.

بررسی و تحلیل امنیت سایبری در برگزار ی رویداد های ورزشی :مطالعه مروری

یاسمن سادات اصل احمدی *[۱]، مهرعلی همتی نژاد [۲]

۱. دانشجوی دکتری مدیریت ورزشی دانشگاه گیلان

Yasaman77yasaman@gmail.com

۲.استاد دانشگاه گیلان

ma_hemati@yahoo.com

چکیده

اصطلاح امنیت سایبری در ورزش از زمان گسترس فناوری های دیجیتال در رویدادهای ورزشی پررنگ شده است فن آوری های دیجیتالی مجموعه تهدیدات متنوعی را برای رویدادهای المپیک به وجود آورده اند که امروزه اکثر هک ها روی سیستم های آی تی و استادیوم های ورزشی تمرکز دارند، خطرات آینده رویدادهای ورزشی شامل هک هایی خواهد بود که به یکپارچگی نتایج رویداد ورزشی و عملکردهای اصلی ورزشگاه ها را کاهش می یابد. این مطالعه هشت زمینه اصلی خطر برای رویدادهای ورزشی آینده را مشخص می کند:۱.سیستم استادیوم هک می شود؛۲.امتیاز سیستم هک؛۳. هک های پخش عکس و فیلم؛۴. هک های مراقبت از ورزشکاران؛۵. دستکاری ورودی؛۶. هک های حمل و نقل؛۷. هک هایی برای تسهیل تروریسم یا آدم ربایی؛۸. وحشت حاصل از هک شدن.بنابراین از آنجاکه هک های موثر بر تمامیت ورزش به طور ویژه نگران کننده هستند .پیشنهاد می شود مسئولان ورزشی با توجه به فناوری های جدید ، خطرات مربوط به امنیت سایبری ناشی از چنین فناوری هایی را در برابر فرصت هایی که برای رویداد ورزشی گسترده تربسنجند و با دستگاه های آنالوگ با تاکید بر مزایای ملموس خطرات را به نسبت قابل توجهی کاهش دهند.

واژه‌های کلیدی :امنیت سایبری، رویداد های ورزشی،هک ، امنیت سخت ،امنیت نرم

مقدمه

در دنیای امروز که همه‌چیز در پرتو فناوری اطلاعات قابل‌تعریف است بشر و بدون استفاده از چنین امکاناتی نمی‌تواند زندگی خویش را ادامه دهد توجه به‌پیش فرض‌های این زندگی مدرن مشکلات زیادی با خود به همراه دارد اما باید توجه کرد که اولین قدم ، شناخت خطرات و موجود عواقب وخیم آن‌هاست. اولین رسالت ،امنیت حفاظت از سرمایه‌های یک سازمان است که ممکن است شامل آیتم‌های ملموسی نظیر یک صفحه وب و یا اطلاعاتی بانک مشتریان و یا آیتم‌های غیرملموسی نظیر شهرت و اعتبار یک سازمان باشد. امنیت یک مسیر است نه یک مقصد و به تجزیه‌وتحلیل زیرساخت و برنامه‌های موجود می‌بایست اقدام به شناسایی تهدیدات و خطرات ناشی از آنان نمود. فضای سایبری در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. به امنیت فناوری اطلاعات، وابسته به سیاست دولت‌ها امنیت سایبری گوییم. این اصطلاح عموماً توسط مؤسسه‌های دولتی و سیاست‌گذاران ملی در اسناد، قوانین و پروژه‌های تحقیقاتی استفاده می‌شود و کمابیش مترادف با " امنیت اینترنت "است. هردو عبارت به جوانب امنیت شبکه و اصول سیاست‌گذاری شبکه‌ها مثل تعریف حریم خصوصی جرائم سایبر، تجارت و ارتباطات جهانی اشاره دارند(بستان و همکاران،۱۳۹۱).

در فضای سایبر ،از مقوله‌ی امنیت سخت به نام قدرت یاد می‌شود که به این صورت تعریف می‌شود (استفاده‌ی طراحی‌شده از تبلیغات و فعالیت‌ها جهت تأثیرگذاری عقاید نگرش‌ها، احساسات و رفتار گروه‌های خارجی به شکلی که از اهداف ملی حمایت و در افکار عمومی نیز کسب اعتبار نماید (نوری،۱۳۹۴). قدرت متقاعد کردن مردم و شکل‌دهی افکار آنان به‌صورت فرماندهی و توانایی تغییر آنچه دیگران انجام می‌دهند .در عصر سایبر جهان جدید به شبکه‌ی نیرومندی تبدیل‌شده است که بافت اصلی و تاروپودان را اطلاعات و نظام ارتباطات الکترونیک تشکیل می‌دهد .در درون این شبکه به‌جز گروهی از نخبگان دیگران کنترل خود را بر زندگی خویش و محیط پیرامون از دست دادند یا به‌سرعت در حال از دست دادن هستند. امنیت نرم یا تهدید در عرصه‌ی سایبری تحولاتی است که موجب دگرگونی در هویت فرهنگی و الگوهای رفتاری موردقبول یک نظام سیاسی می‌شود(احمدزاده،۱۳۸۸).

تحلیل: خطرات امنیت سایبری رویدادهای مهم ورزشی

خطرات امنیت سایبری در رویدادهای ورزشی شامل :امنیت فیزیکی؛یکپارچگی امکانات ورزشی؛ یکپارچه‌سازی ورزش؛ امتیازدهی و بازی؛ خطر مالی و چاپ بلیط و نشر آن‌که در ادامه موردبحث و بررسی قرار خواهد گرفت(کوپر[1]،۲۰۱۷)

امنیت فیزیکی

جدی‌ترین حملات سایبری احتمالی در مسابقات مهم ورزشی مواردی است که می‌تواند به تماشاگران ورزشکاران ، مسئولان و یا سایر شرکت‌کنندگان صدمات جسمی وارد کند. به‌طورکلی ، چنین حملاتی کاملاً نادر است و اغلب به هدف قرار دادن سیستم‌های امنیتی زیرساخت‌های فیزیکی - حمل‌ونقل ، وسایل پزشکی و غیره که برای محافظت از زندگی انسان‌ها طراحی‌شده‌اند.

1 .cooper

درحالی‌که تصور می‌شود که دستگاه‌های دیجیتالی می‌توانند برای تسهیل آسیب‌های جسمی دست‌کاری شوند - به‌عنوان‌مثال، یک اسکنر بدنه می‌تواند هک شود تا به یک تروریست اجازه دهد با اسلحه وارد محل شود، یا وسیله نقلیه حمل‌ونقل فراری می‌تواند از راه دور برای ربودن یا آسیب رساندن ورزشکاران یا تماشاگران کنترل شود — چنین حوادث بعید نیست که به درجه بالایی از مهارت نیاز داشته باشد، و به دلیل اینکه نقاط لمس نسبتاً کمی در این رویداد وجود دارد که از طریق آن می‌توان چنین تأثیراتی را حاصل کرد. حتی در این صورت، به‌احتمال‌زیاد، تماشاگران یا ورزشکاران می‌توانند در اثر وحشت باعث حوادث ناشی از نقض سیستم غیرقانونی شوند. به‌عنوان‌مثال، یک صفحه‌نمایش دیجیتالی شبکه‌ای در استادیوم می‌تواند هشدار داده شود تا هواداران را از تهدید تروریستی آگاه سازد، و این پیام را منتشر می‌کند که باید در اسرع وقت ازآنجا خارج شوند. حتی اگر هشدار نادرست بود، احتمالاً وحشت ناشی از آن رخ خواهد داد باعث آسیب‌دیدگی جسمی تماشاچیانی که می‌خواستند از ورزشگاه خارج شوند، می‌شوند. (چنین هک بدون سابقه نیست؛ برای نشان دادن محتوای توهین‌آمیز و گمراه‌کننده، تعداد زیادی علائم راهنمایی و رانندگی هک شده است).توجه داشته باشید که، برای هر یک از این موارد - حمله تروریستی، تصادف وسیله نقلیه موتوری یا خرد شدن جمعیت - خطر ابتلا به فن‌آوری‌های دیجیتالی است. همه این حوادث ممکن است امروز رخ دهند، حتی مداخله دیجیتالی نیز وجود ندارد. آنچه هک انجام می‌دهد، مداخله در یک نقطه امنیتی سنتی (اسکنر امنیتی ؛ راننده اتومبیل ؛ خروج اضطراری)، از بین بردن محافظت در برابر آسیب‌های جسمی است که به‌راحتی در عصر آنالوگ قابل دست‌کاری نیست(مجیک برند[2]،۲۰۱۷).

یکپارچگی امکانات ورزشی

دسته دوم حملات شامل مواردی است که در یکپارچگی تأسیسات ورزشی تداخل دارند ، اما از آسیب دیدن جسمی به ورزشکاران یا تماشاگران کاسته می‌شوند. در این موارد ، ضرر اصلی به‌خودی‌خود ورزشی است ، زیرا این رویداد طبق برنامه‌ریزی قادر به خاموش شدن نخواهند بود.

اولین حمله به خود امکانات پزشکی است. مانند بازی‌های لندن ، شبکه برق از دست دادن برق همچنان یک نگرانی جدی است ، اگرچه ازنظر محافظت‌شده نیز پشتیبانی می‌شود. سایر سیستم‌های نگهدارنده کلیدی - به‌عنوان مثال ، سیستم‌های گرمایشی / سرمایشی یا لوله‌کشی به‌طور مشابه می‌توانند تحت تأثیر قرار بگیرند تا از وقوع رویداد جلوگیری کنند. این بردارهای حمله در حال حاضر وجود دارند ، اما احتمالاً با دیجیتالی شدن سیستم‌های تسهیلات گسترش می‌یابند. علاوه بر این چالش ، این سیستم‌ها در بسیاری موارد نه توسط خود تسهیلات بلکه توسط پیمانکاران خارجی کنترل می‌شوند

سایر تهدیدات احتمالی زیرساخت‌های فیزیکی مربوط به استفاده از فناوری‌های جدید برای سایر جنبه‌های رویدادهای ورزشی ازجمله امتیازدهی و مشاهده است. به‌عنوان‌مثال، هواپیماهای بدون سرنشین دوربین در طول بازی‌های المپیک ریو برای تأمین پوشش تلویزیون در امتداد مسیرهای قایقرانی طولانی استفاده می‌شدند. (بازی‌های قبلی المپیک برای پشتیبانی از یک دوربین رونگ، به مسیری ۲،۰۰۰ متری آویزان بود.) باعث آسیب جدی جسمی به ورزشکاران یا تماشاگران می شود. فن‌آوری‌ها منطقه دیگری که به‌شدت در جهت دیجیتال گرایش پیدا می‌کند، بلیط فروشی و پرداخت در مراکز مهم ورزشی است. به‌طور فزاینده، بلیط‌فروشی با مکانیزم های پرداخت خرده‌فروشی به یک دستگاه الکترونیکی پوشیدنی همراه است. یکی از پیشگامان این فضا دیزنی است که هم‌اکنون بندهای — MagicBands را ارائه می‌دهد که به‌صورت الکترونیکی به پارک تفریحی، هتل و کالاهای تجاری دسترسی پیدا می‌کنند

2 . MagicBands & Cards

درعین‌حال، به دلیل این دستگاه‌ها و سیستم‌های پایان‌بخش پشتیبان آن‌ها چندین هدف باارزش بالقوه - اعتبار برای دستیابی به رویدادها، قدرت خرید، دسترسی به امکانات اولویت را یکپارچه می‌کنند - برخی از این خطرات نسبتاً جزئی هستند. به‌عنوان‌مثال، اگر یک باند واحد و دارای صندلی‌های باارزش برای کپی کردن اعتبارنامه دسترسی، هک شد، ضرر اصلی در جبران مصرف کننده آسیب‌دیده رخ می‌دهد(مجیک برند،۲۰۱۷).

یکپارچه‌سازی ورزش

دسته سوم - تهدید به حمله سایبری که بر یکپارچگی یک رویداد ورزشی تأثیر می‌گذارد لذا سوال اصلی این است که آیا فناوری می‌تواند باعث شود نتایج ورزشی در آینده موردتردید واقع شود؟ در این بخش به بررسی احتمالات ، با نگاهی به هک‌های گلزنی و بازی ، پخش ویدئو و مراقبت از ورزشکاران پرداخته می‌شود.

امتیازدهی و بازی

در بسیاری از ورزش‌ها، امتیاز و بازی شامل سیستم‌های دیجیتالی است که نقش مهمی در تعیین نتیجه مسابقه دارند. بیشترین آشنایی در اینجا سیستم‌های امتیازدهی دیجیتال است که رویدادهای مبتنی بر زمان مانند شنا، پیگیری و قایقرانی را کنترل می‌کنند. تابلوهای زمان‌بندی برای ردیابی چرخش شناگران و ردیابی خودکار هنگام عبور یک دونده از خط، به‌طور فزاینده‌ای متداول بوده و آسیب‌پذیری احتمالی را نشان می‌دهد. قوانین بین‌المللی شنا اکنون به‌صراحت استفاده از این قانون را مجاز می‌دانند

امتیازدهی و بازی

در بسیاری موارد، از فناوری برای تعیین نتایج نهایی نمره استفاده نمی‌شود، بلکه برای کمک به داوران درنتیجه گیری در مورد نتایج به کار می‌رود. در اکثر ورزش‌های المپیک، افزایش سرعت استفاده از فناوری به‌عنوان کمک گلزنی با سرعت ، به‌طور پیوسته افزایش‌یافته است که متکی بر سیستم عکاسی است .درحالی‌که جابجایی عکس برای پزشک در زمان واقعی بسیار دشوار خواهد بود، در مواردی که چندین ورزشکار به‌طور مداوم در یک سطح مشابه مسابقه می‌دهند، ممکن است یک هکر بتواند عکس واقعی را با عکس آماده‌شده قبلی جایگزین کند یا داده‌های عکس واقعی مسابقه را حذف کند. در کل حتی بدون تغییر نتیجه به‌طور مستقیم، یک عکس نادرست یا گمشده می‌تواند در نتایج کلی شک ایجاد کند پیروزی مایکل فلس را مقابل میلوراد کاویچ به دست آورید(همبیلینگ[3]،۲۰۱۷)

مراقبت از ورزشکاران

تجزیه‌وتحلیل فوق متمرکز بر تلاش برای تغییر امتیازات مسابقات ورزشی، چه مستقیم و چه با تأثیرگذاری بر تصمیمات مسئولان است. اما راه دیگری وجود دارد که عدم امنیت کافی در سایبر می‌تواند با تأثیرگذاری بر عملکرد ورزشکاران، صداقت حوادث مهم ورزشی را به خطر بی اندازد . حمله به امنیت سایبری می‌تواند به‌طور مستقیم بر عملکرد ورزشکاران در طول رویداد تأثیر بگذارد، بااین‌حال ، روشی را شناسایی کنید که با استفاده از آن هکر بتواند عملکرد خود را در خارج از زمینه رقابت با دست‌کاری موارد انجام دهد. سیستم‌های خودکار مواد غذایی به‌طور فزاینده‌ای متداول شده‌اند. زنجیره غذایی

3 . Hambling

استارتاپ کالیفرنیا، Eatsa، اکنون کاسه‌ها و سالادهای غذایی را از طریق مبادله‌ای که در آن همه‌چیز به‌جز پخت‌وپز واقعی صورت می‌گیرد، توزیع می‌کند(رابیسنون[۴]،۲۰۱۷) .

خطر مالی: چاپ بلیط و نشر آن

هرکدام از حملات ذکرشده تاکنون علاوه بر ایجاد مزاحمت در یکپارچگی ورزش و مکان‌هایی که در آن اتفاق می‌افتد، می‌تواند عواقب مالی جدی داشته باشد. علاوه بر این، برخی از حملات بالقوه مستقیماً درآمدهای مالی قرار دارند. برخی از این حملات، مانند وب‌سایت‌های ورزشی جعلی و کلاه‌برداری بلیط، در سال ۲۰۱۷ به‌خوبی شناخته‌شده‌اند. احتمالاً این موارد به آینده ادامه خواهند یافت، اما بعید است مکانیسم‌های دستیابی به آن‌ها تغییر چشمگیری داشته باشد .علاوه بر خطرات مشخص‌شده قبلی، چنین سیستمهایی می‌توانند برای جمع‌آوری جزئیات مالی تلفیقی مشتریان مورد سوءاستفاده قرار بگیرند. ازآنجاکه هر شرکت‌کننده ملزم به استفاده از باند برای فروش بلیط است، در صورت نفوذ به سیستم، جمع‌آوری هکرها راحت‌تر خواهد بود جزئیات پرداخت برای چندین کاربر به‌طور همزمان. امروزه این خطر محدود به افرادی است که در این رویداد از روش‌های پرداخت الکترونیکی استفاده می‌کنند و بسته به نوع پرداخت مورداستفاده، خطر متفاوت است(مونیکا[۵]،۲۰۱۷)

ریسک اعتبار: مشاهده تجربه

نوع دیگر خطر امنیت سایبر ایجاد خسارت جسمی یا مالی است، هکرها می‌توانند به اعتبار یک رویداد پرمخاطب خسارت قابل‌توجهی وارد کنند. فعالیت‌های هک شدن در ورزشگاه، مگر اینکه پخش گسترده‌تری داشته باشد، فقط روی ورزشگاه‌ها تأثیر می‌گذارد. این توانایی برای به اشتراک گذاشتن تجربه المپیک با میلیون‌ها نفر از مردم در خانه است که به ورزش می‌دهد.توجه به شیوه تماشای مخاطبان مهم رویدادهای ورزشی، هکرها فرصت‌هایی را برای تغییر آنچه که آن بینندگان تجربه می‌کنند، تغییر می‌دهند. به‌عنوان‌مثال، سیستم‌های واقعیت مجازی در حال حاضر به تیم‌های اصلی ورزشی مانند غول های نیویورک در درک شرایط بازی خود کمک می کنند و بسیاری گمان می‌کنند که واقعیت مجازی با اجازه دادن به تماشاگران در مسابقات مهم ورزشی، تجربه دیدنی بعدی را فراهم می‌کند تا این رویداد را از منظر رسمی یا حتی ورزشکار تجربه کنند(ماتریس خطر ،۲۰۱۷).

به‌طور خلاصه، این بررسی نشان می‌دهد که اگرچه نقض‌های موجود در امنیت سایبر - که بیشتر در ریسک مالی متمرکزشده‌اند - احتمالاً ادامه خواهد یافت، احتمالاً موج جدیدی از حملات نیز رخ خواهد داد. هک‌هایی که بر تمامیت ورزش تأثیر می‌گذارند بسیار نگران‌کننده هستند زیرا می‌توانند بسیار شدید باشند .شناسایی خصوصاً در ورزش‌هایی که داوران تصمیمات بسیار کوچکی را می‌گیرند که تأثیر می‌گذارد،دشوار می‌باشد.درنتیجه ، تشخیص زمانی که یک سیستم دیجیتال به خطر بیفتد بسیار دشوار است.مسئولان ورزشی در نظر دارند که باید یک فناوری جدید در ورزش را مهم معرفی کنند رویدادهای ورزشی باید خطرات امنیت سایبری را که توسط چنین فناوری‌هایی در برابر فرصت‌ها ایجاد می‌شود ، تعیین کند.

---

4 . Robinson

5 .Monica

خطرات معاصر در فضای مجازی ورزش نیز شامل: نفوذ به وب‌سایت‌های ورزشی و سیستم‌های IT ؛ کلاه‌برداری‌های مربوط به بلیط؛ هک شدن و رهایی از داده‌های حساس ورزشکار؛ خطر هک شدن هواداران هنگام حضور در یک رویداد.هک‌های مؤثر بر تمامیت ورزش به‌طور ویژه نگران‌کننده هستند زیرا شناسایی آن‌ها بسیار دشوار است. به‌خصوص در ورزش‌هایی که داوران تصمیمات بسیار کمی را در تصمیم‌گیری می‌گیرند که نتیجه را تحت تأثیر قرار می‌دهد، تشخیص این‌که چه موقع یک سیستم دیجیتال به خطر بیفتد بسیار دشوار است مسئولان ورزشی با توجه به اینکه فناوری‌های جدید را در یک رویداد مهم ورزشی معرفی می‌کنند، باید خطرات مربوط به امنیت سایبری ناشی از چنین فناوری‌هایی را در برابر فرصت‌هایی که برای رویداد ورزشی گسترده‌تری که ارائه می‌دهند، بسنجند. به‌خصوص هنگامی‌که فروشندگان دستگاه‌های دیجیتالی جدیدی را به مقامات ورزشی معرفی می‌کنند، دیجیتالی شدن روزافزون رویدادهای مهم ورزشی وسوسه‌انگیز خواهد بود. بااین‌وجود، دستگاه‌های آنالوگ اغلب می‌توانند همان کار را به روشی مطمئن‌تر انجام دهند. سازمان دهندگان باید با تأکید بر مزایای ملموس دستگاه‌های دیجیتال- خطرات قابل‌توجه را نیز کاهش دهند.لذا مهم‌ترین مرحله در جلوگیری از تهدیدات و حملات سایبری آموزش عمومی ، امنیتی و پلیسی است . لذا باید در ایمن کردن فضای سایبر آن‌ها را متقاعد کرد و با آگاهی دادن به مردمان تا را وادار کرد تا تمهیدات لازم را برای مقابله با تهدیدات سایبری اعمال کنند. علاوه بر سازوکار موفق باید سازوکار حقوقی و قضایی مناسبی را برای مقابله با تهدیدات سایبری ایجاد کرد.مانند از بین بردن خلا های قانونی نیروی امنیتی و قضایی و تقویت دفاعی سازمان‌های مقابله با حملات و تهدیدات سایبری (نوری،۱۳۹۴).لذا پیشنهاد می‌شود در این زمینه پژوهش‌های بیشتری صورت گیرد

منابع

- ✓ احمدزاده کرمانی، روح اله.(۱۳۸۸). درآمدی بر ماهیت شناسی جنگ نرم پس از انقلاب اسلامی ایران. مطالعات بسیج، ۱۲(۴۳). SID. https://sid.ir/paper/479459/fa
- ✓ بستان، شکوفه و کارگر، محمد جواد.(۱۳۹۱).امنیت در محاسبات شبکه‌ای،همایش منطقه ای علوم کامپیوتر، مهندسی کامپیوتر و فناوری اطلاعات،دورود، https://civilica.com/doc/173490
- ✓ نوری، فاطمه.(۱۳۹۴).فضای سایبری: امنیت سخت یا امنیت نرم،اولین همایش بین المللی نوآوری و تحقیق در هنر و علوم انسانی، https://civilica.com/doc/431872

- ✓ Dan Benton, “Giants Implementing Virtual Reality Screen to Aid Practice,” Giants Wire, July 26th, 2017, http://giantswire.usatoday.com/2017/07/26/new-york-giants- implementing-virtual-reality-screen-aid-practices/.
- ✓ David Hambling, “Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon,” New Scientist, August 10, 2017, https://www.newscientist.com/article/ 2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/.
- ✓ MagicBands & Cards – FAQs,” Disney World, accessed October 3, 2017, https://disneyworld.disney.go.com/faq/bands-cards/understanding-magic-band/.
- ✓ Melia Robinson, “This Salad-Making Robot Can Build 1,000 Different Salads in 60 Seconds Each,” Business Insider, April 14, 2017, http://www.businessinsider.com/ sally-the-salad-robot-chowbotics-2017-4.

- ✓ Monica Nickelsburg, "Walmart Cuts in Front of Amazon Go with App That Lets Shoppers Check Out without Lines or Registers," Geek Wire, August 8, 2017, https:// www.geekwire.com/2017/walmart-cuts-front-amazon-go-app-lets-shoppers-check-without-lines-registers/.
- ✓ Russell Brandom, "Podesta's Email Hack Hinged on a Very Unfortunate Typo," The Verge, December 13, 2016, https://www.theverge.com/2016/12/13/13940514/dncemail- hack-typo-john-podesta-clinton-russia.
- ✓ There are very few reviews connecting cybersecurity and major sporting events. A handful come from cybersecurity-related magazines: Adam Finkelstein, "CyberSecurity at Major Sporting Events," Israel Defense, December 4, 2016, http://www.israeldefense.co.il/en/content/cyber-security-major-sporting-events.; Idan Udi Edry, "A New Kind of D-fense: Cybersecurity in Sports Stadiums," Engadget, October 15, 2016, https://www.engadget.com/2016/10/05/a-new-kind-of-d-fense-cybersecurity-in-sports-stadiums/; "Securing the 2012 Olympics," Infosecurity Group, November 19, 2009, https://www.infosecurity-magazine.com/magazine-features/securing-the-2012-olympics/; Alan Brill and Snezana Petreska, "Are Cyber Criminals Competing at the Olympics?," Freedom From Fear Magazine, (May 2015) : 24-37, http:// insct.syr.edu/wp-content/uploads/2015/05/Brill_Olympics.pdf. The articles focus on digital attacks on computing infrastructure at major sporting events, rather than the broader array of ways that cyberattacks could affect sporting event outcomes
- ✓ ThreatMetrix Identifies the Top Five Cybersecurity Threats of Olympic Proportions," ThreatMetrix, press release, July 19, 2012, https://www.threatmetrix.com/press-releases/threatmetrix-identifies-the-top-five-cybersecurity-threats-of-olympic-proportions/.