افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــــاد بدین بوم و بر زنده یک تن مــــباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com afgazad@gmail.com

Political	سیاسی

نوشتهٔ: جرمن فارین پالیسی
برگردان از: تحریریه سایت
فرستنده: دپلوم انجنیر نسرین معروفی

۱۰ جولای ۲۰۱۹

نیروهای تهاجمی سایبری

مطابق گزارش نیروهای چند ملیتی شرکت کننده در مانور سالانهٔ ناتو به نام "سپر غیرقابل نفوذ" ، ارتش المان در مسیر درست آماده سازی خود برای به دست گیری رهبری در یک جنگ تمام عیار سایبری در فضای مجازی حرکت می کند.

ارتش المان خود را برای یک جنگ تمام عیار سایبری آماده می کند. موضع گیریهای تا کنونی واحدهای نظامی نشاندهندهٔ این سمت گیری برای ارتش المان می باشند. بر اساس شواهد تا کنونی نیز سربازهای عضو "مرکز عملیات سایبری " (ZCO) مدتها قبل در چهارچوب یک مانور نظامی تمام حملات سایبری ممکن را "برای نفوذ" در شبکه های کامپیوتری کمپانی نظامی سی جی آی (CGI شرکت خدمات کامپیوتری نظامی برای ارتش المان-م) را عملی ساختند. این عملیات که در جریان مانور نظامی اخیر ناتو، که به تازگی تحت عنوان "سپر غیرقابل نفوذ" برگزار شد، از طریق نفوذ یابی و جایگذاری نرم افزارهای بد خیم با هدف تزریق کلر به آب آشامیدنی کشور دشمن فرضی برای مسموم کردن آب شرب مورد نیاز مردم این کشور متخاصم انجام شد. ازاجزای دیگر این مانور "مبارزهٔ" اطلاعاتی با " اخبار دروغین-(فیک نیوز)" پخش شده از جانب "نیروهای متخاصم" در شبکه های اجتماعی بود. واحد نامبردهٔ (ZCO) اساساً برای پیشبرد "عملیات سایبری-تهاجمی" تشکیل شده است. وظیفهٔ این واحد در اختیار گذاشتن مجموعه ای از "امکانات و ابزار اجرائی غیر فعال" در خدمت فرماندهی نظامی- سیاسی کشور در شرایط جنگی می باشد.

هکر های ارتش المان

بنابرادعای ارتش المان، فعالیت میدانی واحد "مرکز عملیات سایبری " (ZCO) در پایان ماه مارچ سال جاری از جانب سربازان این واحد و در طی مانور نظامی ناتو با تمرین حملات سایبری به شبکهٔ داخلی کامپیوتری کمپانی خدمات رسانی نرم و سخت افزاری به ارتش المان - کمپانی نظامی سی جی آی، که مرکز سازمانی اش در شهر لاین فلد-اشتردینگن ایالت بادن ورتمبرگ قرار دارد، شروع شد. در این عملیات تمام زیر و بم و منافذ احتمالی و مجاری ورودی شبکهٔ محافظتی کمپیوتری این شرکت مورد حمله قرار گرفت. در مقابل نیز کارشناسان این شرکت وظیفهٔ دفع این حملات را داشتند. مطابق اطلاعات سایت این شرکت "نیروهای تهاجمی سایبری" همزمان با تلاش در دفع این حملات

سعی کردند، کنترول سرورهای مهاجمان را به دست گرفته و تحلیلی دقیق از ساختارها و زیرپایه های سخت و نرم افزاری مهاجمان به عمل آورده و راه ها و شرایط کنترول سیستمهای مهاجم را مدون کرده و در روند این جنگ سایبری با کلیت "ساختار پیچیدهٔ سخت افزارهای مرتبط"، "سنسورهای مراقبتی مدرن"، "سیستمهای پایه ئی کمپیوتری مختلف" و "سیستمهای فایروال پیشرفته که امروزه تقریباً همه جا رایج می باشند" درگیر شوند. از قرار معلوم هکرهای ارتش در پیشبرد اهداف تعیین شده برای این مانور موفق بوده اند. بنابر گزارش ارتش المان در نتیجهٔ این حملات کمپانی سی جی آی مجبور شد، تمامی سنسورهای تشخیص گر خود را یا تعویض کرده (یا به روز رسانی کند). [۱].

حمله به سیستم تأمین آب آشامیدنی

از جانب دیگر نیز مطابق گزارش نیروهای چند ملیتی شرکت کننده در مانور سالانهٔ ناتو به نام "سپر غیرقابل نفوذ" ، ارتش المان در مسیر درست آماده سازی خود برای به دست گیری رهبری در یک جنگ تمام عیار سایبری در فضای مجازی حرکت می کند. در اپریل امسال واحدهائی از ارتش سایبری المان در"مرکز پیشرفتهٔ همکاری دفاع سایبری" [۱-آ] متعلق به ناتو در شهر تالینین کشور استونی در جریان مانور مربوطه وظیفهٔ پدافندی مقابله با حملات سایبری کشور فرضی "بریلیا" علیه شبکه های کامپیوتری و سیستمهای آی تی" پیمان را به عهده گرفتند. مطابق سناریوی این مانور می بایستی ویروس بدخیمی برای به دست گرفتن کنترول کمپیوتر هائی که وظیفهٔ تنظیم مقدار و دوز مجاز ورودی کلر برای تصفیهٔ آب آشامیدنی در سدها و سایر مراکز مربوطهٔ آبرسانی را به عهده دارند، به دست گرفته و نقشهٔ مسموم کردن آب آشامیدنی مورد مصرف شهروندان غیر نظامی این کشوررا با افزایش دوز سمی کلر در در شبکهٔ آبرسانی را به اجراء درآورند. بنا برگزارش ارتش المان هدف دیگر این حملهٔ سایبری کشور مهاجم که نامش برده نشده است، انجام حملات هکری بر روی شبکهٔ سراسری برق رسانی کشور به منظور قطع برق رسانی در این کشور بوده است. [۲] به گفتهٔ جگرِن بِرند کامِر مایِر فرمانده واحد سایبری ارتش المان، یکی از دیگر اهداف وحشتناک مانور"سپر غیرقابل نفوذ" سناریوئی است، مبنی بر هک کردن یک پهپاد نظامی و به دست گرفتن کنترول هدایت آن توسط یک گروه تروریستی برای حمله به مناطق مسکونی پرجمعیت از طریق سرنگونی هدفمند آن در میان جمعیت. [۳]

مطبوعات به مثابهٔ "سیستمهای تسلیحاتی"

یک بخش لاینفک دیگر مانور"سپر غیرقابل نفوذ" جنگ سایبری استفاده از اخبار جعلی (فیک نیوز) بود. وظیفهٔ تعیین شده برای مهاجمان شرور در سناریوی مذکور پخش و جایگذاری هوشمندانهٔ اطلاعات گمراه کننده (فیک نیوز) در رسانه های اجتماعی و به ویژه در "سایتهای رسمی دولتها و مراکز اداری" بود، که از طریق هک این سایتها کنترول محتویات آنها را عملی سازد. از این طریق مردم کشور باید "احساس ناامنی" کرده و "اعتمادشان به دستگاه دولتی کشورشان" از بین برود.[٤]

برای ارتش المان رسانه های جمعی و مطبوعات مدتهاست که به عنوان "سیستم های تسلیحاتی" مورد طبقه بندی قرار گرفته اند. بازهم بنا بر خبر رسانی فرماندهی اتاق سایبری-اطلاعاتی ارتش، شاغلان ارتش شامل متخصصان فن آوری اطلاعاتی (آی تی) ، محققان و دانشمندان رسانه های جمعی و دانشمندان روانشناسی در این بین افزارهای مناسب و مورد نیاز برای "جمع آوری هدفمند و طبقه بندی شده، رصد ارزیابی از اوضاع در پیرامون فضای رسانه ها و آنهم تحت شرایط میدانی و زنده" را ساخته اند. نتیجهٔ این تلاشها ایجاد یک سیستم الکترونیکی است، که " با جست و جوی

تمام اطلاعات علنی و آزاد در اینترنت همهٔ داده ها را جارو کرده و مورد تجزیه و تحلیل قرار می دهد." در این گزارش همچنین آمده است: " با استفاده از آلگوریتمهای تعریف شده، اطلاعات غلط به طور هدفمند شناسائی شده و سرنخ ارتباطی آن با کاربران معینی، که آنها را پخش می کنند برقرار می شود (سیبل کردن روی فعالان-م) گردد." از آن گذشته و براساس ادعا، ارتش المان اکنون می تواند با استفاده از این سیستم، "حد و حدود زیان رسانی این اخبار جعلی (فیک نیوزها) و تأثیرات ثانویهٔ منفی آن بر اهداف نظامی المان" را مورد ارزیابی قرار دهد. به این خاطر "فرماندهی نظامی در منطقهٔ عملیاتی" می تواند در کوتاه ترین مدت با تزریق "اطلاعات خنثی کننده" واکنش نشان دهد. در مراحل اولیهٔ آزمایش، این نرم افزار توانست در چندین میدان جنگ با "موفقیت ازاین آزماشها سربلند" بیرون بیاید. مقامات ارتشی می گویند: "به این طریق و با کمک این نرم افزار یک متد علمی تبدیل به یک ابزار قدرتمند نظامی می شود."[٥]

"امکانات عمل قدرت غیر فعال"

متناسب با این، "مرکز عملیات سایبری" ارتش المان دیگر تفاوتی بین اقدامات تهاجی و دفاعی در زمان پیشبرد جنگ الکترونیک و دیجیتال قائل نخواهد بود. ارتش اکنون در وضعیتی قرار گرفته است، که "توانائیهای" لازم را "در مرکزی واحد" متحد سازد. اعضای این مرکز در حال برنامه ریزی و آماده سازی عملیات شبکه ئی کامپیوتری برای دوران "دفاع عمومی" و در صورت لزوم ادامهٔ عملیات نیابتی از جانب ارتش المان از مراکز معین ثابت و متحرک ...می باشند."

مسؤول "مرکز عملیات سایبری " (ZCO) می گوید: "برای اینکار از یک سو سیستمهای ارتباطی و شبکه های زیربنائی دشمن مورد شناسائی قرار می گیرند و از جانب دیگر نقاط ضعف شبکهٔ خودی نیز روشن می شوند." وی در ادامهٔ توضیحاتش می گوید: شبیه سازی و سیمولاسیون مدام ورود غیر مجاز به سیستم "شبکهٔ کامپیوتری خودی" نه تنها باعث افزایش سطح امنیتی سیستمهای خودی می گردد، بلکه از آن گذشته تمرینی دائمی است، که زمینه را برای "تکمیل و رشد" توانائیها و ابزارهای مورد استفاده فراهم می سازد.[٦] " از آن گذشته :"این شیوهٔ کار "امکانات و ابزار اجرائی غیر فعال" نوینی را در اختیار فرماندهی نظامی و رهبری سیاسی قرار می دهد، تا در زمان لازم با دسترسی به تجهیزات بیشتری از زرادخانهٔ عملیاتی، با دست بازتری تصمیمات مطلوبتر را اتخاذ کنند."[٧]

"مهاجمین باید خنثی شوند"

برای دستگاه رهبری المان قائل شدن تفاوت بین "توانائی های سایبری" نظامی و غیر نظامی نیز مثل تمایز بین عملیات دفاعی و تهاجمی، مدتهاست که به امری منسوخ شده تبدیل شده است. در جزوه ای که در سال ٢٠١٦ از جانب دولت المان به نام "سیاستهای ستراتیژیک امنیت سایبری" انتشار یافته است می خوانیم:" توانائیهای دفاعی ارتش المان در فضای مجازی بخش عمده ای از مهندسی امنیتی سایبری را تشکیل می دهند...چه در رابطه با امر هماهنگی و انطباق درونی ساختاری اقدامات ایمنی لازم و چه در هنگام شکل دادن ساختارها، روند های عملیاتی و اطلاع رسانی مدافعهٔ سایبری برای دستیابی به این توانائیها." [٨] آندراس کونِن مسؤول واحد "امنیتی اطلاعات و امور سایبری" در وزارت داخلهٔ المان نیز براساس منطق این سیاست خواست "هماهنگی همه جانبهٔ اقدامات امنیتی سایبری در زمینه های نظامی و غیر نظامی در موارد دفاع از ساختارهای حساس، دفع خطرهای موجود در فضای مجازی، سیاست امنیتی سایبری

در سطحی فراملیتی و مدافعهٔ فعال سایبری" را مطرح می کند. مورد آخر بنا بر نظر کونن در برگیرندهٔ "خنثی سازی پیشگیرانهٔ سیستمهای مهاجم" [از طریق حملهٔ پیشگیرانه] نیز است، مثلا "هنگام احساس خطرنابهنگام".[۹]

جرمن فارین پالیسی، ۲۷ ژوئن ۲۰۱۹

منابع:

https://www.german-foreign-policy.com

[۱] Zentrum Cyber-Operationen kooperiert erfolgreich mit Firma CGI. cir.bundeswehr.de 18.04.2019.

[۱-(a] Cooperative Cyber Defense Center of Excellence (CCDCOE)

[۲] Zehn Fragen - zehn Antworten. cir.bundeswehr.de 09.04.2019.

[۳] Auf dem digitalen Gefechtsfeld - Locked Shields. bmvg.de 16.05.2018.

[٤] Zehn Fragen - zehn Antworten. cir.bundeswehr.de 09.04.2019.

[٥] Medien sind Waffensysteme. cir.bundeswehr.de 21.03.2019.

[٦] Zentrum Cyber-Operationen offiziell in Dienst gestellt. cir.bundeswehr.de April 2018.

[۷] Das Zentrum Cyber-Operationen - Über uns. cir.bundeswehr.de 06.03.2019.

[۸] Bundesministerium des Innern (Hg.): Cyber-Sicherheitsstrategie für Deutschland. Berlin 2016.

[۹] Andreas Könen: Cybersicherheit und Cyberverteidigung. Stärkerer Schutz durch ressortübergreifende Zusammenarbeit. In: Ethik und Militär 1/2019