حفاظت از غیرنظامیان در برابر تهدیدات دیجیتالی و دیپلماسی سایبری بشردوستانه صلیب سرخ در اتحادیه اروپا

از آنجایی که فناوری‌های دیجیتال در درگیری‌های مسلحانه معاصر در کانون توجه قرار دارند ، جمعیت صلیب سرخ بلژیک و هیاتی که در بروکسل تشکیل شده است و رهبری آن با کمیته بین‌المللی صلیب سرخ (ICRC) و شرکای کلیدی اتحادیه ی اروپاست ، سعی دارند تا ازغیرنظامیان در برابر تهدیدات دیجیتال حمایت کنند

افزایش عملیات سایبری و اطلاعاتی در درگیری های مسلحانه چیز جدیدی نیست .با این حال، استفاده از ابزارهای دیجیتال در جنگ چالش‌های فزاینده‌ای را به همراه دارد، از جمله خطر اختلال در خدمات ضروری مانند تجهیزات پزشکی، برق، آب و بهداشت .صلیب سرخ به عنوان مسئول و حافظ حقوق بین الملل بشردوستانه IHL ، از تخصص خود برای ارتقاء حفاظت از غیرنظامیان در برابر تهدیدات دیجیتال استفاده می کند.

در 17ژانویه ۲۰۲۴، بلژیک به عنوان رئیس شورای اتحادیه اروپا (EU) و سرویس اقدام خارجی اروپا (EEAS) میزبان نشستی بود که سفیران و فرماندهان سایبری اتحادیه اروپا را گرد هم آورد.

گرد هم آوردن کشورها، سازمان‌های بشردوستانه و کارشناسان یکی از توصیه‌های کلیدی هیئت مشورتی جهانی صلیب سرخ در مورد حفاظت از غیرنظامیان در برابر تهدیدات دیجیتال در درگیری‌های مسلحانه است . کمیته بین المللی صلیب سرخ از علاقه بلژیک و EEAS استقبال می کند و آنها را تشویق می کند که به توسعه این عملکرد مطالبه گرانه و مدافعه گرانه در بستر حقوق بین الملل بشردوستانه IHL و اختصاصا در بحث های سایبری ادامه دهند.

افزایش مشارکت غیرنظامیان در عملیات دیجیتال

در طول این بحث، تیلمان رودنهاوزر، کارشناس حقوقی کمیته بین‌المللی صلیب سرخ در زمینه سایبری، به نگرانی‌ها و توصیه‌های مربوط به مشارکت فزاینده غیرنظامی در میدان نبرد دیجیتالی پرداخت .وی گفت این روند خطرناک خطرات متعددی را به همراه دارد، زیرا اصل تمایز و افتراق را مخدوش می کند. این اصل یک اصل مهم و زیر بنایی حقوق بین الملل حقوق بشر است و مستلزم وجود یک خط مشخص بین غیرنظامیان و نظامیان دخیل در جنگ است.

هکریست ها، متخصصان امنیت سایبری و هکرهایی که عملیات سایبری را در درگیری های مسلحانه جاری انجام می دهند باید از محدودیت های قانونی بین المللی، از جمله محدودیت های تحمیل شده توسط نظام حقوق بین الملل بشردوستانه یا IHL پیروی کنند.

فرض کنید یک فرد غیرنظامی که در حال انجام یک عملیات سایبری ست واحتمالاً قبلاً نام IHL را نشنیده و در مورد تعهدات خود و خطراتی که با آن روبروست هیچ پیش زمینه ذهنی ندارد تا چه حد میتواند از منظر حقوقی آسیب پذیر و مسئول اتفاقاتی که رخ میدهد باشد .

غیرنظامیانی که به هر نحو فعالانه در خصومت ها شرکت می کنند، حتی از طریق عملیات دیجیتال و بخصوص در درگیری های مسلحانه، ملزم به رعایت مفاد حقوق بین الملل حقوق بشر هستند و باید از هدف قرار دادن اشیاء غیرنظامی یا ایجاد اختلال در خدمات ضروری مانند بیمارستان ها و بانک ها خودداری کنند.

آنها زمانی که به هر نحو در سیستم سایبری در خصومت ها و جنگ ها شرکت می کنند ، خطر از دست دادن حفاظت خود را در برابر حملات نظامی را به جان میخرند و به طور موقت به اهداف قانونی در جنگ تبدیل می

شوند که نمیتوان از آنان دفاع بشردوستانه کرد .این مساله همچنین خطر آسیب احتمالی را برای افراد غیرنظامی و اشیاء غیرنظامی بی گناه و بی دفاع که در نزدیکی افراد شرکت کننده در خصومت هستند را افزایش می دهد.

راه هایی برای کاهش آسیب

هشت قانون طلایی برای هکرها:

در پاسخ به افزایش فعالیت‌های هکرهای غیرنظامی در درگیری‌های مسلحانه، کمیته بین‌المللی صلیب سرخ **"هشت قانون برای هکرهای غیرنظامی در طول جنگ"** و چهار تعهد برای دولت‌ها برای مهار آنها را در اکتبر ۲۰۲۳ منتشر کرد. این ابتکار براساس قوانین موجود IHL ، بر افتراق و جداکردن و بر حفاظت ویژه ای که IHLبرای پرسنل و امکانات پزشکی و پرسنل و اشیاء بشردوستانه که اشیاء ضروری برای بقای جمعیت غیرنظامی است ، دوری کردن از نیروهای بالقوه خطرناک که میتوانند هدف جنگی باشند ، و ممنوعیت گسترش وحشت در بین مردم غیرنظامی یا تحریک برای نقض حقوق بین الملل بشردوستانه و حقوق بشرتاکید می کند، تاکید می کندو در نهایت، قاعده ی مهم عدم عمل متقابل غیر نظامیان را مطابق با حقوق بین الملل بشردوستانه و حقوق بشر یادآور می شود.

قوانین هشت گانه :

۱- حملات سایبری را علیه اشیاء غیرنظامی هدایت نکنید.

اشیاء غیر نظامی همه اشیایی هستند که اهداف نظامی نیستند .این شامل زیرساخت‌های غیرنظامی، خدمات عمومی، شرکت‌ها، اموال خصوصی و داده‌های غیرنظامی است" .اهداف نظامی" اساساً شامل زیرساخت فیزیکی و دیجیتالی ارتش یک طرف متخاصم است .بسته به اینکه چگونه توسط ارتش مورد استفاده قرار می گیرند، چرا که ممکن است شامل اشیاء غیرنظامی نیز باشند.

۲- از بدافزارها یا سایر ابزارها یا تکنیک هایی که به طور خودکار پخش می شوند و به اهداف نظامی و اشیاء غیرنظامی آسیب می رسانند استفاده نکنید.

به عنوان مثال، بدافزارهایی که به طور خودکار منتشر می شوند، و بدون تمایز به اهداف نظامی و غیرنظامی آسیب می رسانند، نباید استفاده شوند.

۳- هنگام برنامه ریزی یک حمله سایبری علیه یک هدف نظامی، هر کاری که ممکن است انجام دهید تا از اثراتی که عملیات شما ممکن است بر غیرنظامیان داشته باشد اجتناب کنید یا به حداقل برسانید.

برای مثال، اگر قصد دارید برق یا خدمات راه آهن مورد استفاده نیروهای نظامی را مختل کنید، باید از اثراتی که ممکن است عملیات شما بر غیرنظامیان داشته باشد اجتناب کنید یا آن را به حداقل برسانید .تحقیق و درک اثرات یک عملیات از جمله موارد ناخواسته ، قبل از انجام آن ضروری است .هنگام برنامه ریزی یک حمله سایبری علیه یک هدف نظامی، هر کاری ممکن است انجام دهید تا از اثراتی که عملیات شما ممکن است بر غیرنظامیان داشته باشد اجتناب کنید یا آن را به حداقل برسانید، و اگر خطر آسیب به غیرنظامیان بیش از حد باشد، حمله را متوقف کنید. اگر به یک سیستم عامل دسترسی پیدا کرده اید اما عواقب احتمالی عملیات خود را درک نمی کنید، یا متوجه شدید که آسیب به غیرنظامیان بیش از حد ممکن است، حمله را متوقف کنید.

۴- هیچ گونه عملیات سایبری علیه تاسیسات پزشکی و بشردوستانه انجام ندهید .

بیمارستان ها یا سازمان های امداد بشردوستانه هرگز نباید هدف قرار گیرند.

۵- .هیچ گونه حمله سایبری علیه اشیایی که برای بقای مردم ضروری است یا می تواند نیروهای خطرناک را آزاد کند، انجام ندهید.

در حقوق بین‌الملل بشردوستانه، از اشیاء حاوی نیروهای خطرناک نام برده شده که شامل : سدها، دایک‌ها و ایستگاه‌های تولید برق هسته‌ای هستند . در ضمن سلاح ها و مواد شیمیایی و مشابه آن نیز حاوی مواد خطرناکی برای گیاهان ، درختان میوه ، گندم زارها و در کل برای مزارع و دامداری ها هستند . اینها اشیایی هستند که برای بقای مردم غیرنظامی ضروری اند . تاسیسات آب آشامیدنی یا سیستم های آبیاری را هدف قرار ندهید .

۶- برای گسترش وحشت در میان مردم غیرنظامی تهدید به خشونت نکنید.

به عنوان مثال، هک کردن سیستم های ارتباطی برای انتشار اطلاعاتی که در درجه اول برای گسترش وحشت در میان مردم غیرنظامی طراحی شده اند، ممنوع است .به همین ترتیب، طراحی و انتشار محتوای گرافیکی برای گسترش وحشت در بین غیرنظامیان به منظور فرار و آوارگی آنها، غیرقانونی است.

۷- نقض قوانین بین المللی بشردوستانه را تحریک نکنید.

دیگران به انجام عملیات سایبری یا دیگر عملیات علیه غیرنظامیان یا اشیاء غیرنظامی تشویق نکنید .برای مثال، جزئیات فنی را در فضای مجازی برای تسهیل حملات علیه نهادهای غیرنظامی به اشتراک نگذارید.

۸- این قوانین را رعایت کنید حتی اگر دشمن رعایت نکند.

انتقام یا اقدام متقابل هیچ بهانه ای برای نقض قوانین بین المللی بشردوستانه نیست.

واکنش‌های هکرهای غیرنظامی به این کار متفاوت بوده است اما خوشبختانه به‌تازگی نشانه‌های مثبتی از سوی گروهی منتشر شد که اعلام کردند در عملیات اخیر به قوانین مذکور پای بند هستند.

توصیه ها

هیئت مشورتی جهانی کمیته بین‌المللی صلیب سرخ ، در مورد تهدیدات دیجیتال در طول درگیری‌های مسلحانه، ۲۵ توصیه مهم را به گروه ها یا کشورهای متخاصم، دولت‌ها، سازمان‌های بشردوستانه و شرکت‌های فناوری ارائه و برآنها تاکید کرد تا از غیرنظامیان در برابر تهدیدات دیجیتال محافظت کنند.

هنگامی که صحبت از مشارکت غیرنظامیان در عملیات دیجیتالی می شود، کمیته بین المللی صلیب سرخ در جریان اجماع و مشورت با رهبران کشورها در سطوح بالا و کارشناسان حقوقی، فنی، سیاست گذاری و امنیتی آنها تلاش میکند تا آنها را قانع کندکه غیرنظامیان به هیچ وجه نباید به مشارکت مستقیم در خصومت ها از طریق

ابزارهای دیجیتال تشویق شوند .هشدارهای واضح باید به غیرنظامیان دخیل در اقدامات سایبری در مخاصمات داده شود که خطر از دست دادن حفاظت و امنیت شان وجود دارد و احتمال حمله به آنها مانند نظامیان هست و کمیته هم نمیتواند از آنها مدافعه کند.

هیئت مشورتی جهانی کمیته بین‌المللی صلیب سرخ با تکیه بر تعهد مشترک همه کشورها برای احترام به حقوق بین الملل بشردوستانه وحقوق بشر، توصیه می کند که آگاهی از قوانین حقوقی نه تنها برای افراد غیرنظامی بلکه به طور مشخص برای شرکت های فناوری دیجیتال باید افزایش یابد .علاوه بر این، توصیه می‌شود خدمات شرکت‌های فناوری در حال توسعه شرکت ها و افراد دخیل در فعالیت های دیجیتال که اهداف بالقوه مضردارند، کنترل شود.

اتحادیه اروپا و کشورهای عضو آن چه کاری می توانند انجام دهند؟

اتحادیه اروپا بسته ی ابزار دیپلماسی سایبری خود را توسعه داده و اخیراً دستورالعمل های اجرایی خود را اصلاح کرده است .این مهم اتحادیه اروپا و ۲۷ کشور عضو آن را به بازیگران مرتبط در بحث‌های جهانی درباره **دیپلماسی سایبری** و هدف کلیدی دیپلماسی بشردوستانه ی صلیب سرخ تبدیل می‌کند .این دیپلماسی مشترک اتحادیه اروپا درمورد فعالیت های سایبری مخرب با هدف جلوگیری از درگیری بیشتر غیر نظامیان ، کاهش تهدیدات امنیت سایبری و تضمین ثبات بیشتر در روابط بین الملل را تا حد زیادی تضمین می کند.

اتحادیه اروپا بر تعهد دولت ها به حمایت مسئولانه از این دیپلماسی در فضای سایبری و اقدامات اعتمادساز منطقه‌ای برای کاهش خطر درگیری‌های ناشی از استفاده از فناوری‌های اطلاعات و ارتباطات تاکید میکند .

فرایند در حال انجام در مورد مسائل سایبری، منطبق با سیاست اتحادیه اروپا، حوزه های حقوقی و دفاعی را در بر می گیرد و این مهم درسیاست دفاع سایبری اخیر اتحادیه اروپا مشخص شده است . قدرت اتحادیه اروپا در متحد کردن ۲۷ کشور عضو است زیرا اینکارمی تواند ظرفیت و ابزار لازم برای احترام و اطمینان از احترام به IHLو محافظت از غیرنظامیان در برابر تهدیدات دیجیتال را فراهم کند.

اتحادیه اروپا در بحث فناوری اطلاعات و ارتباطات و به عنوان مثال در مبحث اقدامات سایبری بشردوستانه در زیر چتر سیاست دفاع سایبری آن اتحادیه ، *برای* اعمال و اجرای قوانین بین المللی، از جمله حقوق بشر و حقوق بین الملل بشردوستانه، ثابت قدم بوده است و با دولت ها درخصوص نظارت بر رعایت قوانین بشردوستانه در فضای مجازی در تعامل نزدیک است.

هیئت مشورتی جهانی کمیته بین‌المللی صلیب سرخ ، تمام کشورها و جمعیت های ملی آنها که عضو فدراسیون بین المللی صلیب سرخ و هلال احمرهستند را موکدا تشویق میکند که در بحث‌های دفاع

سایبری به توسعه ی آموزش حقوق بین الملل بشردوستانه و مدافعه از آن ادامه دهند و به طور خاص توصیه می‌شود با تقویت امنیت سایبری، در برابر اختلالات دیجیتالی، تاب آوری خود را افزایش دهند.

از آنجایی که ابتکارات مختلف اتحادیه اروپا، مانند قانون همبستگی سایبری اتحادیه اروپا و قانون دفاع سایبری در حال انجام است ، کمیته ی بین المللی صلیب سرخ از تمام کشورها می خواهد که قوانین موجود IHL را به درستی برای همگان تبیین و اعمال کنند تا از حفاظت کافی غیرنظامیان، زیرساخت های غیرنظامی و داده های غیرنظامی اطمینان حاصل کنند.

برای کسب اطلاعات بیشتر در مورد چگونگی کاربرد IHL در استفاده از فناوری‌های اطلاعات و ارتباطات مقالاتی منتشر شده است که علاقمندان میتوانند به آنها مراجعه کنند .

آدرس برخی سایت های مرتبط با موضوع :

https://t.co/tmIxqaavLr

https://t.co/ayoh3uT9Xw

pic.twitter.com/LWsYnWJ2zr

https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/?utm_source=twitter&utm_medium=social

۲۶ژانویه ۲۰۲۴

بلژیک