 15, Last Visited at: 15 Jul 2020.
4. www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html (10.9.1394)
5. http://www.int/osg/csd/cybersecurity/gca/pillars-goals/index.html

نمایندگان کشورهای عضو، نمایندگان بخش‌های صنعت و علوم تشکیل داد. در سال ۲۰۰۸ گروه مذکور پس از جمع‌بندی مذاکرات خود، گزارش راهبردی جهانی[1] را منتشر کرد (تقی‌زاد، ۱۳۹۵: ۸۷).

همچنین مرتبط‌ترین موضوعات راجع به جرایم سایبری شامل تدابیر حقوقی و قانونی لازم در فصل اول این گزارش آمده است که علاوه بر آن به منظور مرور رویکردهای متفاوت منطقه‌ای و بین‌المللی در مبارزه با جرایم سایبری و ایجاد امنیت سایبری، مقررات و قوانین کیفری، اسناد شکلی و آئین دادرسی، قواعد حاکم بر مسئولیت ارائه‌کنندگان خدمات اینترنتی و تأمین حقوق بنیادین کاربران اینترنتی را مورد بازبینی قرار می‌دهد.

۴-۲. قطعنامه‌های اتحادیه بین‌المللی مخابرات

اتحادیه بین‌المللی مخابرات چندین قطعنامه مرتبط با موضوع امنیت سایبری را درحالی‌که مستقیماً و با مقررات و قوانین کیفری مشخص به مسئله نمی‌پردازند، صادر نموده است. از جمله مهم‌ترین این قطعنامه‌ها عبارتند از:

۴-۲-۱. قطعنامه شماره ۱۳۰؛ تقویت نقش اتحادیه بین‌المللی مخابرات در امنیت سایبری و ایجاد اطمینان و امنیت در استفاده از فناوری‌های ارتباطی و اطلاعاتی.

در کنفرانس مستقل اتحادیه در گوادالاخارای مکزیک در سال ۲۰۱۰[2]، به صدور قطعنامه ۱۳۰ بر اهمیت حیاتی زیرساخت‌های اطلاعاتی و ارتباطی و کاربرد آنها، تقریباً در تمام انواع فعالیت‌های اجتماعی و اقتصادی تأکید شده است و همچنین اشاره گردیده است که با استفاده از فناوری اطلاعات و ارتباطات، تهدیدات جدیدی از منابع مختلف ایجاد شده است که بر وجود اعتماد و امنیت در استفاده از فناوری اطلاعات و ارتباطات در همه کشورهای عضو، اعضای بخش و سایر ذی‌نفعان، از جمله همه کاربران استفاده‌کننده از فناوری اطلاعات و ارتباطات و همچنین حفظ صلح و توسعه اقتصادی و اجتماعی همه کشورهای عضو نیاز است. تهدیدات و آسیب‌پذیری شبکه‌ها همچنان سبب افزایش چالش‌های امنیتی در مرزهای ملی برای همه کشورها، به‌ویژه کشورهای درحال‌توسعه، کشورهای کمتر توسعه یافته، کشورهای دارای اقتصاد در حال گذار را شده است، درحالی‌که در این زمینه تقویت نقش اتحادیه بین‌المللی مخابرات در ایجاد اعتماد و امنیت در استفاده از فناوری اطلاعات و ارتباطات و نیاز به تقویت همکاری بین‌المللی و توسعه مناسب اقدامات ملی، منطقه‌ای و بین‌المللی (به عنوان مثال: توافق‌نامه، یادداشت‌های تفاهم و غیره) لازم می‌نماید و نیز به تکامل مداوم در زمینه فناوری‌های جدید برای حمایت از شناسایی زودهنگام

1.ITU Global Strategic Report from:www.itu.int/osg/cybersecurity/gca/global-strategic-repot/index.html
2.ITU Resolution 130 (Rev.Guadalajara, 2010)

و واکنش‌های هماهنگ و به‌موقع وقایع یا حوادثی که امنیت رایانه‌ها را به خطر می‌اندازد یا حوادث امنیتی شبکه کامپیوتری که می‌تواند در دسترس بودن، یکپارچگی و محرمانه بودن زیرساخت‌های حیاتی در کشورهای عضو اتحادیه اروپا و برای استراتژی‌هایی که تأثیر این حوادث و خطرات و تهدیدات رو به رشدی که این سیستم‌عامل‌ها در معرض آن قرار دارند را کاهش می‌دهد؛ به عنوان یک نیاز اشاره کرد[1].

مداقه در متن این قطعنامه نشان می‌دهد که صرف اشاره به اهمیت زیرساخت‌های اطلاعاتی و ارتباطی و کاربرد آنها در فعالیت‌های اجتماعی و اقتصادی و چالش‌های امنیتی آنها به ویژه در کشورهای درحال‌توسعه یا کمتر توسعه‌یافته و یا دارای اقتصاد گذار با اتکا به اقداماتی از قبیل امضا تفاهم‌نامه یا یادداشت‌های همکاری مکفی نبوده و نیازمند بسترسازی حقوقی، تدوین و قانون‌گذاری در جهت رفع چالش‌های امنیتی اقتصادی و اجتماعی در فضای سایبری می‌باشد که لازمه آن تغییر رویکرد حقوقی از حقوق نرم به حقوق سخت است؛ اما به نظر می‌رسد که اتحادیه در مراحل اولیه پذیرش حقوق نرم هست و رفع این چالش‌ها را تنها با عنوان یک نیاز اشاره می‌کند.

۴-۲-۲. قطعنامه شماره ۱۸۱؛ بهره‌مندی از تعاریف و اصطلاحات مربوط به ایجاد اعتماد و امنیت در استفاده از فناوری اطلاعات و ارتباطات

قطعنامه مذکور که در کنفرانس مستقل اتحادیه در گوادالاخارای مکزیک در سال ۲۰۱۰[2] صادر شده هست، نیاز به ایجاد اعتماد و امنیت در استفاده از ارتباطات راه دور با تقویت چهارچوب اعتماد و نیاز به دولت‌ها، در همکاری با سایر سهامداران در درون نقش‌های خود، برای ایجاد قوانین لازم برای تحقیق و تعقیب جرایم اینترنتی در سطح ملی، منطقه‌ای و بین‌المللی مورد تأکید واقع شده است.

نحوه بهره‌مند شدن از تعاریف و اصطلاحات برای ایجاد قوانین لازم در این قطعنامه با هاله‌ای از ابهام روبه‌روست؛ چراکه هیچ اشاره‌ای به اینکه تعاریف و اصطلاحات از کدام منظر (حقوقی، فناوری و ...) مورد توجه قرار گیرند، صورت نگرفته است.

نحوه تحقیق و تعقیب جرایم اینترنتی در قوانین داخلی هر کشوری متفاوت بوده و بعضاً وجود ضعف در قوانین داخلی کشورها (به‌ویژه کشورهای در حال توسعه یا کمتر توسعه‌یافته) موجب می‌گردد، امکان یکسان‌سازی قوانین در جامعه بین‌المللی سخت به نظر رسد؛ بنابراین بایستی در وهله نخست، نقاط ضعف قوانین داخلی کشورها رفع گردد سپس ارائه تعاریف واحد دست‌کم در سطح منطقه‌ای صورت گیرد تا بتوان در سطح بین‌المللی جهت یکسان‌سازی قوانین گام برداشت.

1. ITU Resolution 130 (Rev.Guadalajara, 2010)
2. https://www.itu.int/osg/csd/cybersecurity/.../RESOLUTION_181.pdf

۴-۲-۳. قطعنامه شماره ۵۸؛ تشویق به ایجاد تیم‌های فعال کامپیوتری ملی؛ به‌ویژه در کشورهای درحال‌توسعه

این قطعنامه، صادره از مجمع استانداردسازی جهانی مخابرات در دبی در سال ۲۰۱۲[1]، دبیرکل و مدیر ۳ بخش اتحادیه بین‌المللی ارتباطات را به منظور همکاری با یکدیگر جهت پیگیری ابتکاراتی که در برطرف کردن شکاف استانداردسازی که بین کشورهای در حال توسعه وجود دارد، ملزم نمود؛ اما ذکری از برطرف کردن شکاف استاندارسازی در کدام جهت را ننموده است.

۳-۲-۴. قطعنامه شماره ۱۷۴؛ نقش اتحادیه بین‌المللی مخابرات در رابطه با مسائل سیاست عمومی بین‌المللی در مورد خطر استفاده غیرقانونی از فناوری اطلاعات و ارتباطات

در قطعنامه شماره ۱۷۴، صادره در اجلاس جهانی جامعه اطلاعاتی در بوسان کره جنوبی در سال ۲۰۱۴[2]، اجلاس جهانی جامعه اطلاعاتی در بیانیه اصول ژنو، از فعالیت سازمان ملل متحد برای جلوگیری از استفاده بالقوه از فناوری اطلاعات و ارتباطات برای مقاصدی با اهداف حفظ ثبات و امنیت بین‌المللی متناقض که ممکن است بر روی یکپارچگی زیرساخت‌ها در داخل کشور تأثیر بگذارد؛ حمایت کرد و اشاره نمود که لازم است از استفاده منابع اطلاعاتی و فناوری برای مقاصد جنایی و تروریستی و با رعایت احترام به حقوق بشر جلوگیری شود.

البته می‌توان به این نکته هم اشاره نمود که با تسلط کشور آمریکا بر زیرساخت اینترنت، این کشور قصد دارد تا با بسط حقوق و قوانین بین‌المللی به فضای سایبری بر اساس تفسیر و منافع خود، فرآیند منتسب کردن جرم و حملات تروریستی سایبری را در اختیار بگیرد و در مواقع لزوم از منافع آن در برابر کشورهای رقیب استفاده نماید که این عمل جز بهره‌گیری از سیاست و حقوق بین‌الملل کذب آمریکایی به نفع خود چیز دیگری نمی‌تواند باشد.

همچنین در این اجلاس با توجه به بیانیه اصول ژنو اشاره گردیده است که دولت‌ها در همکاری با بخش خصوصی، باید دستورالعمل‌هایی را برای جلوگیری، شناسایی، مقابله با جرایم اینترنتی و سوءاستفاده از فناوری اطلاعات و ارتباطات ایجاد نمایند که این امر با در نظر گرفتن تلاش‌های مداوم در این زمینه، مانند تدوین قوانینی که می‌تواند مؤثر باشند و تحقیق و تعقیب چنین سوءاستفاده‌هایی، تقویت حمایت نهادی در سطح بین‌المللی برای جلوگیری و تشخیص چنین حوادثی و تشویق به آموزش و پرورش و افزایش آگاهی حاصل می‌شود.

1. https://www.itu.int/en/ITU-T/.../resolutions/Resolution%2058.pdf
2. https://www.itu.int/en/action/internet/.../Resolution_174_pp14.pdf

۴-۲-۵. قطعنامه شماره ۱۷۹؛ نقش اتحادیه بین‌المللی مخابرات در حفاظت از کودکان آنلاین

در کنفرانس مستقل اتحادیه در بوسان کره جنوبی در سال ۲۰۱۴[1] و صدور قطعنامه ۱۷۹، با توجه به موضوع آن اشاره گردیده است که اینترنت نقش مهمی را در ارائه آموزش و غنی‌سازی برنامه درسی برای کودکان دارد. به گونه‌ای که به یک برنامه کاری در اشکال مختلف از جمله فعالیت‌های آموزشی، فرهنگی و سرگرمی برای کودکان تبدیل شده است که کودکان به عنوان فعال‌ترین شرکت‌کنندگان آنلاین هستند. والدین، راهنمایان و مربیان برای مراقبت از کودکان مسئولیت راهنمایی و هدایت کردن فعالیت‌های کودکان در اینترنت را دارند. نوآوری حفاظت آنلاین کودکان باعث محافظت از حقوق مدنی و سیاسی آنها نیز می‌شود و همچنین نیاز فوری و تقاضای جهانی برای حفاظت از کودکان از استثمار و قرار گرفتن در معرض خطر و فریب هنگام استفاده از اینترنت یا فناوری اطلاعات و ارتباطات وجود دارد. همچنین اشاره گردیده است که به دلیل توسعه رو به رشد، تنوع و گسترش دسترسی به فناوری اطلاعات و ارتباطات در سراسر جهان، به‌ویژه اینترنت و استفاده روزافزون از آن توسط کودکان در زمان‌های بدون کنترل و هدایت بسیار مهم و ضروری است که به‌منظور رسیدگی به مسئله امنیت سایبری کودکان، اقدامات پیشگیرانه برای محافظت از کودکان در سطح ملی، منطقه‌ای یا بین‌المللی به عمل آید.

همچنین در این کنفرانس بر الزام همکاری بین‌المللی و ادامه درخواست از یک رویکرد به شکل چندجانبه برای ارتقاء مسئولیت اجتماعی در بخش فناوری اطلاعات و ارتباطات به‌طوری‌که به شکل مؤثر در استفاده از انواع ابزارهای موجود برای ساخت اعتمادبه‌نفس در استفاده از شبکه‌های فناوری ارتباطات و اطلاعات و خدمات و کاهش خطرات بر فرزندان باشد، تأکید شد و حفاظت آنلاین کودکان در اولویت کاری جامعه جهانی قرار گرفت که نیازمند همکاری ملی، منطقه‌ای و بین‌المللی برای ترویج حفاظت آنلاین کودکان با ارائه راهنمایی در مورد رفتار ایمن آنلاین می‌باشد[2].

به نظر می‌رسد اتخاذ یک رویه نظارتی واحد و راه‌اندازی شبکه‌های سایبری مطمئن و ایمن برای کودکان از سوی کشورها بتواند برای ایجاد امنیت سایبری کودکان آنلاین در هنگام فعالیت برای جلوگیری از بزه دیده‌گی و بزهکاری مؤثر باشد.

1. https://www.itu.int/.../cybersecurity/.../Resolutions/pp-14_Res.%20179.pdf
2.Ibid

۴-۲-۶. قطعنامه شماره ۴۵؛ افزایش مکانیزم‌های همکاری در زمینه امنیت سایبری؛ شامل مبارزه با اسپم و مهار آن

قطعنامه شماره ۴۵، صادره در کنفرانس توسعه جهانی مخابرات در دبی در سال ۲۰۱۴[1] بر نقش مخابرات و فناوری ارتباطات و اطلاعات به عنوان ابزار مؤثر برای ترویج صلح، توسعه اقتصادی، امنیت و ثبات و افزایش دموکراسی، انسجام اجتماعی، حکمرانی شایسته و حاکمیت قانون اشاره گردیده است و نیاز به مقابله با چالش‌ها و تهدیدهای روزافزون ناشی از سوءاستفاده از این تکنولوژی، از جمله برای اهداف جنایی و تروریستی درعین‌حال با احترام به حقوق بشر و همچنین نیاز به اعتماد و امنیت در استفاده از فناوری ارتباطات و اطلاعات با تقویت چارچوب اعتماد و نیاز به دولت‌ها در همکاری با سایر سهامداران در نقش‌های خاص خود، برای ایجاد قوانین لازم برای تحقیق و تعقیب جرایم اینترنتی در سطح ملی و همکاری در سطح منطقه‌ای و بین‌المللی با توجه به چهارچوب‌های موجود مطرح شده است و نیز بیان گردیده است که زیرساخت‌های مخابراتی کلیدی در سطح جهانی به همدیگر متصل هستند؛ به این معنی که امنیت زیرساختی پایین در یک کشور باعث آسیب‌پذیری بیشتر و خطرات بیشتر در کشورهای دیگر می‌شود؛ بنابراین بایستی اطلاعات مختلف، مواد، بهترین شیوه‌ها و منابع مالی به‌صورت مناسب در اختیار کشورهای عضو سازمان‌های ملی، منطقه‌ای و دیگر سازمان‌های مربوط با توجه به نقش آنها قرار گیرد تا در این زمینه تمهیدات لازم را بیندیشند.

برای ایجاد قوانین لازم جهت تحقیق و تعقیب جرایم اینترنتی در سه سطح ملی، منطقه‌ای و بین‌المللی از طریق توجه به چهارچوب‌های موجود و اشاره صرف به آن رفع مشکل نمی‌نماید. لذا بهتر بود در این کنفرانس چهارچوب‌های موجود و محدودیت‌های آنها در صورت وجود، بررسی و ذکر می‌گردید تا کشورها نیز بهتر می‌توانستند در جهت قانون‌سازی و قانون‌گذاری در این حوزه عمل نمایند.

همچنین از طریق الزام کشورهای قدرتمند به لحاظ زیرساخت‌های امن مخابراتی در ارائه نحوه توانمندی آنها می‌توان به سایر کشورهای آسیب‌پذیر کمک نمود.

۴-۲-۷. قطعنامه شماره ۵۲؛ در زمینه مبارزه و مهار کردن اسپم

قطعنامه شماره ۵۲ که در مجمع جهانی استانداردسازی جهانی مخابرات در حمامه تونس در سال ۲۰۱۶[2] صادر شده، در متن این قطعنامه آورده شده است که مبادله ایمیل و سایر ارتباطات از راه دور در اینترنت به یکی از ابزارهای اصلی ارتباطات بین مردم در سراسر جهان تبدیل شده است. در این میان کلمه «اسپم» که برای آن تعاریف گوناگونی هم بیان شده است به عنوان یک مشکل

1. https://www.itu.int/en/ITU-D/Cybersecurity/.../45revDubai.pdf
2. https://www.itu.int/dms_pub/itu-t/.../T-RES-T.52-2016-PDF-E.pdf

گسترده‌ای است که موجب تلفات بالقوه برای ارائه دهندگان خدمات اینترنت، اپراتورهای مخابراتی تلفن همراه و کاربران تجاری شده است. اسپم برای فعالیت‌های جنایی، جعلی یا فریبنده استفاده می‌شود؛ که یک مشکل جهانی می‌باشد و دارای ویژگی‌های مختلف در مناطق مختلف است که بر بسیاری از ذی‌نفعان تأثیر می‌گذارد. بنابراین نیازمند همکاری بین‌المللی برای حل و فصل آن است. همچنین در این کنفرانس تأکید شده است که رسیدگی به مسائل مربوط به اسپم فوری می‌باشد؛ زیرا که بسیاری از کشورها به ویژه کشورهای در حال توسعه برای مقابله با اسپم‌ها نیاز به کمک فوری دارند و توصیه‌های مربوط به بخش استانداردهای مخابراتی و اطلاعات مربوطه از سوی دیگر سازمان‌های بین‌المللی در دسترس که با توجه به درس‌های آموخته شده می‌تواند جهت توسعه آینده در این زمینه ارائه شود و بیشتر بر اقدامات فنی در مبارزه و مهار کردن اسپم اشاره شده است.

عدم توافق واحد بر تعریف اسپم و عدم توجه به اقدامات فنی در مبارزه و مهار آن و اشاره به انجام فعالیت‌های جنایی یا فریبنده در محیط اسپم نشانگر این امر است که مجمع عملکردی ضعیف در این حوزه داشته است؛ چراکه با ایجاد یک کارگروه تخصصی (فنی- حقوقی) می‌توانست به اقدامات فنی در مبارزه و مهار اسپم سرعت بخشیده و از بروز فعالیت‌های جنایی و فریبنده در این محیط ممانعت به عمل آورد.

بحث و نتیجه‌گیری

دهه اخیر توسعه قابل توجهی را در ترویج اسناد بین‌المللی و منطقه‌ای راجع به مبارزه و مواجهه با جرایم سایبری به خود دیده است که البته خاستگاه، وضعیت حقوقی، قلمرو جغرافیایی، تمرکز ماهوی و سازوکار این اسناد به طور قابل ملاحظه‌ای با یکدیگر متفاوت می‌باشد که این اسناد گاهی الزام‌آور و گاهی نیز غیر الزام‌آور می‌باشند. در خصوص اتحادیه بین‌المللی مخابرات بایستی گفت که این اتحادیه برنامه کاری متفاوت جهانی را در جهت امنیت سایبری به صورت راهبردی برگزیده و چندین قطعنامه را در این خصوص به تصویب رسانده است.

یکی از اقدامات مهم اتحادیه بین‌المللی مخابرات، پروژه شاخص جهانی امنیت سایبری و اندازه‌گیری سطح توسعه امنیت سایبری در هر کشور است. هدف نهایی این پروژه کمک به ایجاد فرهنگ جهانی امنیت سایبری و یکپارچه‌سازی آن در هسته اصلی فناوری‌های اطلاعات و ارتباطات است. این پروژه توسط اتحادیه بین‌المللی مخابرات و شرکت بخش خصوصی[1] در حال انجام است.

1. ABI Research

همچنین اتحادیه بین‌المللی مخابرات هماهنگ‌کننده برای عمل به اصول پنج‌گانه ژنو و اجلاس سران جامعه اطلاعاتی برای کمک به کلیهٔ ذی‌نفعان در راستای ایجاد اطمینان و امنیت در استفاده از فناوری اطلاعات و ارتباطات در سطوح ملی، منطقه‌ای و بین‌المللی می‌باشد؛ که در سطح ملی، این یک مسئولیت مشترک است که مستلزم اقدام هماهنگ در رابطه با پیشگیری، آماده‌سازی و واکنش از سوی مقامات دولتی، بخش خصوصی و جامعه مدنی می‌باشد.

فعالیت اتحادیه بین‌المللی مخابرات در حوزه امنیت توسط قطعنامه ۵۸ این سازمان با عنوان «ایجاد تیم‌های امداد و نجات رایانه‌ای به خصوص برای کشورهای درحال توسعه و همکاری بین این تیم‌ها» و قطعنامه ۱۳۰ در سال ۲۰۱۰ پشتیبانی می‌گردد. در این چارچوب، برنامه جهانی امنیت سایبری توسط دبیرکل اتحادیه بین‌المللی مخابرات به عنوان چارچوب ارائه شده توسط این اتحادیه برای همکاری‌های بین‌المللی به منظور ایجاد جامعه اطلاعاتی ایمن و امن‌تر ارائه گردیده است. این برنامه دارای حوزه‌های کاری حقوقی، فنی، سازمانی، ظرفیت‌سازی فنی و همکاری می‌باشد. این پنج حوزه مشخص‌شده پایه نشانگرهای شاخص امنیت سایبری را شکل می‌دهند. این پنج نشانگر برای اندازه‌گیری قابلیت‌های ملی در امنیت سایبری دارای اهمیت هستند؛ زیرا بلوک‌های سازنده فرهنگ ملی در حوزه امنیت سایبری هستند.

اما به دلیل سرعت بسیار بالای پیشرفت این تکنولوژی سازمان‌ها و نهادهای بین‌المللی از جمله اتحادیه بین‌المللی مخابرات نیز باید همپای این سرعت پیشرفت در فضای سایبری گام‌های مستحکمی را بردارند و تنها به تصویب قطعنامه اکتفا ننمایند؛ چنان‌که از سال ۲۰۱۶ تا اکنون قطعنامه‌ای صادر نشده و فقط به ارائه گزارش بسنده شده است و این نشان از عدم اجماع جهانی دولت‌ها بر ایجاد قطعنامه‌ها و ناکارآمد بودن آنها تا به اکنون است و همچنین در زمینهٔ اجرایی نیز تدابیری را بیندیشند و یا در صورت امکان برنامه‌هایی را در جهت سهولت به‌کارگیری و انجام تدابیر اجرایی از سوی تمامی دولت‌ها ایجاد نمایند که در این زمینه نیز عملکرد ضعیفی داشته است.

همچنین تغییر رویکرد اتحادیه از حقوق نرم به سمت حقوق سخت و تدوین کنوانسیونی مستقل در زمینه امنیت سایبری به گونه‌ای که از قدرت الزام‌آوری کافی برخوردار بوده و تمامی کشورها اعم از توسعه یافته یا در حال توسعه بتوانند از آن پیروی نمایند؛ نیز می‌تواند به عنوان یک تدبیر حقوقی در سطح بین‌المللی مطرح گردد.

منابع

- تقی‌زاد، مهرداد. (۱۳۹۵). *سازمان‌های بین‌المللی و قاعده‌مندسازی فضای سایبری*. چاپ اول. انتشارات خرسندی.

- تقی‌زاد، مهرداد؛ زمردی، کیوان؛ حاجیان، مهدی. (۱۳۹۶). نقش اتحادیه اروپا در قاعده‌مندسازی جرایم سایبری. *مطالعات بین‌المللی پلیس*، ۷ (۲۹)، ۱۴۳- ۱۰۴.
http://interpol.jrl.police.ir/article_12920.html

- جباری، منصور؛ تاج‌آبادی، حسین. (۱۳۹۱). تخصیص فرکانس در مدار ثابت زمین در نظام حقوق بین‌الملل فضا. *پژوهش حقوق عمومی*، ۱۴(۳۸)، ۱۱۹- ۱۰۱.
http://qjpl.atu.ac.ir/article_2339.html

- جباری، منصور؛ حاتمی، فاطمه. (۱۳۹۳). نقش اتحادیه بین‌المللی مخابرات در تدوین و توسعه حقوق بین‌الملل فضای ماورای جو. *پژوهش حقوق عمومی*، ۱۵(۴۲)، ۱۷۲- ۱۴۱.
http://qjpl.atu.ac.ir/article_257.html

- راهنمای اصطلاحات و واژه رادیویی (۱۳۸۹). *سازمان تنظیم مقررات و ارتباطات رادیویی*. وزارت ارتباطات و فناوری اطلاعات (بر اساس مفاهیم و تعاریف بین‌المللی ITU). بینش نو.

- رضی‌پور، فریبا؛ گلرو، علی اکبر. (۱۳۸۸). *سازمان‌های بین‌المللی فضایی (گزارش دوم پروژه بررسی و تحلیل اسناد بین‌المللی حقوق فضایی، عملکرد سازمان‌های بین‌المللی فضایی و ارائه راهکارهای مناسب برای جمهوری اسلامی ایران)*. پژوهشگاه هوا- فضا. وزارت علوم، تحقیقات و فناوری.

- علی‌آبادی، گیتا. (بی‌تا). اجلاس جهانی سران درباره جامعه اطلاعاتی. *رسانه*، ۱۴(۴)، ۱۴۵- ۱۴۰.
http://ensani.ir/fa/article/299068

- محسنی، فرید؛ صوفی‌زمرد، محسن. (۱۳۹۶). پلیس و چالش‌های اجرایی تأمین امنیت سایبری. *پژوهش‌های دانش انتظامی*، ۲۰(۴)، ۱۸۸- ۱۶۳.
http://ensani.ir/file/download/article/1537073714-9967-101.pdf

- نامخواه، ناصر. (۱۳۹۰). *امنیت دنیای سایبری کاربران عمومی*. چاپ اول. بی‌نا.

- Brunot, R. (2018). *United Nations Security Council Background Guide*, p.p 1-11. http://www.ccwa.org/wp-content/uploads/2018/09/UNSC-Final.pdf

- Gabrial, P. (2019). Cyber security - a Romanian Perspective in the European Context, *International Journal of Information Security and Cybercrime*, 8(1), 1-4. https://www.ceeol.com/search/article-detail?id=833988

- Gasser, M. (1988). *Bulding a Secure Computer System*, Division of Canada Publishing Corporation.
https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf

- Gercke, M. (2012). *Understanding Cybercrime: Phenomena*, Challenges and Legal Responses, ITU.

- Marion, N. (2010). The Council of Europ`s Cyber Crime Treaty: An exercise in Symbolic Ligislation, *International Journal of Cyber Criminology*, 4(1), 699- 712.
https://books.google.com/books?id=FHSFDwAAQBAJ&pg=PA151&lpg=PA151&dq=Marion,+Nancy,+(2010)

- (FARC-63) Extraordinary Administrative Radio Conference to Allocate Frequency Bnds for Space Radiocommunication Purposes –Space Radiocommunication Conference (Geneva, 1963). Retrieved 2016, Feb,06. From:
http://www.itu.int/en/history/Pages/ListOFITUConferencesAssembliesAndEvents.aspx.Las - t

- Additional Plenipotentiary Conference, (Geneva, 1992). Retrieved 2020, Jan.22. From:
http://www.itu.int/en/history/Peges/ ListOFITUConferencesAssembliesAndEvents,aspx.

- CCIR – Ixth Plenary Assembly (Los Angeles, 1959). Retrieved 2019, Des.11. From: http:// www.itu.int/en /history/ Pages/ Listof ITUConferencesAssembliesAndEvents.aspx.
- Geneva Action plan – Action Line C5 http://groups.itu.int/stocktaking/About/WSISActionLines/C5.Cybersecurity.aspx
- GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY, STRATEGIC ENGAGMENT IN CYBERSECURTIY. From: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

http://www.int/osg/csd/cybersecurity/gca/pillars-goals/index.html
http://www.itu.int/en/history/pages/ITUsHistory.asp.Last Visited at: 24 Dec 2019.
http://www.itu.int/en/ITU-D/Pages/About.aspx.
http://www.itu.int/en/Pages/default.aspx.
http://www.itu.int/inunews/manager/display.asp?lang=en&year=2009&issue=02&ipage
https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf, p.p. 1-21, Last Visited at: 15 Jul 2020
ITU Global Strategic Report www.itu.int/osg/cybersecurity/gca/global-strategic-repot/index.html
Report by the Secretary-General, ITU COUNCIL CONTRIBUTION TO THE 2016 UNITED NATIONS HIGH-LEVEL POLITICAL FORUM ON SUSTAINABLE DEVELOPMENT, Document C16/INF/13, //sustainabledevelopment.un.org/content/documents/10422International%20Telecommunication%20Union%20Council%20.pdf

- The Administrative Radio Conference (Radio Conference), (Geneva, 1959). Retrieved 2020, Feb,06. From: http://www.itu.int/ en/history/Pages/ListOFITUConferences Assemblies andEvents.aspx:1.
- The Plenipotentiary Conference, (Malaga Torremolinos, 1973). Retrieved 2020, Feb,06. From: http://www.itu.int/en/history/ Pages/listOFITUConferencesAssembliesAndEvents.aspx.
- The Plenipotentiary Conference, (Nairobi, 1982). Retrieved 2020, Feb,06. From: http://www.itu.int/en/history/Pagest/ListOFITU ConferencesAssembliesAndEvents.aspx.
- The Plenipotentiary Conference, (Nice, 1989). Retrieved 2020, Feb,06. From: http://witu.int/en/history/Pages/ListOFITU.ConferencesAssembliesAndEvents-
- World Administrative Radio Conference on the Use of the Geostationary – Satellite Orbit and the Planning of the Space Service UTILIZNG IT (1 ST SESSION) (Geneva, 1985). Retrieved 2020, Feb,06. From: http://www.itu. Inten/history/pages/ListOFITUConferencesAssembliesAndEvents,aspx. Last
- World Administrative Radio Conference on the Use of the Geostationary – Satellite Orbit and the Planning of the Space Service UTILIZNG IT (1 ST SESSION) (Geneva, 1988). Retrieved 2020, Feb,06. From: http://www.itu.Into/en/history/pages/ListOFITUConferencesAssembliesAndEvents,aspx.

Resolution

- https://www.itu.int/.../cybersecurity/.../Resolutions/pp-14_Res.%20179.pdf
- https://www.itu.int/dms_pub/itu-t/.../T-RES-T.52-2016-PDF-E.pdf
- https://www.itu.int/en/action/internet/.../Resolution 174 pp14.pdf
- https://www.itu.int/en/ITU-D/Cybersecurity/.../45revDubai.pdf
- https://www.itu.int/en/ITU-T/.../resolutions/Resolution%2058.pdf
- https://www.itu.int/osg/csd/cybersecurity/.../RESOLUTION_181.
- ITU Resolution 130 (Rev.Guadalajara, 2010). pdf
- www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx, see at 30/1/2020
- www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html (10.9.1394)