

تحدید حملات سایبری

در پارچوب قواعد حقوق بین الملل بشر دوستانه

تألیف:

دکتر افشین بعفری

استادیار دانشگاه پیام نور



مجمع علمی و فرهنگی مجد

سرشناسه : جعفری، افشین،
عنوان و نام پدیدآور : تحدید حملات سایبری در چارچوب قواعد حقوق بین الملل بشردوستانه /
تألیف افشین جعفری.

مشخصات نشر : تهران: مجد، ۱۳۹۷.

مشخصات ظاهری : ۳۰۳ ص.

شابک : ۹۷۸-۶۰۰-۱۹۳-۹۸۷-۷

وضعیت فهرست نویسی : فیبا

موضوع : تروریسم رایانه‌ای

موضوع : Cyberterrorism

موضوع : تروریسم رایانه‌ای -- پیشگیری -- همکاری‌های بین‌المللی

موضوع : International cooperation -- Prevention -- Cyberterrorism

موضوع : کامپیوترها -- ایمنی اطلاعات

موضوع : Computer security

موضوع : جرایم کامپیوتری -- پیشگیری

موضوع : Computer crimes -- Prevention

موضوع : حقوق بین‌الملل بشر دوستانه

موضوع : Humanitarian law

رده بندی کنگره : HV ۶۷۷۳/ج۷ت۳: ۹۷

رده بندی دیویی : ۳۶۳/۱

شماره کتابشناسی ملی : ۵۴۷.۶۲۹

هرگونه تکثیر کامل یا قسمتی از کتاب بدون اجازه ناشر مجاز نیست. آلوده، یا ناشر خلاف قانون، شرع و اخلاق است.
موارد تخلف از حقوق ناشر، مجاز نیست. مجید گزارش فرماید.

تحدید حملات سایبری در چارچوب قواعد حقوق بین‌الملل بشردوستانه

تألیف: دکتر افشین جعفری

انتشارات مجد

چاپ اول: ۱۳۹۷ قیمت: ۳۷۰۰۰ تومان

حق چاپ محفوظ و منحصر «مجد» است.

شابک: ۹۷۸-۶۰۰-۱۹۳-۹۸۷-۷

ISBN: 978-600-193-987-7

دفتر مرکزی مجد:

تهران، میدان انقلاب، تقاطع خیابان منیری جاوید و شهدای ژاندارمری، پلاک ۵۷

تلفن و دورنگار: ۶۶۴۹۵۰۳۴ - ۶۶۴۱۲۰۷۸ - ۶۶۹۶۳۳۸۶

فروشگاه مرکزی: تقاطع خیابان منیری جاوید و شهدای ژاندارمری، پلاک ۵۹

تلفن: ۶۶۴۰۹۴۲۲ - ۶۶۴۸۶۸۷۴

www.majdlaw.com

E-mail: info@majdlaw.com

کانال رسمی انتشارات مجد در تلگرام: @majdlaw

فهرست مطالب

مقدمه	۱۳
بخش اول: کلیات	۱۵
فصل اول: شبکه‌های رایانه‌ای و فضای سایبر: مفاهیم، ساختار و ویژگی‌ها	۱۷
گفتار اول: مفاهیم مقدماتی شبکه	۱۷
گفتار دوم: مفاهیم مقدماتی فضای سایبر	۱۸
مبحث اول: تاریخچه	۱۸
مبحث دوم: مفهوم فضای سایبر	۲۰
مبحث سوم: ساختار و کارکرد فضای سایبر	۲۱
بند اول: ویژگی‌های فضای سایبر	۲۲
بند دوم: نقش فضای سایبر	۲۳
فصل دوم: حملات سایبری	۲۶
گفتار اول: مفاهیم و مصادیق	۲۶
مبحث اول: مفاهیم مقدماتی	۲۶
بند اول: تعریف حمله سایبری	۲۶
الف- تعریف مقدماتی	۲۷
ب- تعاریف ارائه شده از حمله سایبری در رصه بین‌المللی	۲۹
۱- مفهوم حمله سایبری	۲۹
۲- ارائه تعریف حمله سایبری توسط برخی نهادهای دولتی	۳۰
۳- تعریف پیشنهادی	۳۳
بند دوم: قیاس با حملات مرسوم سنتی و جنگ سایبری	۳۵
الف- مقایسه با حملات سنتی	۳۶
ب- تفاوت حمله سایبری با جنگ سایبری	۳۷
بند سوم: تاریخچه و سوابق حمله سایبری	۳۹
الف- تاریخچه	۳۹
ب- نمونه‌هایی از حملات انجام شده	۴۰
مبحث دوم: انواع عملیات سایبری	۴۲
بند اول: بهره‌برداری سایبری: CNE	۴۳
بند دوم: تروریسم سایبری	۴۳
بند سوم: جاسوسی سایبری	۴۴
بند چهارم: حملات سایبری با هدف تخریب: CNA	۴۵

- ۴۵..... الف- حملات از نوع DoS
- ۴۶..... ب- حملات از نوع DDOS
- ۴۶..... ج- حملات از نوع Back door
- ۴۷..... مبحث سوم: قلمرو حمله
- ۴۸..... گفتار دوم: اوصاف حقوقی حمله سایبری
- ۴۸..... مبحث اول: حملات سایبری از منظر حقوق بین‌الملل
- ۴۹..... بند اول: اصول حقوقی بین‌المللی مرتبط با حملات سایبری
- ۴۹..... الف- مفهوم اصل در اسناد بین‌المللی
- ۵۰..... ب- برخی از اصول مرتبط
- ۵۰..... ۱- اصل منع توسل به زور یا تهدید به آن
- ۵۰..... ۲- اصل حل و فصل مسالمت آمیز اختلافات بین‌المللی
- ۵۱..... ۳- اصل عدم مداخله در امور داخلی
- ۵۱..... ۴- اصل برابری بین‌المللی
- ۵۲..... ۵- اصل برابری حاکمیت دولتها
- ۵۲..... ۶- اصل تأیید اجتناب از کشورها
- ۵۳..... بند دوم: حوزه‌های تأثیر از حملات سایبری در حقوق بین‌الملل
- ۵۳..... الف- تأثیر بر حقوق مشخصات و مکان
- ۵۴..... ۱- حمله سایبری به مثابه نقض حقوق توسل به زور
- ۵۵..... ۲- چالش بین حملات سایبری و حقوق بین‌الملل بشردوستانه
- ۵۵..... ب- حقوق دریاهای و حملات سایبری
- ۵۶..... ج- حقوق معاهدات بین‌المللی و حملات سایبری
- ۵۷..... د- حملات سایبری و حقوق هوا و فضا
- ۵۷..... و- تأثیر بر حقوق مسئولیت بین‌المللی دولت
- ۵۸..... ه- تأثیر بر حقوق ارتباطات و اطلاعات
- ۵۸..... مبحث دوم: حملات سایبری از منظر حقوق مشخصات مسلحانه
- بند اول: جایگاه توسل به زور و حمله مسلحانه در حقوق بین‌الملل قراردادی و عرفی
- ۵۹..... الف- مفهوم زور
- ۶۰..... ب- شیوه‌های کاربرد زور
- بند دوم: حمله سایبری به مثابه حمله مسلحانه در حقوق بین‌الملل قراردادی و عرفی
- ۶۴..... الف- جایگاه حمله سایبری به عنوان حمله مسلحانه در اسناد بین‌المللی
- ۷۰..... ب- رویه دولتها، رویه قضایی و عرف آتی

موضوعی، شخصی و زمانی.....	۷۷
الف- معیارهای ارزیابی ابزارهای حملات سایبری به عنوان توسل به زور	
مسلحانه.....	۷۹
۱- تحدید حمله سایبری به ابزارهای نظامی کلاسیک.....	۷۹
۲- معیار نتیجه محور.....	۸۰
۳- ویژگی‌های "زور مسلحانه" به عنوان سنگ محک.....	۸۱
ب- مشکل اصل صلاحیت شخصی در انتساب.....	۸۳
۱- حملات غیرمستقیم.....	۸۳
۲- حملات تروریستی انفعالی.....	۸۵
۳- شناسایی مبدأ حملات به صورت کلی.....	۸۵
ج- احمال اصل صلاحیت زمانی در دفاع مشروع.....	۸۶
۱- دفاع مشروع پیش‌دستانه.....	۸۷
۲- دفاع مشروع پیش‌گیرانه.....	۸۷
د- مشکلات رمزبندی پارادایم کلاسیک.....	۸۸
مبحث سوم: تحول مفاهیم حقوقی صدمات مسلحانه در پرتو حملات سایبری.....	۸۹
بند اول: مفهوم رزمنده و غیر رزمنده.....	۸۹
الف- تعریف رزمنده طبق حقوق صدمات مسلحانه.....	۸۹
ب- تحول مفهوم رزمنده در حملات سایبری.....	۹۱
۱- رزمنده قانونی.....	۹۱
۲- سربازان سایبری غیر قانونی یا مزدور.....	۹۲
بند دوم: مشارکت مستقیم.....	۹۳
الف- مفهوم مشارکت مستقیم.....	۹۴
ب- تحول مفهوم مشارکت مستقیم در حملات سایبری.....	۹۴
بند سوم: اهداف نظامی، غیرنظامی و دوگانه.....	۹۵
الف- اهداف نظامی.....	۹۶
۱- مفهوم اهداف نظامی.....	۹۶
۲- تحول مفهوم اهداف نظامی در حملات سایبری.....	۹۷
ب- اهداف غیرنظامی.....	۹۸
۱- مفهوم اهداف غیرنظامی.....	۹۸
۲- اهداف غیرنظامی و تحول این مفهوم در حملات سایبری.....	۱۰۰
ج- اهداف دو گانه.....	۱۰۱
بند چهارم: تحول مفهوم حمله.....	۱۰۲

الف- تعریف حمله	۱۰۲.....
ب- تفاوت حمله‌ی سایبری با حمله‌ی نظامی	۱۰۳.....
مبحث چهارم: مکانیزم مقابله با حملات سایبری در نظام حقوقی داخلی و فراملی	۱۰۴.....
بند اول: واکنش نظام حقوقی داخلی	۱۰۴.....
الف- واکنش کشور قربانی	۱۰۵.....
۱- معیارهای دفاع مشروع از منظر منشور ملل متحد	۱۰۵.....
۲- حق دفاع مشروع در حملات سایبری	۱۰۶.....
ب- رویکرد و مکانیزم حقوق داخلی کشورها	۱۰۹.....
۱- رویکرد دکترین امنیت ملی به حملات سایبری	۱۰۹.....
۲- دکترین دفاع پیش‌دستانه در حملات سایبری	۱۱۶.....
۳- آخرین بازدارندگی سایبری	۱۱۹.....
بند دوم: واکنش نظام حقوقی فراملی	۱۲۱.....
الف- واکنش شورای امنیت	۱۲۲.....
۱- مفهوم آسوز - نقض صلح	۱۲۳.....
۲- احراز وضعیت راءال صلاحیت	۱۲۴.....
ب- مکانیزم حقوقی فراملی	۱۲۶.....
۱- مکانیزم منطقه ای	۱۲۶.....
۲- اتحادهای نظامی	۱۲۹.....
۳- نقش سازمان‌های بین‌المللی در مقابله با حملات سایبری	۱۳۳.....
نتیجه	۱۴۲.....

بخش دوم: حملات سایبری از منظر حقوق بین‌الملل بشردوستانه و پیامدهای

نقض آن	۱۴۷.....
فصل اول: رویکرد حقوق بین‌الملل بشردوستانه در مواجهه با حملات سایبری	۱۵۰.....
گفتار اول: درآمدی اجمالی بر روند شکل‌گیری اصول و قواعد حقوق بین‌الملل بشردوستانه	۱۵۰.....
مبحث اول: روند شکل‌گیری	۱۵۱.....
بند اول: حقوق لاهه	۱۵۲.....
بند دوم: حقوق ژنو	۱۵۳.....
بند سوم: منابع حقوق بین‌الملل بشردوستانه	۱۵۴.....
مبحث دوم: قابلیت اعمال حقوق بین‌الملل بشردوستانه	۱۵۷.....
بند اول: تخریب و مالیت داده‌های رایانه‌ای	۱۵۷.....

الف- مبنای حقوقی مالیت داده‌های رایانه‌ای	۱۵۸.....
ب- رویکرد حقوق بین‌الملل بشردوستانه در مواجهه با تخریب داده‌های رایانه‌ای	۱۵۹.....
بند دوم: جایگاه حملات سایبری در حوزه حقوق بین‌الملل بشردوستانه	۱۶۲.....
الف- قلمرو حاکمیت قواعد	۱۶۳.....
۱- دیدگاه مخالفین	۱۶۴.....
۲- دیدگاه موافقین	۱۶۵.....
ب- حملات سایبری از منظر حقوق بین‌الملل بشردوستانه	۱۶۶.....
گفتار دوم: معیارهای حقوق بین‌الملل بشردوستانه در مقابله با حملات سایبری	۱۶۹.....
مبحث اول: تعامل حملات سایبری با موجودیت‌های حقوق بین‌الملل بشردوستانه	۱۶۹.....
بند اول: وجودیت‌های حقوق بین‌الملل بشردوستانه	۱۶۹.....
الف- موجودیت‌های نظامی	۱۷۰.....
۱- رزمندگان	۱۷۰.....
۲- اهداف نظامی	۱۷۱.....
ب- غیرنظامیان و اموال غیرنظامی	۱۷۴.....
ج- اهداف دوگانه	۱۷۷.....
بند دوم: موجودیت‌های برخوردار از حمایت ویژه	۱۷۸.....
الف- تأسیسات حاوی نیروهای خطرناک	۱۷۹.....
ب- اموال ضروری برای بقای سکنه غیرنظامی	۱۸۰.....
ج- محیط زیست طبیعی	۱۸۲.....
د- اموال بهداری	۱۸۲.....
و- اموال فرهنگی	۱۸۳.....
ه- اقدامات تلافی‌جویانه علیه این اهداف	۱۸۴.....
مبحث دوم: اعمال محدودیت‌های حقوق بین‌الملل بشردوستانه در حملات سایبری	۱۸۶.....
بند اول: قاعده ضرورت نظامی	۱۸۷.....
بند دوم: اصل احترام به کرامت انسانی و رفتار انسانی (منع رنج غیرضرور)	۱۸۷.....
بند سوم: اصل تمایز	۱۸۸.....
الف- رایانه‌ها به عنوان سلاح‌های عدم تبعیض	۱۸۸.....
ب- اصل تمایز در حملات سایبری	۱۹۰.....
بند چهارم: اصل تناسب	۱۹۲.....
ب- کاهش صدمات جانبی؛ هدف نهایی اصل تناسب	۱۹۵.....

- ج- نيزنگ‌ها و ترفندهای جنگی..... ۱۹۶
- بند پنجم: اصل بی‌طرفی..... ۱۹۸
- الف- مفهوم بی‌طرفی..... ۱۹۸
- ب- حق بی‌طرفی در حملات سايبری..... ۱۹۹
- مبحث سوم: حقوق بين الملل بشردوستانه؛ مبنای تحديد حملات سايبری..... ۲۰۲
- بند اول: ابزار حملات سايبری به مثابه سلاحی نوین..... ۲۰۲
- الف- مفهوم سلاح سايبری..... ۲۰۳
- ب- قابلیت اعمال کنوانسیون تجارت اسلحه از منظر حقوق بين الملل
- بشردوستانه..... ۲۰۶
- ج- تعامل بين حقوق بين الملل بشردوستانه و حقوق حاکم بر حملات
- سايبری..... ۲۰۷
- بند دوم: معیار تشخیص حملات سايبری به عنوان جنگ نامتقارن از منظر
- حقوق بين الملل بشردوستانه..... ۲۰۹
- الف- مفهوم جنگ نامتقارن..... ۲۰۹
- ب- ویژگیهای جنگ نامتقارن در قالب یک حمله سايبری..... ۲۱۱
- بند سوم: معیار تشخیص حملات سايبری به عنوان جنگ نیابتی از منظر
- حقوق بين الملل بشردوستانه..... ۲۱۱
- الف- مفهوم جنگ نیابتی..... ۲۱۱
- ب- ویژگیهای جنگ نیابتی در قالب یک حمله سايبری..... ۲۱۲
- بند چهارم: فایده اعمال حقوق بين الملل بشردوستانه در حملات سايبری:
- قواعدی ذو وجهتین..... ۲۱۲
- فصل دوم: پیامدهای نقض حقوق بين الملل بشردوستانه در حملات سايبری..... ۲۱۵
- گفتار اول: امکان طرح مسئولیت دولتها و افراد..... ۲۱۵
- مبحث اول: مسئولیت و تعهد دولتها..... ۲۱۶
- بند اول: قواعد کلی مربوط به مسئولیت بين المللی دولت..... ۲۱۶
- الف: مفهوم مسئولیت بين المللی و قواعد حاکم بر آن..... ۲۱۶
- ۱- مفهوم مسئولیت بين المللی..... ۲۱۶
- ۲- تدوین قواعد حاکم بر مسئولیت بين المللی دولت..... ۲۱۷
- بند دوم: اعمال قواعد مسئولیت بين المللی دولت در حملات سايبری..... ۲۲۳
- الف- مسئولیت دولت مرتکب..... ۲۲۴
- ۱- مبنای مسئولیت دولت حاکم..... ۲۲۴
- ۲- نقض کنوانسیونهای چهارگانه ژنو در حملات سايبری..... ۲۲۹
- ۳- قابلیت انتساب حمله سايبری به دولت..... ۲۳۱

۲۳۹.....	ب- مسئولیت دولت‌های ثالث در حملات سایبری
۲۴۰.....	۱- مسئولیت دولت ثالث به مثابه معاونت
۲۴۲.....	۲- چگونگی تحقق مسئولیت دولت ثالث در حملات سایبری
۲۵۴.....	مبحث دوم: مسئولیت و تعهد افراد
۲۵۴.....	بند اول: مسئولیت کیفری فردی ناشی از نقض حقوق بین‌الملل بشردوستانه
۲۵۶.....	بند دوم: تحول مفهوم مسئولیت کیفری فردی در حملات سایبری
۲۵۷.....	گفتار دوم: جبران خسارت ناشی از نقض
۲۵۸.....	مبحث اول: جبران خسارت
۲۵۹.....	بند اول: شیوه‌های جبران خسارت
۲۵۹.....	الف- اعاده وضع سابق
۲۶۰.....	ب- پرداخت غرامت
۲۶۲.....	ج- جبران رضایت
۲۶۲.....	د- وقف و عدم تکرار
۲۶۳.....	بند دوم: مالیه جبران خسارت
۲۶۳.....	الف- دولت در برابر دولت
۲۶۴.....	ب- افراد در مقابل دولت
۲۶۶.....	مبحث دوم: مکانیزم حل اختلافات
۲۶۶.....	بند اول: مکانیزم‌های قضایی و شبه قضایی ملی
۲۶۷.....	بند دوم: نهادها و مکانیزم‌های قضایی و شبه قضایی فراملی
۲۶۸.....	بند سوم: مکانیزم‌های مبنی بر کمیسیون و دادگاه‌های منطقه‌ای
۲۶۸.....	بند چهارم: نهادهای قضایی و شبه قضایی بین‌المللی
۲۶۹.....	بند پنجم: شیوه اعمال صلاحیت دولت‌ها در رسیدگی به جرائم فضای سایبر
۲۷۴.....	نتیجه فصل
۲۷۷.....	نتیجه نهایی
۲۸۶.....	منابع

مقدمه

در قرن اخیر سعی گردیده است که از یک طرف توسل به زور برای حل و فصل اختلافات بین‌المللی مقید و قاعده‌مند گردد (JUS AD BELLUM) و از طرف دیگر در صورت وقوع مخاصمات مسلحانه، محدودیت‌های عینی و سنجش‌پذیری در قالب حقوق بین‌الملل بشردوستانه اعمال گردد (JUS IN BELLO).

در این فرایند اصول و قواعدی طراحی گردیده‌اند که از یک سو ناظر بر ممنوعیت توسل به زور به طور کلی است و از سوی دیگر در پرتو رویکردهای حقوق بشری ناظر بر روابط انسانی در سطوح داخلی و بین‌المللی در مقام اعمال محدودیت در آیین رزم است. این فرایند در طول قرن گذشته تداوم داشته است اما با ورود به هزاره سوم میلادی، تحولات بسیار سریع و مخف‌آوری در همه شئون زندگی نمایان گردیده که بی‌تردید فناوری اطلاعات یکی از عوامل مهم و عمده‌ی این تحولات بوده است. ویژگی برجسته‌ی این فناوری، تأثیری است که بر تکامل ارتباطات راه دور گذاشته است. این تکامل نه‌تنها برای انسان‌ها، بلکه میان انسان‌ها و رایانه‌ها، میان خود رایانه‌ها نیز به وجود آمده است. در نتیجه‌ی این تحولات، جامعه‌ای مجزا با آثار واقعی پدید آمده است. در راستای این تحولات یکی از مسائل جدید که امروزه در روزه حقوق بین‌الملل قرار گرفته، موارد حقوقی مرتبط با فضای سایبر می‌باشد به خصوص مفاهیمی همچون جنگ سایبری، حمله سایبری و یا حتی جرایم سایبری که بعضاً در نوشته‌های حقوقی خلط بحث می‌شوند درحالی که این نوع عملیات از نظر حقوقی با یکدیگ تفاوت دارند.

با توجه به روند رو به رشد حملات سایبری و نقض نفوذ بین‌الملل بشردوستانه در خلال این حملات و از آنجایی که احتمال گسترده شدن این گونه حملات سایبری وجود دارد لذا در بررسی چارچوب حقوقی حملات سایبری بایستی اصول و قواعد حقوق مخاصمات مسلحانه اعم از Jus ad bellum و Jus in bello را نیز مدنظر قرار دهیم.

با توجه به دامنه گسترده‌ای که حمله سایبری دارد در برخی موارد شاید گستره آسیب‌های این گونه حملات چه از لحاظ کمی و چه از لحاظ کیفی چه بسا بسیار بیشتر از حملات متعارف و کلاسیک باشد. بنابراین یکی از نکات بسیار مهم در این نوشتار این است که دیدگاه برخی از دولت‌ها در مواجهه با حملات سایبری در چارچوب حقوق توسل به زور بررسی گردد.

لذا به دلیل ضرورت بررسی جامع مسائل مرتبط با حملات سایبری و به خصوص تبعات آن و بالطبع مواردی همچون رعایت اصول و مقررات حقوق بین‌الملل بشردوستانه

در این گونه حملات و آثار حقوقی آن، در این نوشتار سعی بر آن می‌گردد تا موازین حقوق بین‌الملل بشردوستانه و رعایت آن در پرتو اصول بنیادین حقوق بین‌الملل در حملات سایبری بررسی گردد و از آنجایی که اساس و پایه تمام این مسائل فناوری اطلاعات و فضای سایبر می‌باشد لذا بررسی این مفاهیم و تعیین "مالیت داده‌های رایانه‌ای" از آن جهت که تخریب این داده‌ها در چارچوب تعریف "تخریب فیزیکی" مطابق با قواعد حقوق مخاصمات مسلحانه و حقوق بین‌الملل بشردوستانه قرار می‌گیرد یا خیر، نیز یکی دیگر از ارکان این تحقیق می‌باشد.

با رعایت به مطالب مطرح شده و با توجه به افزایش روز افزون حملات سایبری طی سال‌های اخیر، در نتیجه احتمال افزایش میزان تلفات و قربانیان این نوع حملات و تهدید صلح و امنیت بین‌المللی، آرمان این نوشتار بررسی این نکته است که طرفین درگیر در چنین حملاتی (به خصوص مهاجم)، تعهدات و التزاماتی را در رعایت مقررات بشردوستانه حاکم بر این نوع حملات و در راستای حمایت از غیرنظامیان و دیگر افراد و اموال تحت حمایت قرار دارند، نمایان با توجه به ویژگی حملات سایبری، دامنه این تعهد و التزام به رعایت قواعد بشردوستانه شامل دولت‌های ثالث نیز خواهد بود. همچنین با بررسی آراء دیوان بین‌المللی داد و ستد، ر قضیه نیکاراگوئه و بوسنی و نیز آراء دیوان بین‌المللی کیفری برای یوگسلاوی سابق، در قضیه تادیچ و نیز طرح پیش‌نویس مسئولیت بین‌المللی دولت‌ها مصوب ۲۰۰۱، به این نکته پی می‌آوریم که دولت‌های ثالث هم از بابت نقض حقوق بین‌الملل بشردوستانه ارتكابی طی این گونه حملات ممکن است مستقیم یا غیرمستقیم مسئول شناخته شوند. بنابراین اولین سئوال که به ذهن هر حقوقدانی می‌رسد این است که اصول بنیادین حقوق بین‌الملل بشردوستانه در مواجهه با حملات سایبری چگونه قابل اعمال بوده و آثار حقوقی نقض حقوق بین‌الملل بشردوستانه در حملات سایبری چیست؟

با توجه به اینکه ممکن است برخی حملات سایبری در طول مخاصمات مسلحانه و برخی دیگر در زمان صلح انجام گردد، لذا مسائل مطروحه فوق در دو مقطع؛ زمان صلح و زمان مخاصمه؛ قابل ارائه و ارزیابی می‌باشند.

در خاتمه از جناب آقای "سید عباس حسینی نیک" که انصافاً خدمات شایسته و مثمر ثمری به جامعه‌ی حقوقی کشور عزیزمان ایران عرضه داشته‌اند نهایت امتنان و تشکر را دارم و از درگاه حضرت حق موفقیت روزافزون ایشان را جهت تداوم خدمات علمی و حقوقی خواستارم.