CENTER FOR LONG-TERM CYBERSECURITY

CLTC OCCASIONAL WHITE PAPER SERIES

The Cybersecurity of Olympic Sports:

NEW OPPORTUNITIES, NEW RISKS

BETSY COOPER
WITH KATIE CHEN, ZOE FEIST, AND CHUCK KAPELKE

Executive Summary

As major sporting events become increasingly digitized, sports officials are increasingly concerned about cybersecurity. From scoring and judging systems to retail transactions and the home viewer experience, many aspects of major sporting events are incorporating new forms of internet connectivity. Along with such new technology comes great opportunity – but also great risk.

This report is the first to systematically review the cybersecurity risks posed by digital technologies that are being incorporated into major sporting events. Using the Olympic Games as a case study, it lays out a framework for evaluating potential risks posed by digital technologies in sports, and highlights new possible threats that will arise as these technologies are deployed.

Overall, the paper points to three key findings:

- Digital technologies pose an increasingly diverse set of threats to Olympic events, and the newer forms of threat are likely to have more serious consequences. While most hacks today focus on sports stadium IT systems and ticket operations, future risks will include hacks that cut to the integrity of the sporting event results, as well as to core stadiums operations. This study identifies eight key areas of risk for future sporting events:

  - Stadium system hacks
  - Scoring system hacks
  - Photo and video replay hacks
  - Athlete care hacks
  - Entry manipulation
  - Transportation hacks
  - Hacks to facilitate terrorism or kidnapping
  - Panic-inducing hacks

- Hacks affecting the integrity of sports are of special concern because they can be extremely difficult to identify. Especially in sports where referees make many small decisions that affect the result, it is very difficult to detect when a digital system has been compromised.

- Sporting officials considering whether to introduce a new technology into a major sporting event should weigh the cybersecurity risks posed by such technologies against the opportunities for the broader sporting event they provide. Especially as vendors push out shiny and new digital devices and market them to sports officials, it will be tempting to increasingly digitize major sporting events. Even so, analog devices can often do the same job, and in a more secure way. Organizers should press to ensure that there are tangible benefits to incorporating digital devices—and that significant risks can be mitigated—before going forward.

Introduction

Imagine if, at the 2028 Olympics, the gymnastics all-around final were to be halted mid-event. Several countries file a protest alleging that a new electronic scoring system, using artificial intelligence to gauge the heights of athletes' leaps and the number of completed flips, is systematically misjudging their athletes. A cybersecurity firm is called in, and soon uncovers the organizers' worst nightmare: the system was hacked—and the scores were rigged. Would the event be re-competed on a later date, or re-scored by humans using the television feed?

Even in the pre-digitization era, the integrity of major sporting events has come into question. In the 2000 Sydney Olympics gymnastics final, the height of the vaulting horse was improperly set, leading athletes across several rotations to make mistakes before an Australian athlete noticed the incorrect setting. While the affected athletes were allowed to repeat their routine at the end of the meet, several key competitors, including pre-meet favorite, Svetlana Khorkina, had already made additional errors, believing their hopes of winning were over.[1]

But the digitization of major sporting events poses new vectors of opportunity—and risk. On the one hand, there is an increasing supply of opportunities for digital manipulation as sports incorporate new technologies designed to improve athlete training, accessorize the fan experience, and even help officials decide the results. All of these technologies provide tremendous new opportunities to improve how sports are performed and experienced, but they also provide new vectors of attack. Because so many of these systems will be connected to the internet in the future, malicious actors may not need physical access; they can try to disrupt the event from the comfort of their own home.

On the other hand, the temptation to manipulate major sporting events may only be increasing. Such events are increasingly popular and increasingly profitable,[2] and along with that profitability comes an increase in monetary investment in the surrounding industry. From innovative on-site retailers to new at-home fan experiences, the ways in which the public can engage with sports through technology is ever expanding. Sports gambling in particular poses a threat, because with the growth in "proposition betting" on moment-to-moment events,[3] gamblers can profit without the (more heavily scrutinized) final result necessarily being affected.

Together, these supply and demand vectors present a tremendous landscape for risk. Consider the sport of tennis. In matches where the technology is present, the Hawk-Eye system (which judges whether a ball is in or out of the tennis court) is the ultimate arbiter for any player challenging a line call. Imagine if that system were to be hacked, such that every fifth Hawk-Eye review favored a particular player. Who would catch the difference? Could a clever gambler benefit from the ultimate result? And how could we know whether this type of corruption is already happening? (Any amateur tennis viewer has certainly watched calls that looked to the naked eye to go one way, yet Hawk-Eye called another.)

This paper is meant to tee up important questions about the cybersecurity of sports,[4] using as its frame the Olympics movement, and particularly a Summer Olympics Games set to take place roughly 10-15 years into the future. How will sports be different? What new technologies may exist? And how do they provide both the opportunity to change the way we perceive the role of major sporting events, and the risks that come with technological change?

The white paper begins with a risk framework (Failure Mode and Effects Analysis) to evaluate the seriousness of attacks on major sporting events. It then reviews historical evidence on hacking of major sporting events such as the Olympics, categorizing them according to the framework. Finally, focusing on the Olympics, and particularly on four summer sports—gymnastics, rowing, swimming, and track and field—the paper reviews a variety of potential future risks. The paper concludes with recommendations and next steps.[5]

A Risk Framework for the Cybersecurity of Sports

It is axiomatic that not all cyberattacks are created equal. Yet when it comes to major sporting events, there has been no coherent effort to categorize the risks that are particular to these types of events, and/or to enable officials to prioritize among the various types of attacks. Here, we make a first effort to outline such a framework.

For this analysis, we borrow the technique of Failure Mode and Effects Analysis (FMEA), a process generally used to evaluate the ways in which a product can fail and how serious the consequences will be. FMEA has three dimensions: (1) Severity, or how serious the negative outcome could be; (2) Occurrence, or how likely or frequent the negative outcome could be; and (3) Detectability, or how likely it is that the negative outcome will go undetected.[6] While not normally used to evaluate cybersecurity risks, the framework provides a useful method to weigh dissimilar cyber events against each other. In what follows, we lay out a theoretical framework for how to measure risks in major sporting events.

Severity: We can roughly categorize attacks based on the degree to which a given incident is likely to impede the event from successfully occurring. Most serious would be physical harm caused to the athletes or spectators; in such a case, the event would be overshadowed and likely cancelled as a result of these more serious harms. Disruption to the venue of a major sporting event would also be quite serious, and could prevent the event from occurring altogether. Attacks on the integrity of the sporting event would also be serious; though physical effects are less likely, interference with the outcome could result in a decreased sense of trust that would have lasting impacts on the sport. All three of the previous categories would of course have financial effects; a lesser category of harm would involve purely financial effects that do not otherwise interfere with game or stadium play. Last is reputational loss. Even absent financial or other disruption, cyberattacks can nevertheless sow doubts about the reputation of the sponsoring organization (and its ability to handle disruptions). Note that these effects are roughly additive; an incident that disrupts a sports venue is also likely to have an impact on the integrity of the event, as well as its finances and reputation.

Occurrence: The second dimension is occurrence, or the likelihood of a disruption. Again, this varies widely depending on the specifics, but roughly aligns with the number of ‘touch points,’ or independent spaces on the attack surface, which the attacker can manipulate to affect the sporting event. All else equal, the fewer touch points upon which an attacker can execute an attack, the less likely such an attack is to occur. Least likely are terrorist attacks intended to cause physical harm, because physical attacks using cyber tools are relatively difficult to execute. Wholesale event disruption is also relatively unlikely because of the difficulty in avoiding backup systems. Somewhat more likely is event result disruption, especially because many different components of the event can be affected, such as individual judge scores or official calls. Even more likely is financial harm, because there are so many financial touch points over the course of a major sporting event. Finally, most likely are risks to reputational harm, because they touch every aspect of a major sporting event; any negative effect of a cyberattack can hurt the reputation of the event.

As we reviewed the data in this study, it became clear that, at least in the Olympic sports we considered here, severity and occurrence are closely correlated. The more likely an event is to cause significant harm, the less likely it is to occur. The converse is also true: events less likely to cause significant harm are more likely to occur. While there may be events that are both highly likely and can cause significant harm, we did not uncover any such examples in the course of this study. (There are of course also events that are not likely to cause harm and that are unlikely to occur, but these are not particularly interesting.)

One key reason for the severity-occurrence correlation is that the vulnerability of major sporting events is already understood, and as a result, there are already security protocols in place to try to prevent such harms. Long before the advent of digital technologies, it was recognized that sports events posed significant risks: large crowds, high-impact outcomes, and great public interest all play a role in making such events difficult to secure. As a result, sporting facilities developed infrastructure—such as screening systems, physical barriers, and the like—to prevent the most catastrophic outcomes. Because the same outcomes are at play here—all of the five categories of harm above, from physical to reputational harm could occur without any digital technology whatsoever—there are already infrastructures in place to prevent them. This makes serious attacks less likely. (A good analogy is the risk of flying in an airplane. While there are some risks, such as injury from turbulence, that are relatively common, we have reduced the likelihood of catastrophic loss to the point that it approaches close to zero.)

Because severity and occurrence are correlated, we combine them into an additional concept commonly used in risk frameworks: tolerability, or the willingness of event officials to tolerate the risk of a negative outcome occurring.[7] All else equal, more frequent but less harmful events are more tolerable cybersecurity risks, while the most serious physical harm events are less tolerable.

Detectability: The wild card in this FMEA framework is the third category: detectability. An undetectable cyberattack can cause continued harm, exacerbating the baseline effects. Less detectable events can also recur (for instance, a vulnerability that is repeatedly exploited), leading to multiple undesired incidents.

Not every undetectable event will be disconcerting; there may be small undetected perturbations that cause limited harm. But because less detectable events are by definition less well known, they can exacerbate damages where some are already set to occur. Another way of putting this is that a lack of detectability can affect how we perceive the severity and occurrence of a cyberattack. An event that is low in detectability may appear to be less frequent or less severe in effects than it actually is. Thus, we need to tread cautiously when evaluating the tolerability of particular harms, to ensure that low detectability is not leading us to underestimate their effects.

This is admittedly a rough framework because outcomes vary so widely: a minor event disruption could be less severe than a major financial attack; a certain type of event vulnerability could be more common than expected; and a lack of detectability can change all of the above. Nevertheless, this rough framework does provide a useful way to evaluate which among the many cybersecurity attacks security officials at major sporting events should prioritize. In general, the less tolerable attacks should be prioritized, because the effects they can cause may be greater. Moreover, given that such attacks are less frequent, it will be easier to combat them than to try to account for the many touch points for less severe attacks.

In the remainder of this paper, we evaluate cybersecurity attacks on Olympic events according to this framework. We begin with known, historical events, and then turn to possible future risks that will come to fruition as technology continues to change.

Contemporary Risks in the Cybersecurity of Sports

To date, there are four significant categories of cyberattacks on major sporting events: 1) the infiltration of sporting websites and IT systems; 2) tickets-related scams; 3) the hacking and release of sensitive athlete data; and 4) the risk of fans being hacked while attending an event.[8]

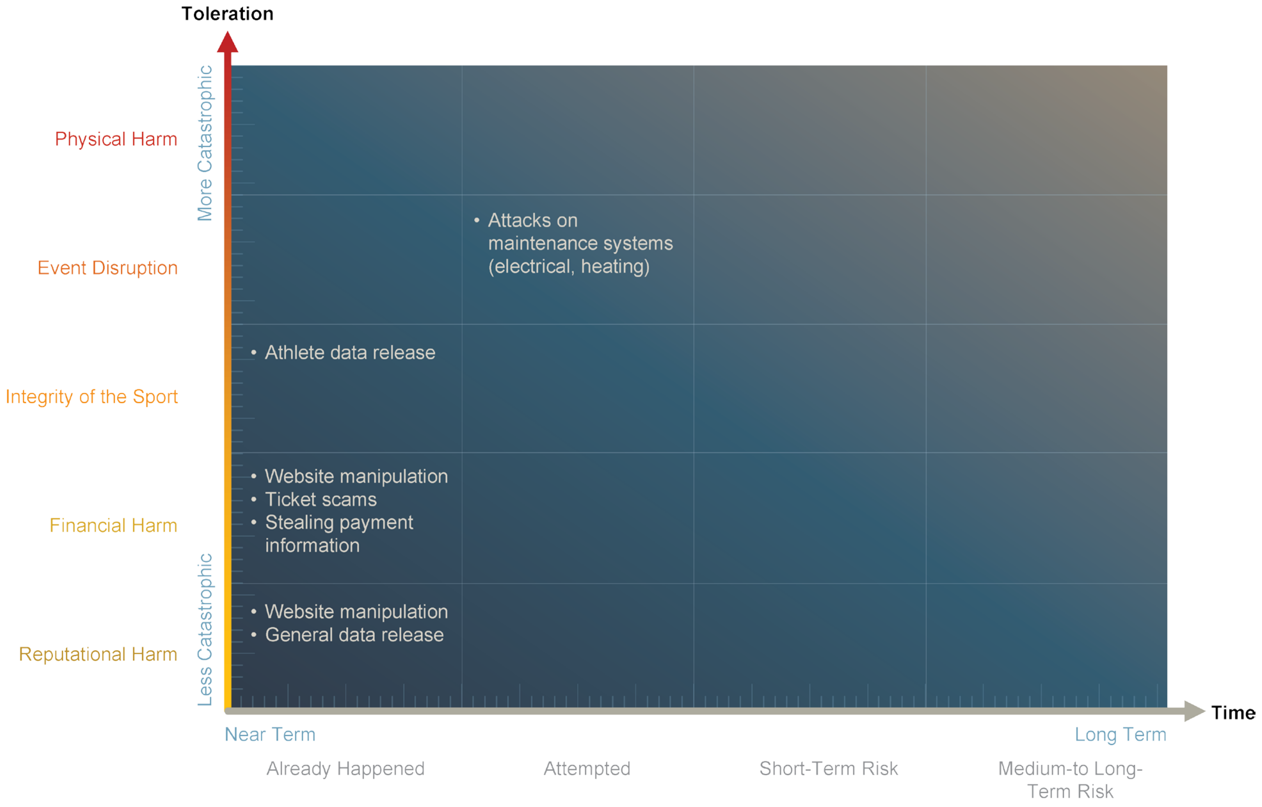
First, like with any other internet-connected system, hackers may seek to manipulate the content or interfere with the functioning of sports websites and email systems. For instance, the hacker group Anonymous once hacked into the Formula One website, protesting the staging of that sport's Grand Prix in the Kingdom of Bahrain.[9] English Rugby League team websites and soccer club Twitter accounts have also been defaced.[10] Organizations that support major sporting events also have been targeted. During the 2014 World Cup, Brazilian officials faced an onslaught of phishing attacks from so-called 'hacktivists', who successfully infiltrated email accounts for many officials with the Ministry of Foreign Affairs, which was helping to organize the Cup.[11] One recurring attack vector is the use of Distributed Denial of Service (DDoS) attacks, which try to make online services unavailable by overwhelming servers with traffic. For instance, the Brazil World Cup faced successful DDoS attacks that took down relevant sporting websites, such as that of the Ministry of Sport.[12] The Rio Olympics similarly combatted a high-volume DDoS attack to keep the Games' website online.[13]

While attempted attacks occur at breakneck speed during major sporting events—in Beijing, officials responded to 11-12 million daily alerts[14]—only a handful rise to the level of imminent threat. The London Olympics reported six major security incidents that were elevated to the Chief Information Officer of the Games. Five of those incidents involved either DDoS attacks or similar attacks (for instance, an infected ad agency associated with the Games sent out so much spam that the IP address used by other press agencies was blocked).[15]

Second, sports tickets are a commonly used prize dangled in front of hopeful members of the public in order to encourage them to divulge credit card information or click on an infected website. Federal courts in the United States shut down several fake ticket websites that promised Beijing Olympic ticket purchases and fraudulently charged credit cards without delivering.[16] The scams were quite effective; family members of Australian Olympians were among those duped.[17] Often, the perpetrators adopt scamming techniques widely used elsewhere, such as advertising a lottery ticket victory. During the London 2012 Olympic Games, scammers sent emails informing recipients that they had won an Olympics-related lottery; those who fell for the scam were asked to pay 'processing' fees to claim their prize.[18] Ticket resale is adding an extra layer of vulnerability. In 2015, hackers plotted to hijack Rugby World Cup online ticket sales in order to force resale on secondary markets and elevate ticket prices.[19]

Third, there is deep recognition of the sensitivity of sports-related data, and the threat of such data being stolen as a result. In 2015, hackers accessed the performance data of leading

TOLERATION OF ATTACKS BY TIME: EVIDENCE SO FAR



cyclist Chris Froome in an attempt to discredit him.[20] Hackers also compromised the World Anti-Doping Agency and released sensitive data about which Rio Olympians had been granted waivers to take drugs normally not permitted due to performance-enhancing qualities.[21] The hackers argued that the evidence showed that American athletes in particular were being given an unfair advantage.[22]

Fourth, fans represent populations vulnerable to hacking at major sporting events, in part because of the increased use of connected devices, the low sophistication of protections, and the increased ease of committing cybercrimes.[23] During the Sochi Winter Olympics, NBC News attempted to demonstrate the ease with which fans in Sochi could have their personal devices hacked.[24] While the report was widely panned as not demonstrating vulnerabilities unique to the Olympics,[25] it nevertheless demonstrated the broader difficulties fans face in avoiding risks while traveling.

Applying these events to the risk management framework discussed above, all of these sports-related hacks share a common theme: a focus on accessing or gaining control of computing systems used to store sports data or data held by sports fans. The main effects of such attacks are reputational or financial; hackers are either seeking to affect the reputation of the sport by taking its IT offline, or they are trying to make a quick buck. The one exception: the athlete data hack, which arguably tried not only to affect the Rio Olympics' reputation, but to call into question the validity of sporting results.

It is worth noting that a hack significantly affecting the physical facilities of a sporting event has yet to occur. However, the concern is not entirely without precedent. In the London 2012 Olympic Games, there was a credible threat that the electrical grid would be hacked, shutting off power during the opening ceremony. Luckily, the threat was a false alarm; even so, such false positives risk 'softening' targets in the future by getting them accustomed to the possibility of non-events.[26]

The Olympics

In light of the perceived cybersecurity risk faced by modern major sporting events, the Olympic movement is taking cybersecurity increasingly seriously. During the London Olympic Games, officials developed Security Operations Centers to ensure real-time detection of threats to the IT and physical infrastructure of the Games.[27] Japan (following in the footsteps of the London Olympics) invited ethical hackers to test its government computer systems in preparation for the Tokyo Olympics.[28] Officials found that government websites were attacked approximately twice per minute.[29]

Selected known cybersecurity incidents from the last three summer Olympic Games include:

BEIJING:

- Ticket scamming
- DDoS and related attacks against IT infrastructure

LONDON OLYMPICS:

- Ticket scamming
- DDoS and related attacks against IT infrastructure
- False alarm threat to the electrical grid

RIO OLYMPICS:

- Ticket scamming
- DDoS and related attacks against IT infrastructure
- Athlete data hack

Future Vectors of Opportunity and Risk

While there have been widespread fears about the role hacking could play in affecting major sporting events, the above history suggests that those fears have largely been cabined to digital systems (like the electrical grid) and basic computing equipment (like websites and phones). Cybersecurity experts worried that those systems could be shut down or manipulated during an attack. But, because those systems were largely separate from the operation of the sporting event, officials haven't generally worried about how hackers could affect the integrity of the results, or how they might disrupt systems operating within the stadiums and other venues, thereby negatively affecting the experience of fans.

This will change—and quickly. The proliferation of the Internet of Things (IoT) is changing the face of the cybersecurity of sports, adding digital dimensions where there were none before. As we see in the sections that follow, digital technologies are being incorporated into every facet of the sporting experience, from scoring systems to athlete care, from 'smart' stadiums to device-enhanced viewing experiences for fans. Such trends include:

- The increased quantification of sports scoring systems, requiring detailed numerical scoring schemes;
- Video review that incorporates technology designed to aid in officials' decisions;
- Increased interest in data collection on athlete performance and training;
- The proliferation of devices in every aspect of sports facilities, from refrigerators to hair dryers;
- The growth in wearable devices and concomitant data tracking; and
- Increased viewer immersion in sports through technology, including virtual reality and drones.

The increased 'technification' of sports will continue, and even accelerate, over the next seven or so years. The remainder of this white paper considers how the Olympic movement can keep pace.

Headlines From the Future

False Fire Alarms Cause Mayhem in Major Olympics Hotels

Marriott, Hilton, and other major hospitality firms have all fallen prey to remote triggering of smoke alarms, sending athletes and dignitaries out into the streets in the wee hours.

Half of Paris Olympics Tickets Sold Online May Be Fake, Experts Say

From a bingo-parlor fraud run in churches across the U.S. South, to a complex online scam targeting major businesses across China, the sale of fake tickets to the 2024 Olympics has gone rampant.

Austrian Swimmer Allegedly Hired Hacker to Gain Access to Competitors' Email

Saying she wanted to be able to play "mind games" on her competition, distance swimmer Ingrid Schild confessed that she read her competitors' emails to unearth dirt, including details about their personal relationships and financial situations.

Counterfeiting and Credit Card Scams in Sale of Olympics Memorabilia

The advent of 3-D printer technologies has made it possible to print collectible pins on the spot—and several souvenir vendors have had their credit card systems hacked.

Event Screening Malware Found: Terrorist Threat Thwarted?

Security officials at the Paris Olympics discovered that a metal-detector had been hacked, possibly as part of a terrorist plot to smuggle guns and weapons into the stadium.

Air Cooling Hack at Qatar World Cup Raises Concerns About Olympics Security

A cooling system designed to use artificial intelligence to maximize efficiency ended up "hacking itself," according to officials familiar with the situation.

Hacked Drone Crashes, Disrupting Olympics Rowing Competition

Viewers watching on television and livestream saw their perspective grow closer and closer to the rowers—before the drone plummeted into the water. A "remote digital control" had taken over the camera, according to NBC. The race—a semi-final heat—had to be rescheduled for tomorrow.

METHODS

Over a six-month period, a research team led by Betsy Cooper, Executive Director of the UC Berkeley Center for Long-Term Cybersecurity (CLTC), together with student assistants Zoe Feist and Katie Chen, studied the cybersecurity of major Olympic sporting events, through literature reviews, more than a dozen informational interviews, and observation of nearly 10 major sporting events. The team partnered with Cal Athletics, a suitable choice not only because of the wide diversity of sports represented, but because UC Berkeley sent 50 Olympic athletes to the Rio Olympics in 2016—more than any other university. The findings here belong to the research team and do not reflect the position of Cal Athletics or of any other party.

This project also draws elements from future-oriented methodologies that we have employed at CLTC before: fictional storytelling.[30] This piece extrapolates future-leaning trends in order to identify where potential sources of change will become most visible and what opportunities and challenges arise as a result. To help bring to life those changes, we incorporate fictional stories, written by Chuck Kapelke, that share possible future examples of what the cybersecurity of sports could someday look like. These stories are not intended to predict the future, but rather to illustrate the range of possibilities that might someday develop.

Please note that the types of hacking incidents outlined above—ticket scams, website defacements, etc.—are unlikely to decrease, but because those threats are already well recognized, our analysis below focuses largely on new attack vectors.

Analysis: Cybersecurity Risks of Major Sporting Events

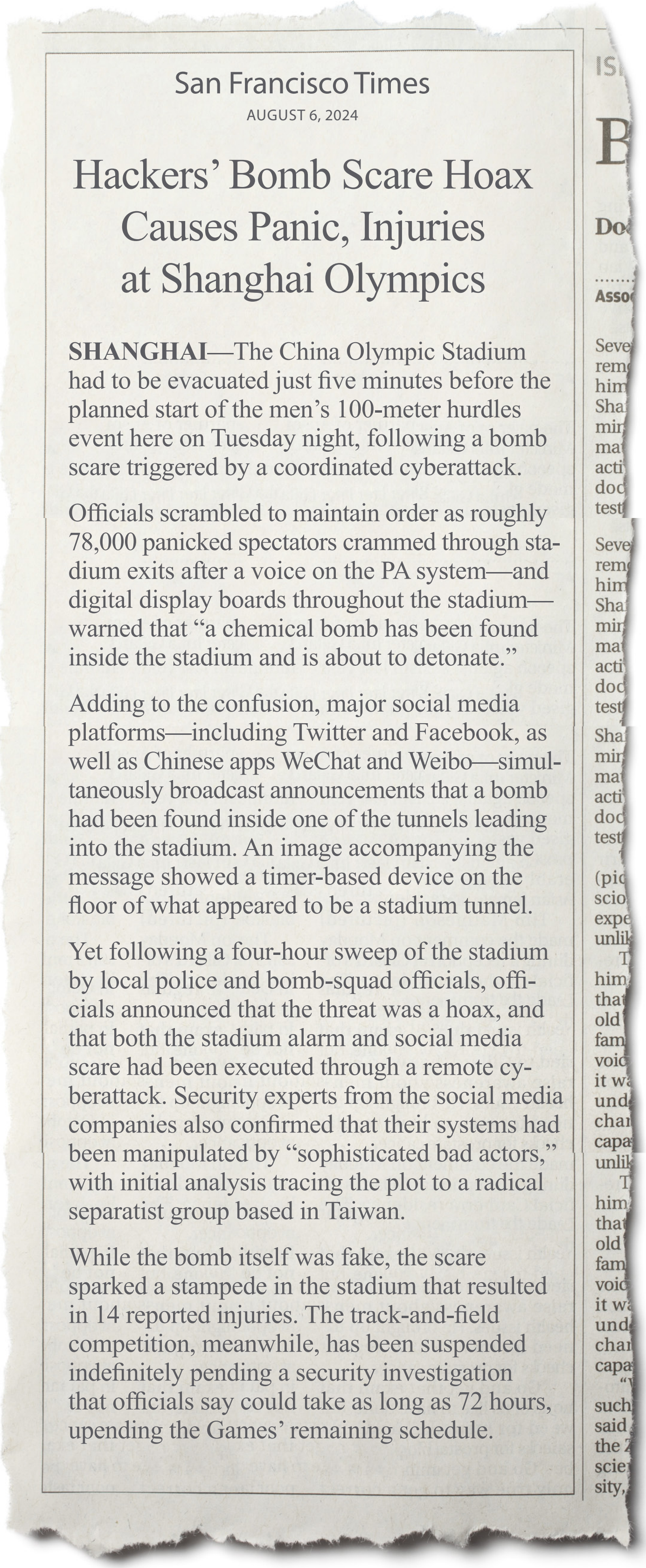
PHYSICAL INTEGRITY

The most serious potential cyberattacks at major sporting events are those that could lead to bodily harm for spectators, athletes, officials, or other attendees. In general, such attacks are exceedingly rare, and they often rely on targeting physical infrastructure—security systems, transportation, medical devices, etc.—that are designed to protect human lives.

While it is imaginable that digital devices could be manipulated to facilitate physical harm—for instance, a body scanner could be hacked to allow a terrorist with weapons into a venue, or a runaway transportation vehicle could be controlled remotely to kidnap or hurt athletes or spectators—such incidents are unlikely as they require a high degree of sophistication, and because there are relatively few touch points within the event through which such effects could be achieved. Even so, especially were such a hack to be coordinated across multiple locations, the results could indeed be devastating.

More likely, spectators or athletes could incur physical harm as a result of panic-causing events caused by an illicit system breach. For instance, a networked digital display board in a stadium could be hacked to alert fans to a terrorist threat, broadcasting a message that they should exit as quickly as possible. Even if the alert was false, the ensuing panic would be likely to cause physical injury to spectators rushing to leave the stadium. (Such a hack is not without precedent; numerous traffic signs have been hacked to display offensive and misleading content.[31] However, those hacks have been largely innocuous to date.)

Note that, for each of these cases—terrorist attack, motor vehicle accident, or crowd crush—the risk predates the advent of digital technologies. All of these incidents could occur today, even absent digital intervention. What the hack does is to interfere with a traditional security point (security scanner; car driver; emergency exits), removing a protection against physical harm that could not so easily be manipulated in the analog age.



San Francisco Times

AUGUST 6, 2024

Hackers' Bomb Scare Hoax Causes Panic, Injuries at Shanghai Olympics

SHANGHAI—The China Olympic Stadium had to be evacuated just five minutes before the planned start of the men's 100-meter hurdles event here on Tuesday night, following a bomb scare triggered by a coordinated cyberattack.

Officials scrambled to maintain order as roughly 78,000 panicked spectators crammed through stadium exits after a voice on the PA system—and digital display boards throughout the stadium—warned that "a chemical bomb has been found inside the stadium and is about to detonate."

Adding to the confusion, major social media platforms—including Twitter and Facebook, as well as Chinese apps WeChat and Weibo—simultaneously broadcast announcements that a bomb had been found inside one of the tunnels leading into the stadium. An image accompanying the message showed a timer-based device on the floor of what appeared to be a stadium tunnel.

Yet following a four-hour sweep of the stadium by local police and bomb-squad officials, officials announced that the threat was a hoax, and that both the stadium alarm and social media scare had been executed through a remote cyberattack. Security experts from the social media companies also confirmed that their systems had been manipulated by "sophisticated bad actors," with initial analysis tracing the plot to a radical separatist group based in Taiwan.

While the bomb itself was fake, the scare sparked a stampede in the stadium that resulted in 14 reported injuries. The track-and-field competition, meanwhile, has been suspended indefinitely pending a security investigation that officials say could take as long as 72 hours, upending the Games' remaining schedule.

INTEGRITY OF THE SPORTING FACILITY

The second category of attacks includes those that interfere with the integrity of the sporting facility, but fall short of causing physical harm to athletes or spectators. In these cases, the main loss is to the sporting event itself, as the event will not be able to go off as planned.

First are attacks to the physical facilities themselves. As with the London Games, the electric grid losing power remains a serious concern, albeit a well-protected one. Other key maintenance systems—for example, heating/cooling or plumbing systems—could similarly be affected to prevent an event from taking place. These vectors of attack exist now, but are likely to expand as facilities systems are increasingly digitized. Adding to the challenge, these systems are in many cases controlled not by the facilities themselves, but by outside contractors. In the well-known breach of payment systems at Target, hackers gained access not through Target systems per se, but through the systems of one of their vendors: a provider of remotely controllable HVAC systems. That same vendor was also used in the Sochi Olympic Games.[32]

Other potential threats to physical infrastructure relate to the use of new technologies for other aspects of sporting events, such as scoring and viewership. For instance, camera-enabled drones were used during the Rio Olympics to provide television coverage along lengthy rowing tracks.[33] (The previous Olympics required wire to be hung across the 2,000 meter course to support a roving camera.) A hacked drone could, however, cause serious physical damage to athletes or spectators. Technologies to stop rogue drones are already under development.[34]

Another area strongly trending in the digital direction is ticketing and payment in major sporting facilities. Increasingly, ticketing is bundled with payment mechanisms for retail into a wearable electronic device. One of the pioneers in this space is Disney, which now offers MagicBands—wristbands that electronically give access to the amusement park, hotel, and merchandise.[35] Such payment schemes are likely to proliferate in the next few years because they facilitate the payment process.

At the same time, because these devices and their back-end systems consolidate several potentially valuable targets—credentials to gain access to events, purchasing power, access to priority facilities—they also pose a strong temptation for hackers. Some of these risks are relatively minor; for instance, if a single band with valuable seats were hacked to duplicate access credentials, the main loss would occur in compensating the harmed consumer. However, the back-end system hosting the bands could also be manipulated to impede entry into the facility for all attendees. Imagine the queue outside the Olympic opening ceremonies if the bands distributed for access all simultaneously failed. Who would be able to prove that they legitimately deserved entry?

A further risk in this category relates to transportation systems used to bring people to and from event venues. Modern cars are increasingly digitized—and hackable as a result. One recent report even showed how a Chevy Volt could be hacked to allow the steering wheel to control the old-school Mario Kart video game.[36] Autonomous driving vehicles will exacerbate the risk of hacked transportation systems, largely because a human driver would be more likely to notice that a vehicle was not responding to controls. Hacked transportation, especially as systems are consolidated in a small set of providers (such as Uber and Lyft), could disrupt or delay events. While events would likely proceed if fan transportation were disrupted, the same would not be true if the athletes were affected.

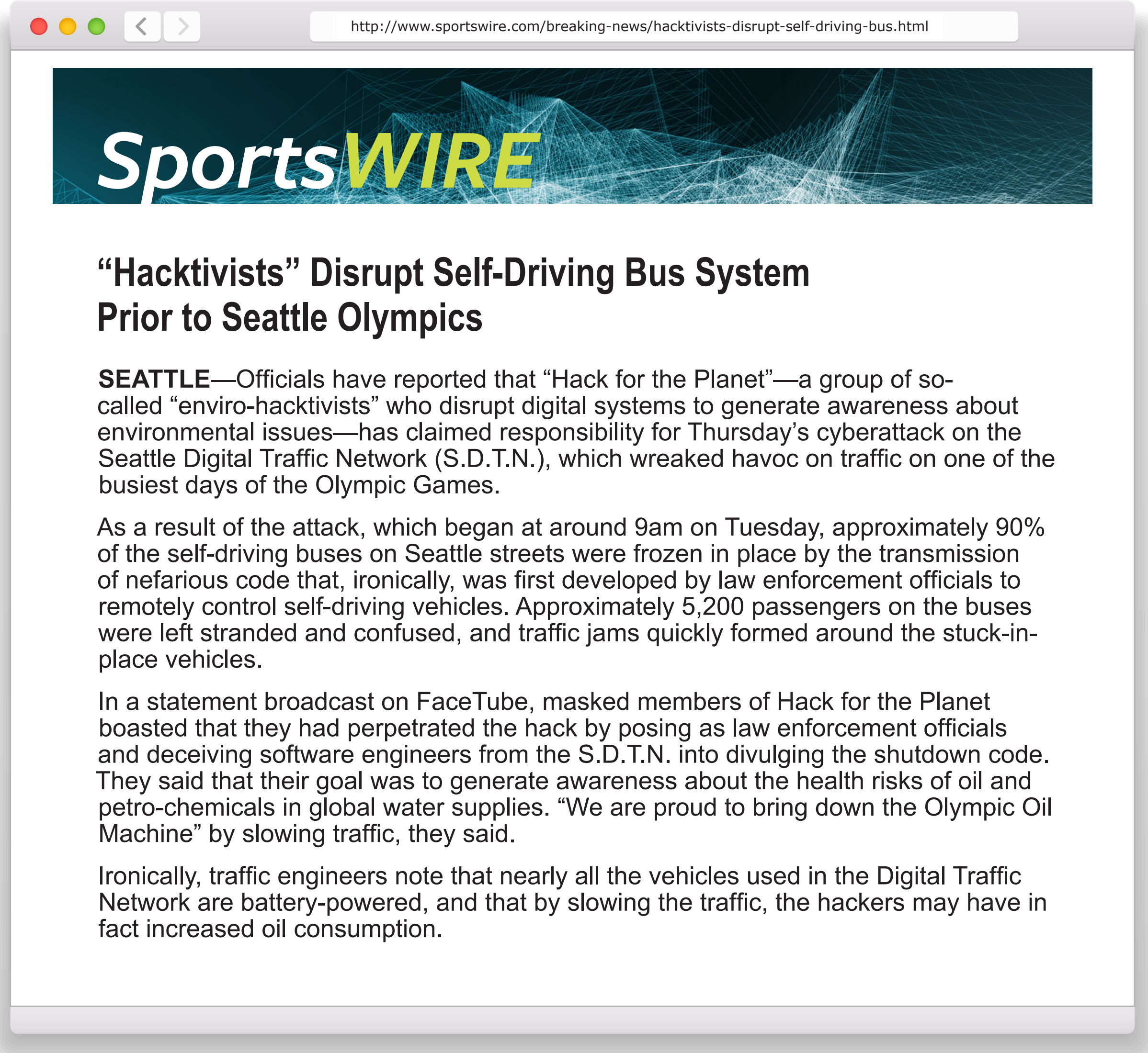
INTEGRITY OF THE SPORT

The third category—the threat of a cyberattack affecting the integrity of a sporting event—cuts to the heart of the Olympic movement. Could technology make it more likely that sports results will be questioned in the future? This section reviews the possibilities, looking at hacks in scoring and game play, video replay, and athlete care.

Scoring and Game Play

In many sports, scoring and game play involve digital systems that play an important role in determining the outcome of the match. Most familiar here are digital scoring systems that control time-based events like swimming, track, and rowing. Timing boards to track swimmers' turns, and to automatically track when a runner has crossed the line, are increasingly common, and represent a possible vulnerability. International swimming rules now explicitly allow for the use of automatic systems to determine results, and provide that the automatic system's times shall be final unless it has been determined to have failed.[37]

Were long-distance events to consider incorporating GPS tracking into the timing system, this could represent an additional vulnerability; GPS has already been spoofed to misdirect ships in the open water.[38] (Olympic sports such as sailing and rowing already use GPS to help monitor boat locations.[39])


http://www.sportswire.com/breaking-news/hacktivists-disrupt-self-driving-bus.html
SportsWIRE

"Hacktivists" Disrupt Self-Driving Bus System Prior to Seattle Olympics

SEATTLE—Officials have reported that "Hack for the Planet"—a group of so-called "enviro-hacktivists" who disrupt digital systems to generate awareness about environmental issues—has claimed responsibility for Thursday's cyberattack on the Seattle Digital Traffic Network (S.D.T.N.), which wreaked havoc on traffic on one of the busiest days of the Olympic Games.

As a result of the attack, which began at around 9am on Tuesday, approximately 90% of the self-driving buses on Seattle streets were frozen in place by the transmission of nefarious code that, ironically, was first developed by law enforcement officials to remotely control self-driving vehicles. Approximately 5,200 passengers on the buses were left stranded and confused, and traffic jams quickly formed around the stuck-in-place vehicles.

In a statement broadcast on FaceTube, masked members of Hack for the Planet boasted that they had perpetrated the hack by posing as law enforcement officials and deceiving software engineers from the S.D.T.N. into divulging the shutdown code. They said that their goal was to generate awareness about the health risks of oil and petro-chemicals in global water supplies. "We are proud to bring down the Olympic Oil Machine" by slowing traffic, they said.

Ironically, traffic engineers note that nearly all the vehicles used in the Digital Traffic Network are battery-powered, and that by slowing the traffic, the hackers may have in fact increased oil consumption.

Given the extensive scrutiny and televised records of Olympic events, as well as duplicated timing systems used in major events,[40] a hacker would be unlikely to change results of final scores in a major Olympic final. However, less heavily scrutinized results—Olympic Games qualifiers, for instance, or heats that do not include top contenders—might be ripe for gamblers seeking to make a quick buck on the results.

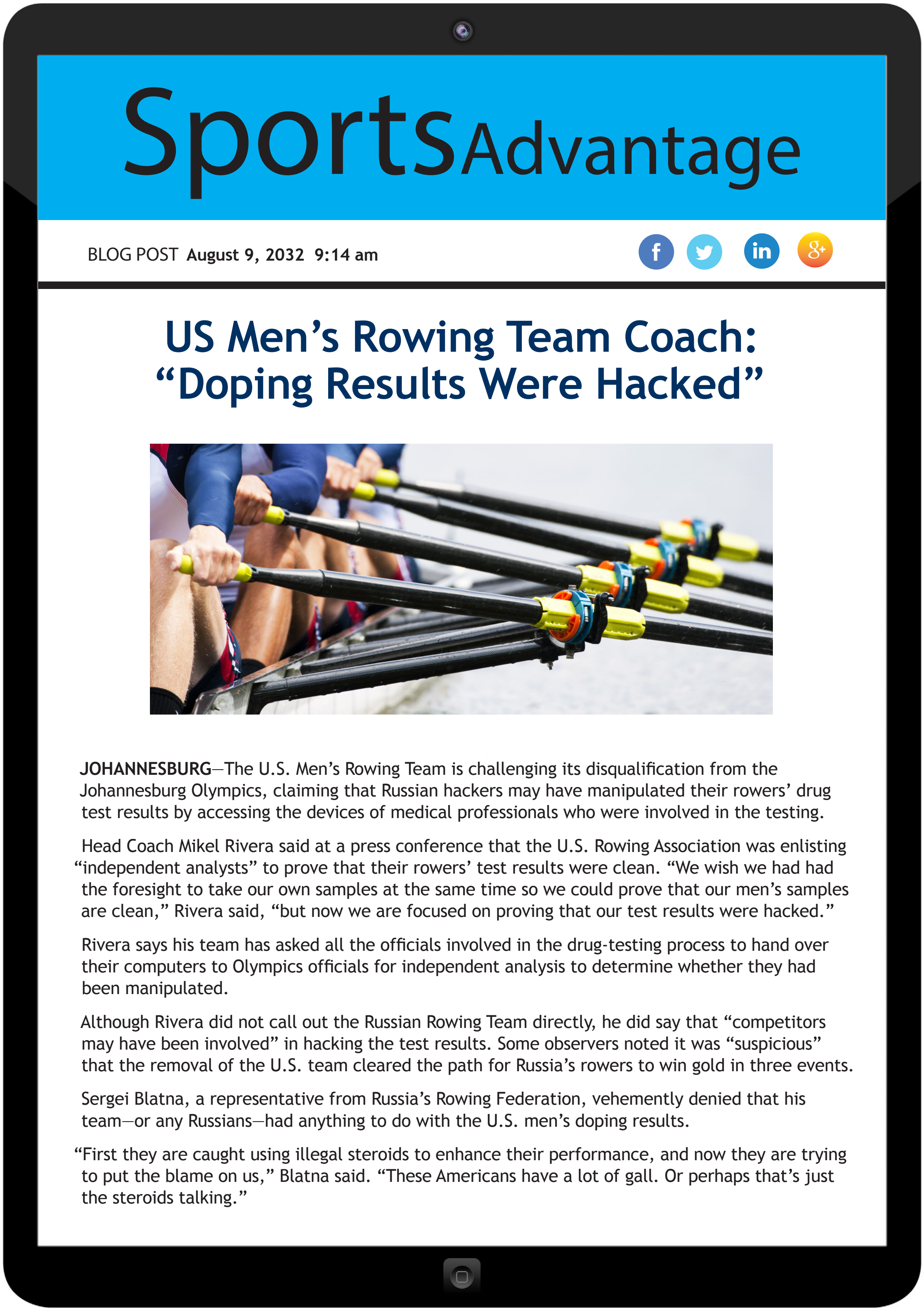
Measured scoring events represent another potential vulnerability. Consider field events such as discus. While historically the distance of a throw was measured using a simple string or measuring tape, companies such as FinishLynx have introduced laser-based measurement systems, accompanied by software, that claim to provide more accurate readings. Such measurement systems have been used at world championships.[41]

RFID-embedded tracking represents another potential method for tracking distances for discus, javelin, and other throwing sports. RFID technology has already become a staple for tracking race results in cycling and cross country. While we found no evidence that such tracking devices are already in use in throwing events, the temptation to use such technology in the future will likely not abate. The systems used to transfer and store readings from such devices could present a temptation for hackers.

In other Olympic sports, electronic devices may not be used to decide the overall result of an event, but nevertheless may support refereeing decisions that could ultimately determine the winner. The Hawk-Eye example from tennis, noted above, is one such example. Hawk-Eye does not choose the winner of a tennis match, but it does determine the outcome of certain points, and where the referee and Hawk-Eye disagree, the digital judge will always come out on top.

Although team sports were not the focus of this review, it is worth noting that scoring and timekeeping in such sports can play a significant role in determining the outcome. For instance, in water polo, timeouts are very carefully used and can only be called when the coach's team has possession; otherwise, the other team gets a valuable penalty shot. In the 2012 Olympics, the United States' women's team erroneously called such a timeout, leading to a penalty goal that brought their match to overtime.[42] An electronic system for calling timeouts could help resolve ambiguity in determining when a timeout is called, but could also create a tempting vulnerability for those interested in the outcome. (Who would believe a coach who said he had not pressed the button to call a timeout when the electronic system registered that he did?) Similar concerns could be raised in basketball, in relation to both timeouts and the shot and game clocks; if the shot clock were to run one tenth of a second faster for one team than another, who would be able to tell?

Finally, in addition to directly scoring performance, technology plays a useful role in helping officials determine whether an athlete should remain in competition or be disqualified. False starts and lane line violations all depend on the ability of a human to tell whether a competitor has moved in an improper way. Olympic events already have adopted technology for registering false starts;[43] while such systems have generally been disconnected from the internet to reduce risk of tampering, hackers seeking a particular race outcome may try to manipulate these systems to report an errant false start.



SportsAdvantage

BLOG POST **August 9, 2032 9:14 am**

US Men’s Rowing Team Coach: “Doping Results Were Hacked”

JOHANNESBURG—The U.S. Men’s Rowing Team is challenging its disqualification from the Johannesburg Olympics, claiming that Russian hackers may have manipulated their rowers’ drug test results by accessing the devices of medical professionals who were involved in the testing.

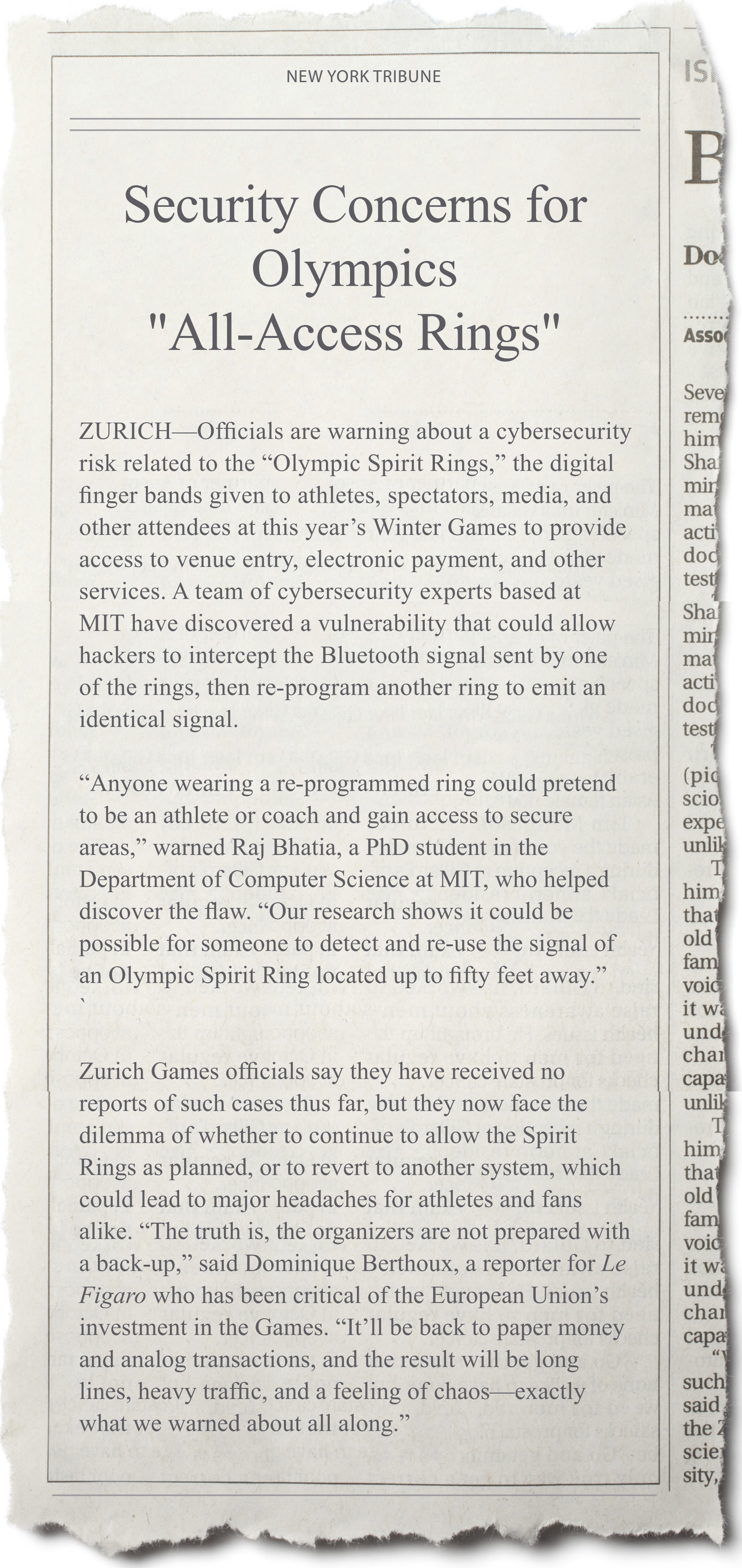
Head Coach Mikel Rivera said at a press conference that the U.S. Rowing Association was enlisting “independent analysts” to prove that their rowers’ test results were clean. “We wish we had had the foresight to take our own samples at the same time so we could prove that our men’s samples are clean,” Rivera said, “but now we are focused on proving that our test results were hacked.”

Rivera says his team has asked all the officials involved in the drug-testing process to hand over their computers to Olympics officials for independent analysis to determine whether they had been manipulated.

Although Rivera did not call out the Russian Rowing Team directly, he did say that “competitors may have been involved” in hacking the test results. Some observers noted it was “suspicious” that the removal of the U.S. team cleared the path for Russia’s rowers to win gold in three events.

Sergei Blatna, a representative from Russia’s Rowing Federation, vehemently denied that his team—or any Russians—had anything to do with the U.S. men’s doping results.

“First they are caught using illegal steroids to enhance their performance, and now they are trying to put the blame on us,” Blatna said. “These Americans have a lot of gall. Or perhaps that’s just the steroids talking.”



NEW YORK TRIBUNE

Security Concerns for Olympics "All-Access Rings"

ZURICH—Officials are warning about a cybersecurity risk related to the “Olympic Spirit Rings,” the digital finger bands given to athletes, spectators, media, and other attendees at this year’s Winter Games to provide access to venue entry, electronic payment, and other services. A team of cybersecurity experts based at MIT have discovered a vulnerability that could allow hackers to intercept the Bluetooth signal sent by one of the rings, then re-program another ring to emit an identical signal.

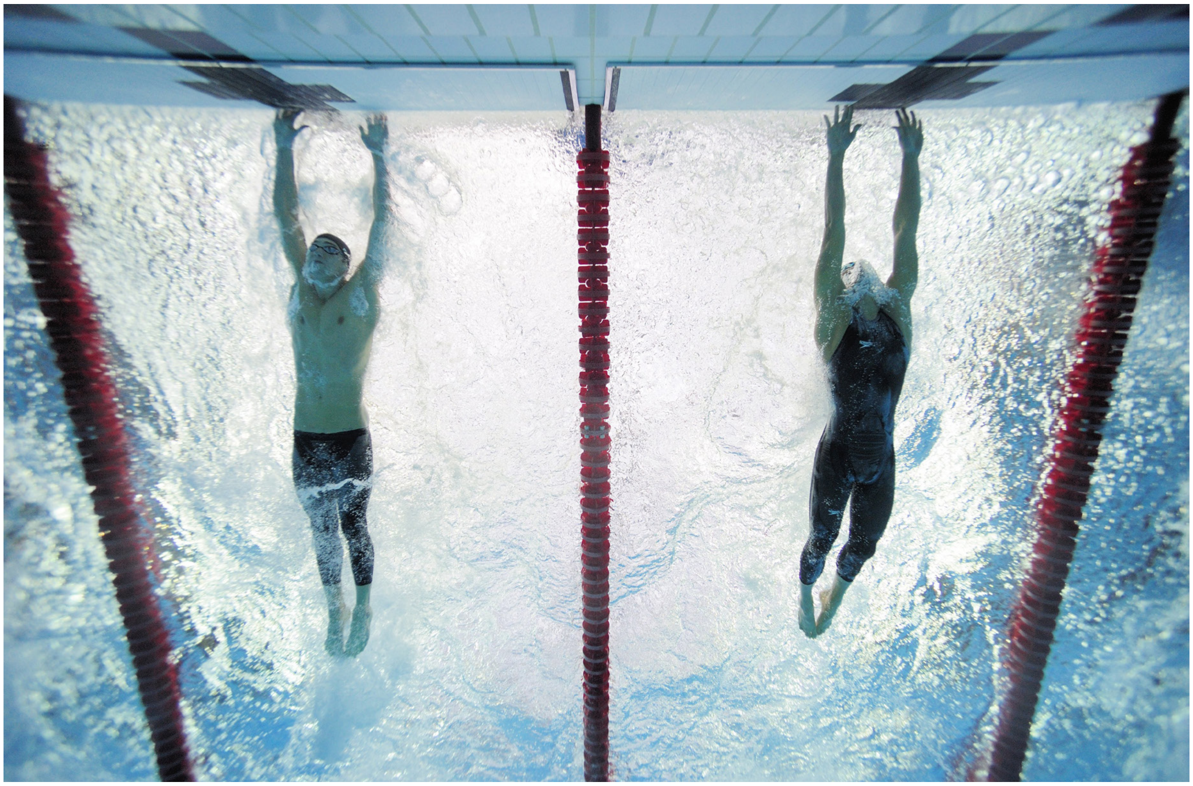
“Anyone wearing a re-programmed ring could pretend to be an athlete or coach and gain access to secure areas,” warned Raj Bhatia, a PhD student in the Department of Computer Science at MIT, who helped discover the flaw. “Our research shows it could be possible for someone to detect and re-use the signal of an Olympic Spirit Ring located up to fifty feet away.”
`

Zurich Games officials say they have received no reports of such cases thus far, but they now face the dilemma of whether to continue to allow the Spirit Rings as planned, or to revert to another system, which could lead to major headaches for athletes and fans alike. “The truth is, the organizers are not prepared with a back-up,” said Dominique Berthoux, a reporter for *Le Figaro* who has been critical of the European Union’s investment in the Games. “It’ll be back to paper money and analog transactions, and the result will be long lines, heavy traffic, and a feeling of chaos—exactly what we warned about all along.”

Scoring Aids

In many cases, technology is used not to make the final scoring determinations, but to assist judges as they draw conclusions about the results. In most Olympic sports, the increased use of technology as a scoring aid has increased steadily, if not at a breakneck pace. Consider photo finish systems in track and field. Unlike in swimming, where the touchpad automatically posts the winner, referees in track races still retain control of the outcome. In close races, the referees use a photo finish system, by which repeated and stretched photographs reveal the spread of the runners, but the referee still measures the first moment at which the torso crosses, and thus makes the final decision. While moving photographs would be extremely difficult to doctor in real time, in cases where several athletes consistently race a similar level, it might be possible for a hacker to replace the real photograph with one prepared in advance—or to delete the real race photo data altogether. Even without changing the outcome directly, an incorrect or missing photo could sow doubts in the overall results.

The most difficult cases involve extremely close races. Take Michael Phelps's victory against Milorad Cavic:



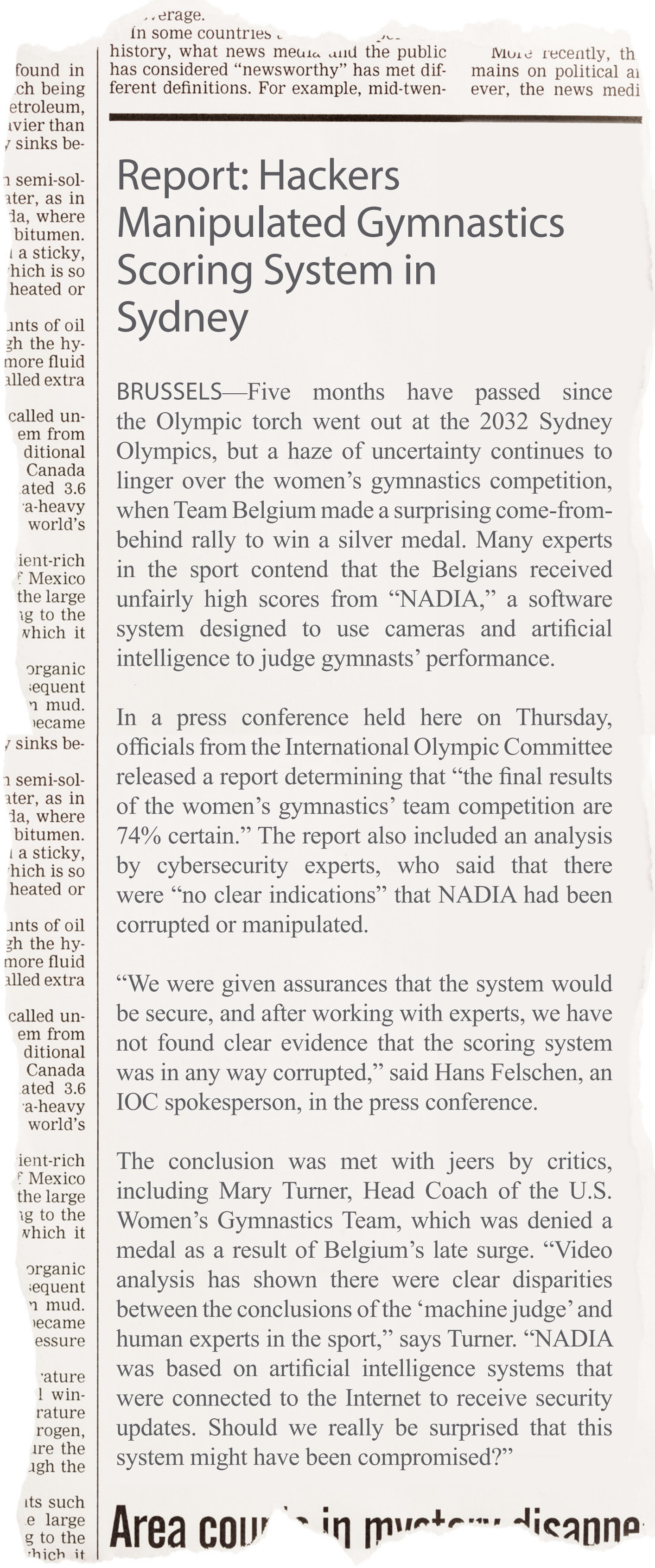
Phelps appears on the left, and Cavic on the right. To many at the time of the race, it appeared in video that Cavic touched first. Nevertheless, the touch pad used in the race apparently determined that Phelps touched first. As officials made clear at the time, the touchpad "is the primary source to determine the race winner, while the photos can only be used as backup material."[44]

One exception to the trend of using scoring aids can be found in sports that are subjectively judged, such as gymnastics. In gymnastics, there are two sets of judges: one determines the difficulty of the routine based on a list of predefined moves, and the other judges s the execution of the routine, taking deductions for balance and form breaks, and other flaws. Outside the use of simple video-based replay to help judges review how skills were performed, and a wired system to transmit scores to a central computer, technology has not significantly changed the way gymnastics is judged.

Over the next seven years, it is possible that technology will evolve to automate both portions of the gymnastics scoring process. First, video recognition software is increasingly able to distinguish different types of content; Wimbledon already employed a type of content-distinguishing technology to help fans better follow game play in 2017.[45] Such software could eventually be deployed to distinguish key gymnastics moves from each other (e.g., a single twist vs. a double twist).

Second, digital technologies could be used to identify form breaks and rate errors; in other words, it could score the routine based on the degree to which a gymnast's move departs from an ideal. Imagine a gymnastics judge deducting points based on the insufficient height of a jump above the balance beam. A computer might be better positioned than a human judge to make such a measurement and/or compare it to other athletes. Gymnastics officials have already reported that they plan to pilot 3-D laser software as a scoring aid at the 2020 Tokyo Olympics.[46]

Of course, many will have deep reservations about incorporating such a system. Not least, gymnastics is a sport founded on artistry, and it is (for now) unclear how a computerized scoring system could take this into account. But cybersecurity risks are also a significant concern. Because a computerized system would contain so many individual moves and judgments made over a very short period of time, it would be relatively easy for a hacker to change some of the scoring values without being detected. (The more individual judgments or 'touch points' that are possible to be changed, the higher opportunity for manipulation, and the less likely any changes will be detected; this is why it is less likely that a hacker could successfully alter a timed swimming result than an automated gymnastics score.)



..erage.
In some countries ...
history, what news media and the public has considered "newsworthy" has met different definitions. For example, mid-twen-

More recently, th
mains on political a
ever, the news medi

found in
ch being
etroleum,
vier than
sinks be-

semi-sol-
ter, as in
da, where
bitumen.
a sticky,
hich is so
heated or

unts of oil
gh the hy-
more fluid
alled extra

called un-
em from
ditional
Canada
ated 3.6
a-heavy
world's

ient-rich
Mexico
the large
ng to the
which it

organic
sequent
mud.
became
sinks be-

semi-sol-
ter, as in
da, where
bitumen.
a sticky,
hich is so
heated or

unts of oil
gh the hy-
more fluid
alled extra

called un-
em from
ditional
Canada
ated 3.6
a-heavy
world's

ient-rich
Mexico
the large
ng to the
which it

organic
sequent
mud.
became
essure

ature
l win-
rature
rogen,
ure the
ugh the

its such
e large
g to the
hich it

Report: Hackers Manipulated Gymnastics Scoring System in Sydney

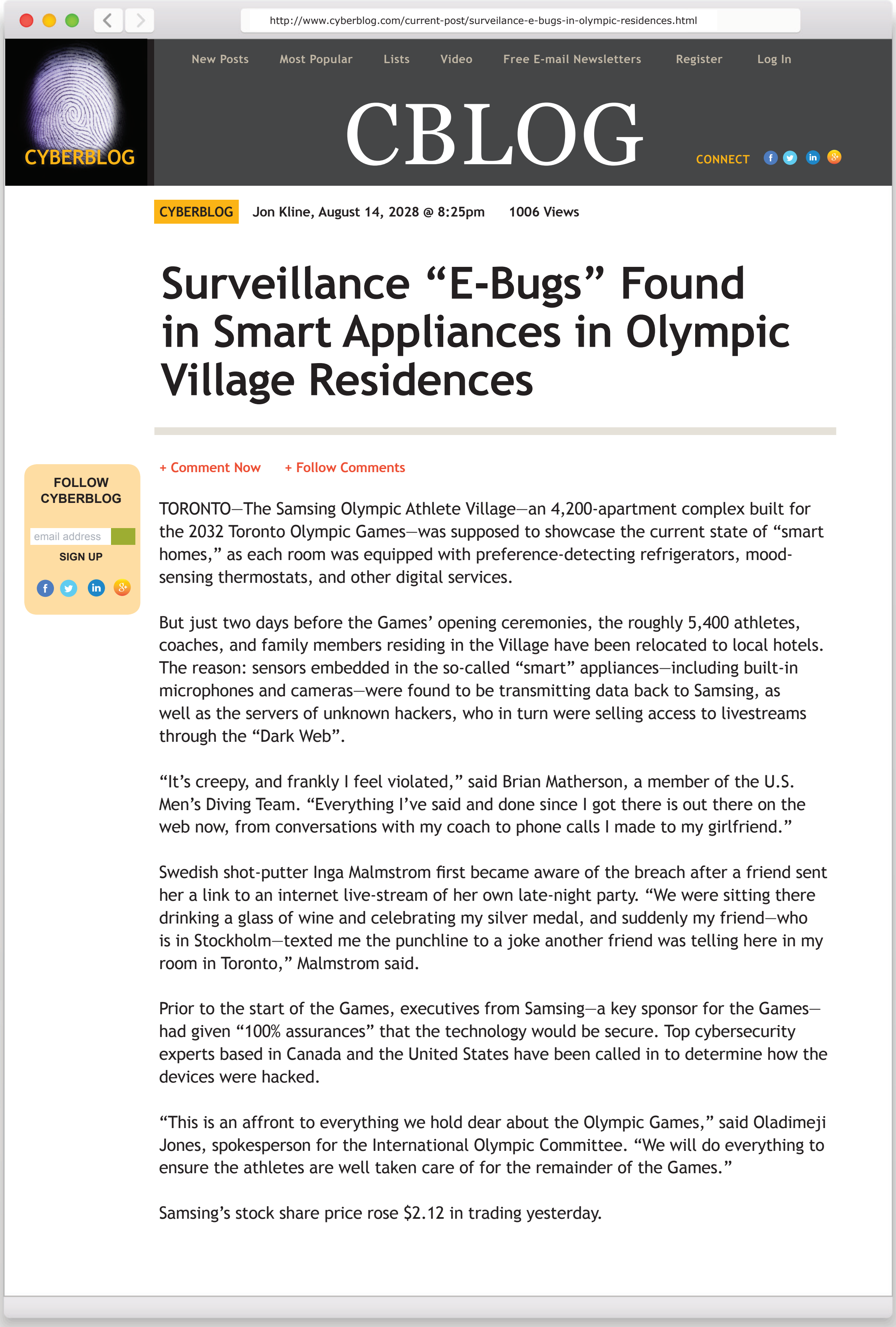
BRUSSELS—Five months have passed since the Olympic torch went out at the 2032 Sydney Olympics, but a haze of uncertainty continues to linger over the women's gymnastics competition, when Team Belgium made a surprising come-from-behind rally to win a silver medal. Many experts in the sport contend that the Belgians received unfairly high scores from "NADIA," a software system designed to use cameras and artificial intelligence to judge gymnasts' performance.

In a press conference held here on Thursday, officials from the International Olympic Committee released a report determining that "the final results of the women's gymnastics' team competition are 74% certain." The report also included an analysis by cybersecurity experts, who said that there were "no clear indications" that NADIA had been corrupted or manipulated.

"We were given assurances that the system would be secure, and after working with experts, we have not found clear evidence that the scoring system was in any way corrupted," said Hans Felschen, an IOC spokesperson, in the press conference.

The conclusion was met with jeers by critics, including Mary Turner, Head Coach of the U.S. Women's Gymnastics Team, which was denied a medal as a result of Belgium's late surge. "Video analysis has shown there were clear disparities between the conclusions of the 'machine judge' and human experts in the sport," says Turner. "NADIA was based on artificial intelligence systems that were connected to the Internet to receive security updates. Should we really be surprised that this system might have been compromised?"

Area cou... in myst... disappe...



CYBERBLOG Jon Kline, August 14, 2028 @ 8:25pm 1006 Views

Surveillance "E-Bugs" Found in Smart Appliances in Olympic Village Residences

TORONTO—The Samsing Olympic Athlete Village—an 4,200-apartment complex built for the 2032 Toronto Olympic Games—was supposed to showcase the current state of "smart homes," as each room was equipped with preference-detecting refrigerators, mood-sensing thermostats, and other digital services.

But just two days before the Games' opening ceremonies, the roughly 5,400 athletes, coaches, and family members residing in the Village have been relocated to local hotels. The reason: sensors embedded in the so-called "smart" appliances—including built-in microphones and cameras—were found to be transmitting data back to Samsing, as well as the servers of unknown hackers, who in turn were selling access to livestreams through the "Dark Web".

"It's creepy, and frankly I feel violated," said Brian Matherson, a member of the U.S. Men's Diving Team. "Everything I've said and done since I got there is out there on the web now, from conversations with my coach to phone calls I made to my girlfriend."

Swedish shot-putter Inga Malmstrom first became aware of the breach after a friend sent her a link to an internet live-stream of her own late-night party. "We were sitting there drinking a glass of wine and celebrating my silver medal, and suddenly my friend—who is in Stockholm—texted me the punchline to a joke another friend was telling here in my room in Toronto," Malmstrom said.

Prior to the start of the Games, executives from Samsing—a key sponsor for the Games—had given "100% assurances" that the technology would be secure. Top cybersecurity experts based in Canada and the United States have been called in to determine how the devices were hacked.

"This is an affront to everything we hold dear about the Olympic Games," said Oladimeji Jones, spokesperson for the International Olympic Committee. "We will do everything to ensure the athletes are well taken care of for the remainder of the Games."

Samsing's stock share price rose $2.12 in trading yesterday.

If the outcomes determined by software-based scoring were called into question, it would be very difficult to restore trust in the integrity of the system afterward. In the vaulting horse error during the 2000 Sydney Olympics, when the apparatus was set to an incorrect height, the officials needed only to adjust the horse height to restore integrity. But if the electronic judging system itself were compromised, it would be nearly impossible to detect what happened—and how to fix it.

Athlete Care

The above analysis focuses on efforts to modify the scoring of athletic events, either directly or by influencing the decisions of officials. But there is another way that a lack of sufficient cybersecurity could compromise the integrity of major sporting events: by affecting the performance of the athletes.

In the sports we studied, we were unable to identify any way in which a cybersecurity attack could directly affect athlete performance during the event (although we did identify ways that athletes could in theory cheat using technology; for instance, a swimmer could wear an electronic device that would help her track and maintain her stroke rate). We did, however, identify a method by which a hacker could affect an athlete's performance outside the context of competition: by manipulating items consumed by athletes, such as nutrition and medical care.

Automated food systems are becoming increasingly commonplace. A California startup food chain, Eatsa, now dispenses food bowls and salads through an exchange in which everything except the actual cooking is automated.[47] And automated cooking may not be far off; a new device called 'Sally the Salad Robot' can make 1,000 salad variations in a minute each. Over the next 5-10 years, the increased automation of food production—especially the repetitive pieces of the job—is only likely to increase.[48]

Couple this trend with the fact that athletes often carefully regulate what they consume, and athlete nutrition systems are likely to play an important part in future Olympic Games. Take protein shakes. Products such as the Weider Pro Shake Machine can store multiple protein shake variations,[49] allowing athletes to customize their consumption according to their nutritionists' detailed specifications. Add electronic connectivity, and such devices will be easily programmable to meet the specific needs of large teams of athletes.

At the same time, such automated systems create a tempting opportunity for hackers seeking to interfere with events results. Imagine the world's top rower is set to compete in the Olympic women's eight final, and a recently published magazine profile reveals that she has a gluten allergy. Each day before her workout, she consumes a protein shake. A malicious actor favoring one of her top competitors could hack into the automatic protein dispensing system, ensuring that gluten is dispensed into the shake. She will not achieve her top performance—and may not be able to compete at all.

FINANCIAL RISK: TICKETING AND RETAIL

Each of the attacks noted so far, in addition to disturbing the integrity of the sport and the venues in which they occur, could have serious financial repercussions. In addition, some potential attacks are more directly targeted at financial gains. Some of these attacks, such as bogus sporting websites and ticket scams, are already well known in 2017. These are likely to continue into the future, but the mechanisms for achieving them are unlikely to change significantly.

We also identified several vectors of additional financial risk. One such threat is based on the tendency of electronic systems to consolidate desirable assets into a single electronic system. One example is the consolidated payment and ticketing systems noted earlier, like the Disney SmartBand. In addition to the risks identified earlier, such systems could be exploited to collect consolidated financial details of customers. Because each attendee would be required to use the band for ticketing, if the system were infiltrated, it would be easier for hackers to collect payment details for multiple users simultaneously. Today, the risk would be limited to those using electronic payment methods at the event, and the risk would vary depending on the type of payment used.

Other potential vectors for cyberattack can be found in the retail sector. One newly developed technology allows shoppers to make purchases without using a check-out machine; both Amazon and Walmart are currently piloting such technology.[50] Again, as long as the system remains protected, no problems will occur. But because such systems require the storage of payment information, they could represent a tempting target for hackers.

Key Olympic Sports Trends

Over the course of our review, we identified both likely trends for the increased digitization of major sporting events, and some game-changers that might come to light in the decades that follow.

GYMNASTICS

Key Trends:
Artificial intelligence in scoring

Possible Surprises:
Embedded tracking in gymnastics equipment

SWIMMING

Key Trends:
Automated start/finish technology

Possible Surprises:
Biometrics in swimsuits

ROWING

Key Trends:
Drones above race; GPS tracking of boats

Possible Surprises:
Virtual reality real-time viewing

TRACK

Key Trends:
Automatic field event measurement

Possible Surprises:
3D images for track finishes

REPUTATIONAL RISK: VIEWING EXPERIENCE

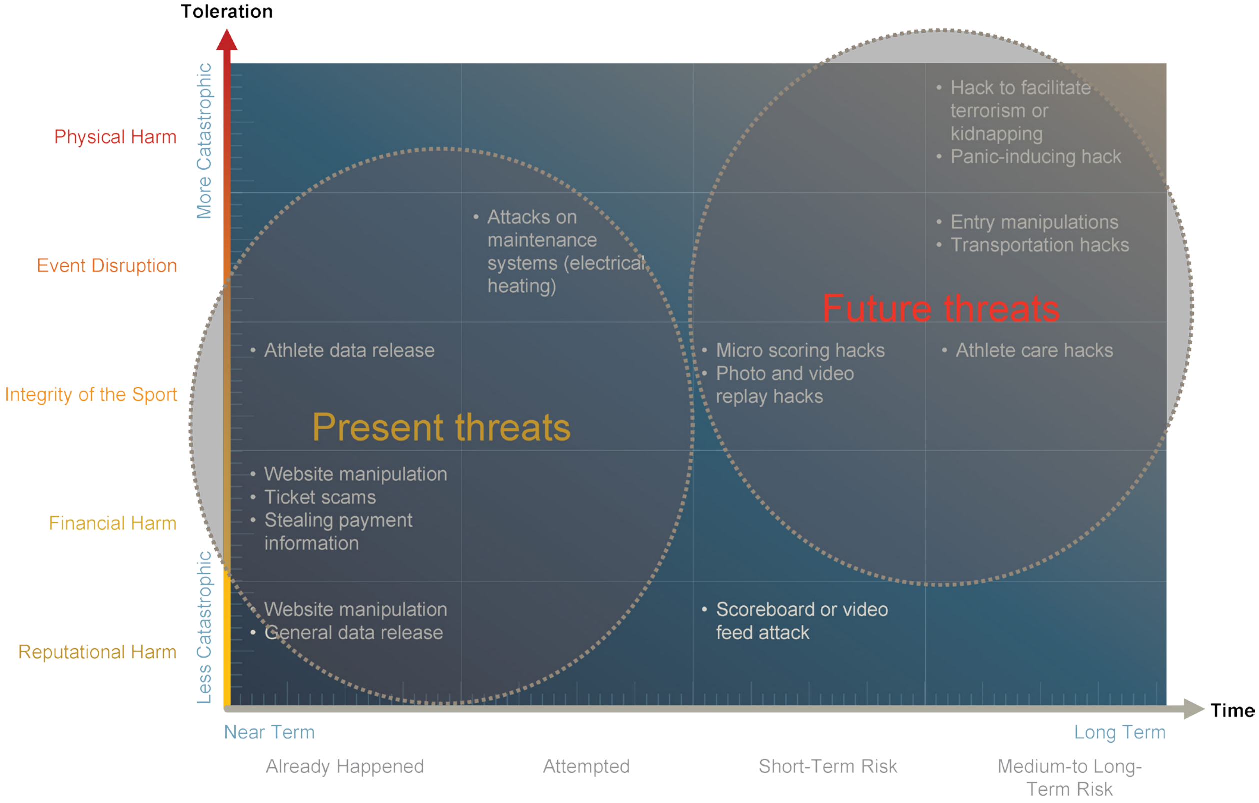
The final type of cybersecurity risk is reputational: even without causing physical or financial damage, hackers could inflict significant harm on the reputation of a high-profile event. For major sporting events, one significant area of reputational interest is the home viewer. Hacking activities in the stadium, unless broadcast more widely, only affect those in the stadium. It is the ability to share the Olympic experience with millions of people at home that gives the sport system its tremendous reach. To take a trite example, if a hacker put an obscene statement on a stadium visual display, it would only affect those in the stadium—at least until an attendee puts it on Twitter.

As the viewing practices of major sporting events audiences change, so will opportunities for hackers to alter what those viewers experience. For instance, virtual reality systems are already assisting major sports teams like the New York Giants in understanding their playing environment.[51] And many suspect that virtual reality will provide the next great viewing experience, by allowing spectators at major sporting events to experience the event from the perspective of the official or even the athlete. (Not least, such an experience might allow differential pricing even for the home viewer, who would pay a premium for this more desirable view.) Yet because such a 3D-based system exposes viewers to so many different views simultaneously, it will be difficult to identify when something nefarious has appeared on screen, whereas with a single TV feed, a producer can quickly tell that something has gone awry. With hundreds or thousands of simultaneous 360 degree views, catching an obscene message will be far harder.

SUMMARY

In brief, this review suggests that while existing cybersecurity breaches—which are mostly concentrated in the financial risk category—are likely to continue, a new wave of attacks are also likely to occur. The below chart shows the attacks that new technologies will make possible (or at least more likely).

TOLERATION OF ATTACKS BY TIME: FUTURE EVIDENCE

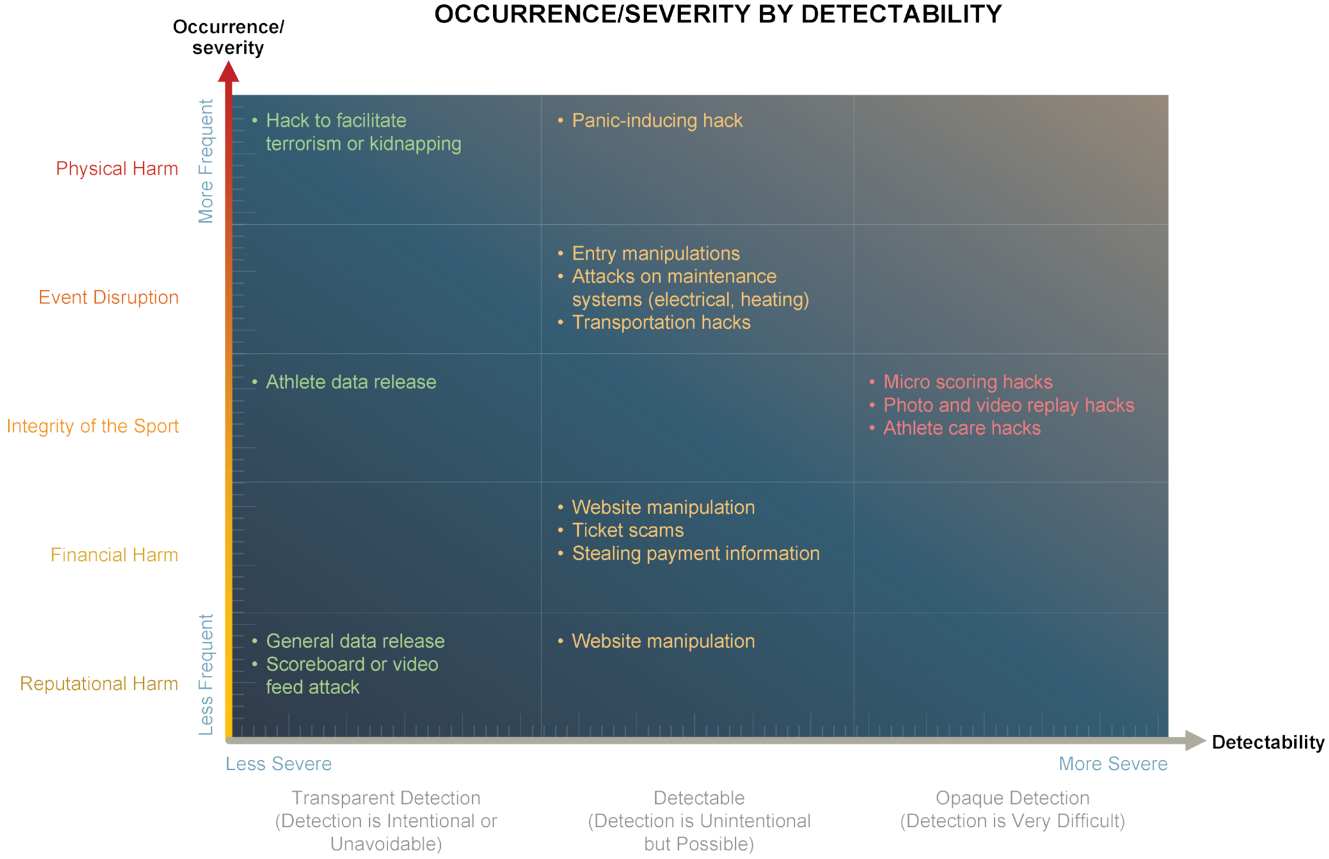


Importantly, the 'Future' attacks are concentrated in the 'less likely, but more serious' category of the table. Future attacks will be harder to pull off, but the consequences for Olympic events may well be more serious.

So far, our discussion has focused on the severity and occurrence of cyber attacks. We now layer on the third category of the risk framework: detectability. The chart below highlights the likelihood that a hack is detectable, with potential attack types colored green if they are highly detectable, orange for moderately detectable, and red if they are highly difficult to detect. The patterns here are less clear in part because, in some cases, hackers actually want their work to become visible immediately (as with a stadium display manipulation or public release of stolen data), or because in some cases the sheer effects of the attack (a terrorist attack or kidnapping) will make the uncovering of the hack highly likely.

As shown below, those hacks that are most difficult to detect are concentrated in the 'integrity of the sport' attack types. As major sports digitize, it will be increasingly hard to tell if a hack has affected the outcome of a major sporting event, perhaps even harder than catching fraudulent financial transactions. As a result, the incentives for those who would benefit from such attacks are only going to grow.

OCCURRENCE/SEVERITY BY DETECTABILITY



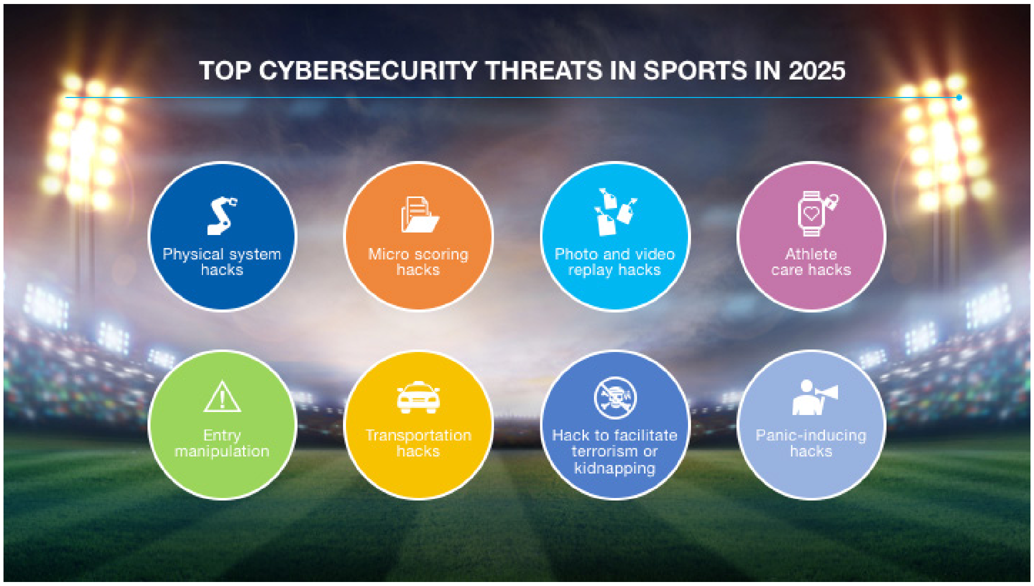
	Transparent Detection (Detection is Intentional or Unavoidable)	Detectable (Detection is Unintentional but Possible)	Opaque Detection (Detection is Very Difficult)
Physical Harm	• Hack to facilitate terrorism or kidnapping	• Panic-inducing hack	
Event Disruption		• Entry manipulations • Attacks on maintenance systems (electrical, heating) • Transportation hacks	
Integrity of the Sport	• Athlete data release		• Micro scoring hacks • Photo and video replay hacks • Athlete care hacks
Financial Harm		• Website manipulation • Ticket scams • Stealing payment information	
Reputational Harm	• General data release • Scoreboard or video feed attack	• Website manipulation	

Recommendations and Conclusion

We began this report by noting that, to date, the cybersecurity of sports has not been considered to be a relevant topic for research or study. We hope this report will help to change that, and that it will be the beginning of a conversation, not just for the Olympics, but for all major sporting competitions (and indeed, for any industry that is shifting from analog to digital).

In essence, Olympic sports (and probably other sporting events as well) face nearly infinite attack surfaces. On the one hand, it is an important goal for a risk manager to mitigate as many of these options as possible. On the other hand, perfection is an impossible goal. There will always be finite resources in this space, and those in charge of ensuring the integrity of major sporting events will have to prioritize where they invest resources to address the wide range of risks facing them.

In 2012, the cybersecurity company ThreatMetrix identified the top five online threats facing the London Games.[52] The main risks were all about devices: how hackers could manipulate search engines, mobile and tablets, phishing, etc. At the time, little thought was given to the proliferation of technologies in the sporting events themselves, or how hackers could alter or influence the competition in more fundamental ways.



Today, this graphic would look significantly different. This study defines eight key areas of risk that should get priority over others because of their low tolerability:

- Physical system hacks
- Micro scoring hacks
- Photo and video replay hacks
- Athlete care hacks
- Entry manipulation
- Transportation hacks
- Hacks to facilitate terrorism or kidnapping
- Panic-inducing hacks

Moreover, because of their low detectability, attacks affecting the integrity of the game (the scoring, replay, and athlete care hacks) are particularly worth paying attention to.

Some key themes have become clear over the course of the project already. One lesson is the need to balance opportunity and risk. Many of our interview subjects emphasized the temptation to adopt the next greatest technology, whether to outdo prior events or to try to make a complex process easier. But with each opportunity for improvement comes risk. The decision to adopt a new technology, especially when the stakes are as high as they are at the Olympic Games, should always be made with potential cybersecurity risks taken into account.

When it is the right decision to adopt a new technology, some of the most important steps are the simple steps. For instance, over the course of this project, we were able to read sensitive information at three different venues using nothing more than a (pretty bad) digital camera to zoom in on a computer screen. We also watched officials type in passwords while spectators were already in the stands, making it easy enough for a careful observer to replicate it. In brief, screen covers should be ubiquitous, all computers used in sporting events should use multi-factor authentication to limit access, and passwords should never be typed in full view of an audience.

Games officials must also ensure that any new technologies use air-gapped networks whenever possible (such networks are connected only through a closed network, and not to the broader internet). It may seem anathema to continue to use wires in an increasingly digital world, but wired networks serve as a deterrent to those who would find it much easier to tap into a wireless network.

Duplication is another key principle: every digital device used at an event needs to have a back-up in case of failure, and humans should provide oversight to verify that any digital technology used in competition is producing the correct result. Simple stopwatches should be used as backup for electronic timers, automated photo finish results should be reviewed by a human, and the raw data fed into Hawk-Eye and similar systems should be validated for accuracy. While this may seem like unnecessary duplication—in the vast majority of cases, the digital

equipment will be accurate—it will only take one serious cybersecurity failure to call the entire integrity of a sporting event into question.

This is particularly true because, as we have recently learned in a setting that also had high stakes—the 2016 U.S. Presidential election– even where the likelihood of harm may be low, the stakes are high. Before the 2016 election, cybersecurity was a known risk, but was seen as unlikely to have a significant effect on the outcome. Recent revelations suggest that this was a naïve view.[53] Major sporting events can draw numerous lessons from the failure points in that setting, including:

- *The Phone Call Might Go To The Wrong Person:* When Hillary Clinton's Chief of Staff John Podesta received a suspicious email, his first instinct was right: to call an IT professional on his staff. But that IT professional gave him wrong advice, allowing his account to be infiltrated as a result. Officials and staff involved in managing major sporting events should be trained on potential risks such as spearphishing and social engineering, and all involved organizations—from the IOC to the governing bodies of each sport to all the athletes, coaches, referees, and partners—should have policies for elevating suspicious activity.[54]

- *Having To Prove a Negative Is Really Hard:* The problem now facing many U.S. election districts is likely to be seen in sports: they can't prove that their results weren't manipulated. Trying to prove a negative in a suspicious, digitally compromised environment is highly difficult, and requires preparation so that the appropriate comparison points are possible.

- *Failure Points Pervade the Organization:* Recent revelations suggest that, in the U.S. elections, attacks may have attempted to target nearly every aspect of the digital election system, looking for weaknesses.[55] This means that the most serious risks need to take priority; perfect security is just not an option.

This last lesson points to a key blind spot, one that pervades not just major sporting events, but industry more broadly. Cybersecurity is often considered solely the domain of IT professionals. Many interview subjects initially told us that they didn't think they would have any information to offer. As they talked with us about possible digital vulnerabilities in their sport, the most common response was "I've never thought of that."

From the ticketing officer to the electrician to the coach, the facility manager, and even the spectators, every individual involved with a major sporting event has a role to play in maintaining good cybersecurity hygiene—and everyone faces potential risks from the failure of digital systems. We need to expand our perspectives about who is involved in the cybersecurity of major sporting events. Going forward, it is likely to be all of us.

Endnotes

[1] Eddie Pells, “Gymnastics: Olympic Vault Set Too Low,” *ABC News,* September 21, 2017, http://abcnews.go.com/Sports/story?id=100494&page=1.

[2] Darren Heitner, “Sport Industry to Reach $73.5 Billion by 2019,” *Forbes,* October 10, 2015, https://www.forbes.com/sites/darrenheitner/2015/10/19/sports-industry-to-reach-73-5-billion-by-2019/#1ba600c11b4b.

[3] Scott Stinson, “If Leagues Decide Gambling Can Help Grow Their Games, Trump Could Help Deliver,” *National Post,* March 4, 2017, http://nationalpost.com/sports/if-leagues-decide-gambling-can-help-grow-their-games-trump-could-help-deliver.

[4] While many of the trends identified in this paper could apply in that domain, this piece does not focus on the cybersecurity of e-sports.

[5] This paper was produced with the generous support of the Hewlett Foundation and the Los Angeles Organizing Committee for the Olympic and Paralympic Games 2028. No obligations were owed by the researcher, nor were deliverables promised, as a result of the support provided here. The paper was not reviewed by the funders in advance of publication. The authors would like to thank Steve Weber, Kristin Lin, Chuck Kapelke, Jackie Jones, and Courtney Allen for their assistance and advice throughout the writing of this report, and Cal Athletics for their invaluable partnership in this project.

[6] Nancy R. Tague, “Failure Mode Effects Analysis (FMEA),” *The Quality Toolbox,* Second Edition, (ASQ Quality Press, 2004), 236-240, http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html.

[7] Ortwin Renn, “The Risk Handling Claim,” *The Tolerability of Risk: A New Framework for Risk Management,* ed. Frederic Bouder, David Slavin, and Ragnar E. Lofstedt (Earthscan Press, 2007), 38-39, https://books.google.com/books?hl=en&lr=&id=fTFJgSks350C&oi=fnd&pg=PR5&dq=tolerability+risk+management&ots=JDPO7FUu-vg&sig=q0V3R-QeB56ohUnAycLbGbpGCGs#v=onepage&q=tolerability&f=false.

[8] There are very few reviews connecting cybersecurity and major sporting events. A handful come from cybersecurity-related magazines: Adam Finkelstein, “Cyber-Security 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.

[9] Iain Thomson, “Anonymous Crashes Formula One Site Over Bahrain Protests,” *The Register,* last modified April 20, 2012, https://www.theregister.co.uk/2012/04/20/f1_anonymous_bahrain/.

[10] James Hampshire, “Professional Sports Teams Are Risking a Cybersecurity Own Goal,” *Infosecurity Group,* August 11, 2015, https://www.infosecurity-magazine.com/opinions/professional-sports-teams/.

[11] Federico Guerrini, “Brazil’s World Cup of Cyber Attacks: From Street Fighting to Online Protest,” *Forbes,* June 17, 2014, https://www.forbes.com/sites/federicoguerrini/2014/06/17/brazils-world-cup-of-cyber-attacks-from-street-fighting-to-online-protest/#49874ca251a8.

[12] *Id.*

[13] David Bisson, “How A Massive 540 Gb/Sec DDoS Attack Failed to Spoil the Rio Olympics,” *Tripwire,* September 5, 2016, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-a-massive-540-gbsec-ddos-attack-failed-to-spoil-the-rio-olympics/.

[14] “Securing the 2012 Olympics,” *Infosecurity Group,* November 19, 2009, https://www.infosecurity-magazine.com/magazine-features/securing-the-2012-olympics/.

[15] Graeme Burton, “How the London Olympics Dealt With Six Major Cyber Attacks,” *Computing,* March 6, 2013, https://www.computing.co.uk/ctg/news/2252841/how-the-london-olympics-dealt-with-six-major-cyber-attacks#comment_form.

[16] Sue Marquette Poremba, “Beijing Olympic Ticket Scam Shutdown,” *SC Magazine,* August 5, 2008, https://www.scmagazine.com/beijing-olympic-ticket-scam-shutdown/article/554792/.

[17] *Id.*

[18] McAfee Labs, "Scams Surround London Olympics," *McAfee,* https://securingtomorrow.mcafee.com/mcafee-labs/scams-surround-london-olympics/.

[19] Ben Rumsby, "Rugby World Cup 2015 Tickets: Cyber Criminals Plotting to Hijack Launch," *The Telegraph,* September 11, 2014, http://www.telegraph.co.uk/sport/rugbyunion/rugby-world-cup/11088098/Rugby-World-Cup-2015-tickets-Cyber-criminals-plotting-to-hijack-launch.html.

[20] James Hampshire, "Professional Sports Teams are Risking a Cybersecurity Own Goal," *Infosecurity Group*, August 11, 2015, https://www.infosecurity-magazine.com/opinions/professional-sports-teams/.

[21] Rebecca R. Ruiz, "U.S. Athletes Reassured After New Russian Hack," *The New York Times,* October 14, 2016, https://www.nytimes.com/2016/10/15/sports/us-officials-reassure-athletes-after-new-russian-hack-of-medical-files.html.

[22] *Id.*

[23] 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.

[24] "Hacked within Minutes: Sochi Visitors Face Internet Minefield," *NBC News,* February 4, 2014, http://www.nbcnews.com/video/nightly-news/54273832#54273832.

[25] Jeremy A. Kaplan, "NBC News Takes Heat over Sochi Phone Hacking Report," *Fox News,* February 7, 2014, http://www.foxnews.com/tech/2014/02/07/nbc-news-takes-heat-over-sochi-phone-hacking-report.html.

[26] Gordon Corera, "The 'Cyber-Attack' Threat to London's Opening Ceremony," *BBC News,* July 8, 2013, http://www.bbc.com/news/uk-23195283.

[27] Chris Peterson, "Big Data and the London Olympics Cybersecurity Challenge," *Tech News World,* July 27, 2012, http://www.technewsworld.com/story/75754.html.

[28] Tim Kelly and Nobuhiro Kubo, "Japan Holds First Broad Cybersecurity Drill, Frets Over Olympic Risks," *Reuters*, March 17th, 2014, http://www.reuters.com/article/us-japan-cybercrime/japan-holds-first-broad-cybersecurity-drill-frets-over-olympics-risks-idUSBREA2G1O920140318.

[29] *Id.*

[30] Center for Long-Term Cybersecurity, *Cybersecurity Futures 2020* (Center for Long-Term Cybersecurity, April 28, 2016), https://cltc.berkeley.edu/files/2016/04/cltcReport_04-27-04a_pages.pdf.

[31] "Caltrans Sign Hacked In Napa Over July 4th Weekend," *CBS SF Bay Area,* July 5th, 2017, http://sanfrancisco.cbslocal.com/2017/07/05/napa-caltrans-sign-hacked-asian-drivers/.

[32] Jaikumar Vijayan, "Target Attack Shows Danger of Remotely Accessible HVAC Systems," *Computerworld*, February 7, 2014, https://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html.

[33] Jake Kanter, "Here's How the Newest Technology is Changing How We Watch the Olympics," *Business Insider,* August 3, 2016, http://www.businessinsider.com/big-tv-innovations-at-rio-olympics-2016-8.

[34] John Constine, "Anti-Done Radio Wave Startup SkySafe Secures $11.5M from Andreessen," *Techcrunch,* July 20, 2017, https://techcrunch.com/2017/07/20/skysafe/.

[35] "MagicBands & Cards – FAQs," *Disney World,* accessed October 3, 2017, https://disneyworld.disney.go.com/faq/bands-cards/understanding-magic-band/.

[36] Eric Loveday, "Chevrolet Volt Hacked to Allow Steering Wheel to Control Mario Kart", *InsideEvs*, February 2017, http://insideevs.com/chevrolet-volt-hacked-allow-steering-wheel-control-mario-kart-video/.

[37] "SW 11 Timing," Fina, accessed September 20, 2017, http://www.fina.org/content/sw-11-timing.

[38] 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/.

[39] Telegraph, "London 2012 Olympics: Britain's Sailors Will Be Under Same Scrutiny as Footballers During Games, Warns Sir Keith Mills," *The Telegraph,* February 21, 2012, http://www.telegraph.co.uk/sport/olympics/sailing/9096214/London-2012-Olympics-Britains-sailors-will-be-under-same-scrutiny-as-footballers-during-Games-warns-Sir-Keith-Mills.html.

[40] Becky Ferreira, "How Olympic Timekeepers Judge False Starts and Photo Finishes," *Motherboard*, August 18, 2016, https://motherboard.vice.com/en_us/article/8q8mp5/how-olympic-timekeepers-judge-false-starts-and-photo-finishes.

[41] "LaserLynx Pro Distance Measurement," *Lynx,* accessed September 30, 2017, http://www.finishlynx.com/product/event-management/laserlynx-distance-measurement/.

[42] Brian Hamilton, "U.S. Women Overcome Coach's Error, Will Play for Water Polo Gold," *Chicago Tribune,* August 7, 2012, http://articles.chicagotribune.com/2012-08-07/sports/chi-us-to-play-for-gold-in-womens-water-polo-20120807_1_water-polo-gold-melissa-seidemann-adam-krikorian.

[43] Rhett Allain, "Olympics Physics: New Platform Is No Chip Off The Old Starting Block," *Wired*, August 28, 2012, https://www.wired.com/2012/07/olympics-physics-swimming-starting-blocks/.

[44] Associated Press, "Omega Releases Official Photos of 100-Meter Butterfly Finish," ESPN.com, August 23, 2008, http://www.espn.com/olympics/summer08/swimming/news/story?id=3550164. Image credit: Getty Images.

[45] Charlie Eccleshare, "How Wimbledon is Using Artificial Intelligence to Enrich the Fan Experience," *Telegraph,* June 27, 2017, http://www.telegraph.co.uk/tennis/2017/06/27/wimbledon-using-artificial-intelligence-enrich-fan-experience/.

[46] Julia Grassie, "3D Lasers to be Part of Gymnastics Judging at 2020 Tokyo Olympics," *NBC Olympics,* May 18, 2016, http://www.nbcolympics.com/news/3-d-lasers-be-part-gymnastics-judging-2020-tokyo-olympics.

[47] Eve Turow Paul, "Why This Robot Restaurant Should Terrify You," *Forbes,* last modified September 27, 2016, https://www.forbes.com/sites/eveturowpaul/2016/09/27/why-eatsa-scares-me/#180c30bd3d60.

[48] 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.

[49] Emily Jed, "Weider Vending Machine Delivers Freshly Blended Protein Shakes," *Vending Times,* June 8, 2015, https://www.vendingtimes.com/main/articles/5859.aspx.

[50] 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/.

[51] 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/.

[52] ″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/.

[53] Nicole Perlroth, Michael Wines, and Matthew Rosenberg, "Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny," *The New York Times,* September 1, 2017, https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html.

[54] 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/dnc-email-hack-typo-john-podesta-clinton-russia.

[55] Perlroth et al., *supra* note 52.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley