SECURING
SMART
CITIES

Securing the Smart City Olympics

February 2018

SECURING
SMART
CITIES

Authors

Mohamad Amin Hasbini, Senior Security Researcher, Kaspersky Lab,

Martin Tom-Petersen, CEO and Co-founder, Smart City Catalyst,

Cesar Cerrudo, CTO, IOActive Labs

Contributors

Krishnakumar Kottekkat, Manager IT Strategy & Governance Aspire Zone Foundation

David Jordan, CISO, Arlington County Government, Virginia, USA

James Mckinlay, Director, Praetorian Consulting International Limited

Alan Seow, Cybersecurity Practitioner

SECURING SMART CITIES

Contents

SECURING SMART CITIES

1. Introduction

The modern Olympic Games started in 1896. The Games are a global stage, bringing together thousands of athletes from across the world every four years, with the Summer and Winter Games on separate four-year cycles in alternating even-numbered years.

The Olympics Games have almost always been used to introduce radically innovative and game-changing technologies, intended to make the sporting events more efficient, entertaining and spectacular, while also influencing global changes and technology standardization.

The Olympics have always necessitated the introduction of improved technologies, just a few examples of these include the use of stopwatches (Athens 1896), photography (Paris 1900), TV telecast (Berlin), Shinkansen bullet trains (Tokyo 1964), quantum timers (London 2012), and virtual reality events monitoring breakthroughs (Rio-2016 and Pyeongchang-2018). New technology has thus been instrumental in shaping the growth of the Games.

From host countries rushing to improve their infrastructure, to networks inventing a more mesmerizing viewing experience for their audiences, the Olympic Games is key to spurring growth in technology. The Games are a high-profile occasion where each operational blunder can sprout away into a global crisis, leading to dire consequences. Because of the important role information technology plays in the success of the events, one area of pivotal concern is cybersecurity.

Previous related research:

- The Smart Cities Internet of Access Control, opportunities and cybersecurity challenges
  https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-IAC.pdf

- Smart Cities Cyber Crisis Management
  https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-SCCCM.pdf

- Establishing a Safe and Secure Municipal Drone Program
  https://securingsmartcities.org/wp-content/uploads/2017/02/municipal_drones_FINAL.pdf

- Cyber Security Guidelines for Smart City Technology Adoption

  https://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf

SECURING SMART CITIES

1.1. The Olympics at the forefront of technology

With the difference of two years between every Summer and Winter Games, as well as the huge advertising opportunity such events offer, leading technology companies from across the world usually strive to showcase their best achievements around the Olympics. Nevertheless, the Olympics are also used to maintain very high standards, including the use of technologies for detecting and blocking the use of performance-enhancing drugs…

Similar to cybersecurity issues, drugs are unwanted, and can disrupt the nature of events. They also require innovative technologies to spot them, and protect The Games against them. A drug's risk of exposure, for example, is limited to athletes, while the risk of cybersecurity issues have a much larger scope, including but not limited to the athletes, committee members, and everyone in the stadiums watching the events or monitoring their progress.

The Olympics are comparable to a business of 200,000 employees, addressing 4 billion customers, operating 24/7, in a new territory, every 2 years. They also present themselves as highly demanding from a trust and compliance point of view (technology, operations, management). The Rio 2016 Olympics, for example, was surrounded by more than 300,000 accredited personnel.

Multiple technological areas have witnessed growth because of these elite Games, including cybersecurity, smart cities, smart transportation systems, the big data revolution, waste recycling, and player tracking and monitoring systems. The Games are the catalyst that makes scientists, engineers, and other experts come up with improved products that are demonstrated in front of millions of people, and which can lead to healthy and more productive lifestyles.

1.2. Planned revelations for the upcoming Olympics

Just like previous events, the upcoming Olympics will be pivotal for showcasing sophisticated emerging technologies worldwide. Even though most of the events are still years away, host cities have been intensifying preparations so that they are ready well before the kickoff.

1.2.1. PyeongChang, 2018

In the forthcoming 2018 Games in PyeongChang, South Korea, an extensive array of cutting-edge technologies is expected to be displayed. In terms of technology and innovation, South Korea is touted as one of the world's leaders.

Furthermore, the country is home to some famous companies in the electronics industry, such as Samsung and LG. Therefore, the upcoming 2018 Olympics, which is budgeted at around $13 billion, forms the best opportunity for South Korea to display its technological

prowess. Consequently, the country has intensified its efforts to develop new, robust technologies ahead of the Games.

The country's authority is planning to use robotic devices to improve security and also carry out some other functions, such as translation services and giving directions to visitors. For the first time, fifth generation or 5G mobile network is likely to be demonstrated at the Games. The 5G network is a cutting-edge cellular technology, which some parts of the world are likely to wait longer for, before adopting.

Autonomous vehicles, manufactured locally in the country, are expected to transport visitors during the Pyeongchang 2018 Games. Furthermore, drones, provided by Intel Corporation, are going to be used extensively for broadcasting and security enhancement.

1.2.2. Tokyo, 2020

In 2020, when the world turns to Tokyo, the city is expected to show the most futuristic technologies rarely seen in other Olympics. With a budget of $17 billion, Japan is likely to showcase a number of revolutionary technologies, which could spread out to other areas of the world.

As one of the most automated countries in the world, Japan is obsessed with using its robust technology to automate almost everything. During the Games, the city is planning to have a "village of robots", consisting of all sorts of robots capable of carrying out various activities, including giving directions to visitors, language translations, and transportation.

The era of self-driving cars could start after the 2020 Olympic Games. Japan has already made significant progress in delivering driverless taxis on the country's roads, something which the biggest names in tech—Google, Uber, and Mercedes—are still struggling to master.

Another interesting technology that is likely to be showcased during the Games is the use of algae as an alternate fuel source. Fukushima, Japan, has been at the forefront of developing such alternate fuel sources, which could be demonstrated at the Olympics.

What's more, renowned global names like Boeing are supporting the plans. If the use of algae can be demonstrated as an effective and useful alternate fuel at the 2020 Games, we could soon see a widespread adoption of this technology across the world.

1.2.3. Paris, 2024

The 2024 Olympic Games will take place in Paris, France. Paris will become the second city, after London, to host the sporting event three times. The city last held the event in 1924, so 2024, will mark exactly one hundred years since then.

Because of its previous experience hosting such events, Paris has started early preparations to stage magnificent and entertaining Games, to shape ideas and forge the future.

eSports, for example, is likely to be a medal event during the 2024 Olympics. This demonstrates the increasing significance of electronic systems to leverage sporting.

1.2.4. Los Angeles, 2028

Los Angeles is going to host the Olympic Games for the third time in 2028. Instead of focusing on building new infrastructure, the city intends to focus its energies on reinventing the Games and using technology to give visitors a desirable experience.

By the time Los Angeles hosts the Olympics, most of today's nascent technologies such as augmented reality, artificial intelligence, or autonomous transportation systems could already be realities. Therefore, we can expect the city to capitalize on already established revolutionary technologies to enhance the magnificence of the Games.

2. Significant technological advantages

The Olympics have played a pivotal role in the growth of technology. Likewise, without technology, the modern Olympic Games could not be enjoying the high levels of opulence and magnificence often associated with them. Technology has been applied to every facet of the events, from increasing the efficiency of booking tickets, to tracking the ball trajectory in tennis, to goal-line technology in football. Without embracing technology, the Olympics could not have reached its modern standing, providing an enhanced experience for athletes and viewers.

Here are some of the significant technological developments seen at the Games.

2.1. Population density management

The Olympics is a global event that attracts people from all around the world. For example, for the Pyeongchang 2018, 1.1 Million tickets are expected to be issued; in the Tokyo 2020 Games, this will be 10 million tickets. It's essential to develop effective technologies for managing such large numbers of people.

As earlier mentioned, one method Tokyo will use to manage the large number of people, is robots and autonomous vehicles. At the Olympics, participants will be able to rely on robots to assist them to complete various tasks, including instant language translations, giving directions, and more.

The use of technologies like IoT, and other sensor-based advancements that churn out a lot of geo-spatial data related to crowd movement with appropriate analytics on top, could facilitate the proper planning of the Games, and act as feedback for urban planning. Such technologies with a well-established and integrated smart infrastructure will facilitate the easier and faster mobilization of people in and out of venues, as well as within the city; increasing the convenience for spectators and visitors. This can only be achieved with better

collaboration between the urban planners, city authorities, the public service providers, and the event organizers themselves.

Without appropriately managing the huge population at such events, small incidents could easily escalate into chaos and even disasters.

2.2. Robot villages

Currently, an increasing number of robots are being used to complete various tasks faster and better. And, the Olympic Games have been a major stage for showcasing the latest improvements in robotics technology.

Particularly in the forthcoming 2020 Games, Japan is planning to have a village of robots capable of completing various tasks to make the events highly reliable and more entertaining. Visitors are expected to see an army of robots strolling the country's streets during the Games. The robots, which are enough to populate a small village, will be assisting participants with almost everything, from transporting luggage to providing directions. Tokyo intends to create an environment where the mechanical attendants can help visitors irrespective of their age, nationality, or status.

2.3. Smart transportation

Nowadays, there is an increase in focus on alternative fuel sources that leave minimal impact on the environment, or even better. And, with the high population of people from around the world attending every Olympic Games, it's usually a good ground for showcasing the latest developments in alternative energy sources.

The options that are currently touted as the best alternative energy sources are algae and hydrogen. In the 2020 Olympics in Tokyo, the world is likely to see smart transport systems powered by both. The interesting fact about algae is its ability to suck up carbon dioxide and change it into energy, therefore generating energy and cleaning the environment at the same time. In contrast to most other land-grown green energies, algae also produces cleaner and more energy per acre, while also being easier to grow. Boeing expects that by 2020, visitors will be able to fly on airplanes powered by fuel from algae, and has already unveiled a Biofuel 'Roadmap' to the 2020 Olympics.

Another smart transportation option is hydrogen, which is capable of generating energy without releasing harmful byproducts to the environment. The Tokyo government is expected to spend more than $300 million to enhance the use of hydrogen energy before its Games. During the Olympics, hydrogen will be used power at least 100 buses and numerous buildings around the city.

SECURING SMART CITIES

2.4. Data analytics

The current massive use of data analytics is proving to be very helpful at the Olympic Games. Importantly, the teams that have employed the use of data analytics have reported impressive results at the events. Numerous sensors are used to gather every bit of data on the behavior and performance of the athletes. Once the data is captured, it's extensively analyzed to discover patterns that can predict better training programs and point to tactics for competitive success.

Analysts usually assess athletes' previous data on workouts, to tailor the optimal balance of strength and endurance performance, to their corresponding sport activity. With such intelligence, it's possible to limit injury cases and reduce the length of recovery time needed.

For example, the British rowing team has depended on data and analytics to help them become successful at the games. The team use their data-driven analytics to make their boats move faster and maximize the performance of each member. Consequently, the team has recorded impressive results and won at least one gold medal in every Olympics since 1984.

Data analytics at the Olympics is currently regarded as a highly critical function that enables new functionalities and services to develop and enhance operations - and the Olympics experience. Furthermore, data analytics is used to forecast how athletes and countries are likely to perform in the medals table. Some data companies use different data signals, advanced analytics, and a unique algorithm to foretell how things are likely to work out at the Olympics - and most of the time they get it right!

Waste management and recycling

Before the 1990s, sustainability was not one of the main concerns of the Olympics. Since waste recycling was not regarded as a serious issue back then, hosting countries would see a huge increase in the garbage leftover after the Games. One example is, during the 1984 Games in Los Angeles, U.S., the participants increased the amount of garbage to 6.5 million pounds.

In the 1990s, most hosting cities started increasingly adopting proper waste management and recycling programs. The 2000 Sydney Olympics was dubbed the "Green Games" because of the city's efforts towards sustainability. These Games achieved various sustainability objectives, including reusing 90% of demolition trash and transferring no refuse to the landfill. The London 2012 Games took Sydney's successes to the next level by realizing zero waste to landfill, saving thousands of tons of carbon dioxide, and decommissioning venues.

In 2020, the Tokyo Olympics plans to take waste management efforts a notch higher by issuing event medals recycled from electronic wastes, such as smartphones and other

devices. Japan is also planning to reclaim electronic wastes and recycle them to produce the gold, silver, and bronze medals to be used in the Games.

Currently, the world is experiencing problems with electronic waste, with about 49.8 million tons of waste generated in 2018. Therefore, the technology that Japan will use to recycle electronics and metals could spread to other areas in the world, resulting in better waste management.

2.5. Contenders tracking, monitoring and protection

Use of statistical analytics for contenders is a rising trend in professional sports, and the Olympics is at the forefront in spurring this growth. Teams from across the world are working hard to implement innovative technologies to enhance their performance and win more medals. Boxing teams are currently using electronic performance measuring tools to assess the best tactics, to guarantee maximum wins.

Similarly, boating teams can accurately forecast the performance of the ocean current and how to maximize their maneuverability. Furthermore, the Adidas miCoach monitoring tool is presently being used by most teams to collect data. This tool is a small sensor that can be easily fitted in the players' shirts, monitoring their average speed, heart rate, and acceleration. Smart suits and helmets are also going to be used in the PyeongChang 2018 Olympics for enhanced protection, and suits for skiers will also use smart airbag technology to detect when control is lost, and open automatically to protect the contenders.

It's at the Olympics that contenders showcase their latest tracking and monitoring tools and techniques. With performance monitoring systems, contenders are able to assess their day to day practice statistics and adopt the best routine for competitive sporting. Furthermore, tracking systems provide athletes with data, ensuring they set specific goals to achieve. This way, they can stay motivated to improve on their weak areas and gain a competitive edge.

2.6. Judgement assistance

The ruling to give an athlete the winning medal at the Olympics is very important, and judges are expected to make accurate decisions without delay. In some instances, a winner can be announced and the decision later revoked after careful judging. As such, properly judging the winner of any game is important for the Olympics to maintain its high reputation. If a referee is accused of influencing a decision or is biased, athletes can lose morale for participating.

Consequently, there has been a growth in judgment assistance technologies that enable organizers and referees to accurately make split-second decisions without bias. For instance, some of the latest technologies used at the 2016 Rio Olympics to improve decision making included slow-motion replay and replay showing different angles. Others included 3D

movement tracking for gymnastics and tracking software to monitor the movement of athletes.

The upcoming Olympics are then increasing their investments in developing sophisticated technologies that present precise scoring mechanisms. High-profile sporting events are now turning to technology for judgment assistance. With such technology, referees and organizers can affirm their “on field” decisions and minimize disputes and contentions, leading to a fairer competition.

2.7. Spectator experience

Every occurrence of the Olympic Games gathers a very large audience from around the world. For example, it’s estimated that the Rio Olympics attracted an audience of about 3.5 billion. The number of people usually packed in the stadiums, as well as the high number of people following from their televisions around the world, has necessitated the need to develop enthralling technology to enhance their experience.

Currently, there is an increase in the development of better technologies meant to transform stadiums into fan-centric places and convert spectators into superfans along the way. Modern fans are very sophisticated, and technology is being utilized to increasingly meet their needs. For example, futuristic technologies such as augmented and virtual reality are being incorporated to transform the spectator experience into a more immersive one.

To ensure spectators enjoy the action at the stadiums, venues are being constructed using flexible, modern, and appealing designs. Modern architecture is integral in ensuring the designs of the Olympic stadiums are constructed to maximize the spectator experience and view.

Hosting cities are depending on apps and digital innovation to enhance fan experiences. In the 2020 Tokyo Games, the city is spending a lot of money on incorporating connectivity and convenience, cutting-edge apps will be deployed to assist fans with complete various tasks, including locating parking spots, identifying their seats, and viewing instant replay videos (stop motion and multi-angle displays…) The modern tech-savvy spectator likes sharing, interacting, and using social media without any restrictions.

2.8. Indoor navigation systems

With the high number of visitors attending Olympics Games, as well as the huge number of events held, the use of indoor navigation systems is indispensable. In the upcoming 2020 Tokyo Olympics, the city has planned comprehensive indoor navigation systems to enable visitors to easily find directions. Tokyo will introduce a free mobile application for smart devices, which will enable indoor navigation with turn-by-turn directions in various languages. Visitors will be able to set the app in their preferred language and use it to track directions for the next event, find their storage cabinet locations, and much more.

If Tokyo demonstrates it has the best technology for indoor navigation, the rest of the world could also adopt this technology. Consequently, airports and other busy places could improve their technology to achieve better accessibility for everyone.

2.9. Access control technologies

Over the years, facial recognition technology has greatly improved. This relies on biometric identification authentication derived from the facial characteristics of people. Once a user has been registered in a database, the technology can be used to retrieve their information and verify his or her actual details. The facial recognition technology provides a non-contact process of getting a user's details - instead of asking users to be physically present, their facial characteristics can be videoed or captured and transmitted for analysis. This is important to note from a security point of view, since a person's biometric facial information can easily be known without his or her knowledge.

Facial recognition technology is capable of delivering quick and accurate results. With such systems, users can attain high recognition rates and minimal processing times, making their use very desirable. With the current advancements in biometric facial technology, experts have found their use at the Olympics to be essential in delivering fast and accurate results. And, any errors or malfunctions recorded during their use can be worked on and improved before the next Games.

For example, in the forthcoming 2020 Games, organizers are planning to apply facial recognition technology to authenticate the identity of ticket holders. After a fan has entered the stadium, the technology will be used to ensure the identity of the ticket holder is the same as the one registered for the booked seat.

Similarly, the use of fingerprint access to control systems has increased, mainly because of reinforced security capabilities. With this technology, a user is required to provide his or her fingerprints before accessing a facility.

Because of the uniqueness of fingerprints and the limited room for machine error, fingerprint access control has been widely used in the Olympic Games for restricting access to athletes' changing rooms and limiting the number of people accessing certain facilities. In the forthcoming Olympics, even as the technology develops, we expect to see an increased use of biometric access control systems to make the Games more secure.

For more information on the cybersecurity of access control in smart city environments, please refer to previous research on the smart cities Internet of Access Control:

https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-IAC.pdf

SECURING SMART CITIES

3. Cybersecurity challenges

Because of the high number of IT infrastructure and communication systems used in any Olympics Games, there is a need to keep them secure and impenetrable from malicious hackers. If any unauthorized third-party were to break into any of the critical devices used in the Games, it could be a major nightmare for the organizers and attendees. Therefore, the Olympics has elevated the importance of cybersecurity and recognized the need to develop tighter cyber defense techniques. In the forthcoming Games, the organizers are already carrying out comprehensive security testing to increasingly solidify IT infrastructure/communication systems and eliminate any weak entry points.

During every Olympics, the computers, communications systems, and other gadgets must be kept secure to prevent the disruption of services. Without adhering to solid protection mechanisms, risks can involve the loss of the Olympics' brand reputation, and legal challenges because of non-compliance to multinational privacy regulations. Although they might also escalate into much worse cases.

In light of the recent increase in cyber threats on a multidimensional scale, malicious hackers are likely to carry out attacks using social engineering techniques, to manipulate and increase the risk of personnel divulging sensitive information. Frequent training is usually held to increase awareness and skills to prevent such attacks.

And, the most common cybersecurity challenges include the following:

- Direct and indirect threats (such as power outages) that can cause the denial of services to essential IT infrastructure and communication systems.
- Hacktivism, state sponsored, cybercriminal and terrorism threats and attacks from organizations or individuals looking to promote certain agendas.
- Malware distribution schemes that can impair the proper function of both IT and communication systems. For example, sending phishing emails to organizers and participants, and the propagation of fake news via compromised communication systems.
- Ransomware distribution schemes that lock IT systems and demand for payment before unlocking the systems.

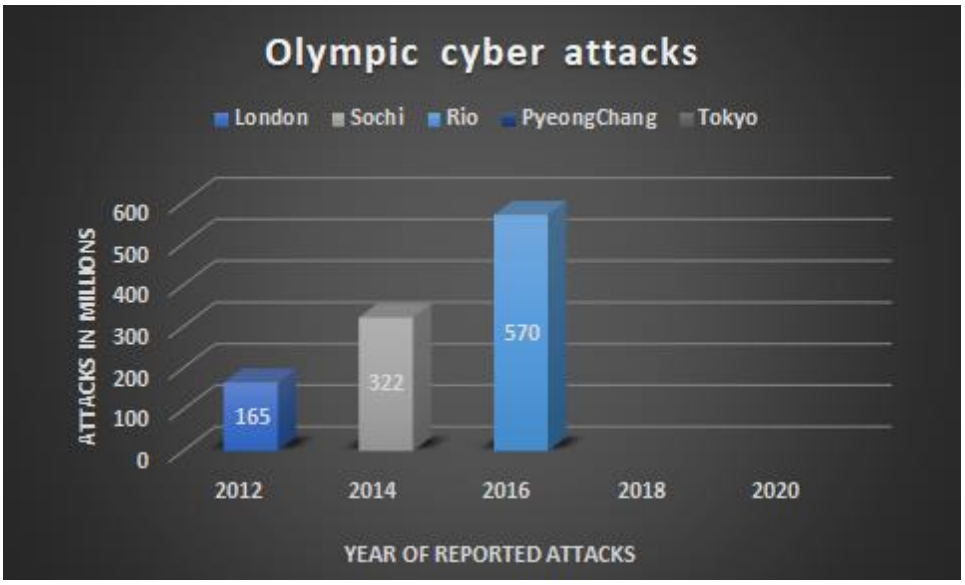
Securing the Olympic Games from the above cybersecurity challenges is a work of great magnitude. It involves a proper understanding of the risks, identifying vital systems and data, and establishing appropriate response mechanisms. The organizers usually establish a defense structure that revolves around three core areas: application code, IT infrastructure/communication systems, and people.

Developers are obligated to develop secure, encrypted systems that cannot be easily penetrated by unauthorized third parties. The infrastructure is constructed with numerous network and server layers to restrict access and solidify their makeup. Lastly, sufficient

training programs are usually carried out to equip people with the skills needed to ward off cyberattacks.

4. Scenarios of cyberdamage

At the 2008 Beijing Games, around 190 Million cyber-attacks were reported during the games (12 million per day). At the 2012 London Games, cybercriminals targeted over 200 million failed attacks to the single official website of the events. At the 2014 Sochi Olympics, 322 million attacks were reported, followed by 570 million at the 2016 Rio Olympics.



There is an increase of 95% in the number of attacks when comparing the London 2012 with the Sochi 2014 number of attacks. This could be considered as anomaly however we see an even equally high increase in attacks comparing 2014 with 2016, around 77%. At the 2020 Olympics, Japan is planning drastic measures to enhance the safeguards of its IT infrastructure from cyberattacks and should consider a projected increase in cyberattacks of at least 57% based on the average increase from the 3 last Olympics. The rise in attacks could merely be caused by the increased adoption rate of technology to support the Olympics, the contenders and the whole spectator experience.

The Olympics offer the world an excellent stage for trying out various emerging technologies to prevent the growing number of cyberattacks. Consequently, the lessons learnt overcoming the cybersecurity challenges at the Olympics are usually applied by organizations and individuals from around the world.

Below is a list of the possible damages which could occur due to a cyberattack during the Olympic Games:

1. Cyberattacks on online ticketing services, including reservations, seating, hotels, transport services and food orders (ie: compromise or denial of service), can all be the cause of essential Olympic services/ operations becoming paralyzed.

2. Cyberattacks on authentication and authorization systems (onsite access control accuracy), if successful, can enable attackers to remotely control access to the Games, blocking or allowing anyone access inside the stadiums, operational or athlete rooms.

3. The possibility of attacks to robotic machinery, disabling or controlling this machinery remotely, has already been demonstrated. Such incidents could have terrible consequences as robots are intended to support operations not cripple them or cause harm to the attendees

4. Attacks on cyber physical operational technologies: such as heating, ventilation, and air conditioning (HVAC), elevators, emergency lighting, traffic signals, water treatment facilities, sewage pumps, monitoring drones and cameras...

5. Attacks on the employees and attendees of the games (phishing, hacking, remote monitoring or data manipulation, blackmailing...). Such incidents can be the cause of financial damage to attendee victims or even the ruin of their trip. In the case of employees, access to their devices could be granted to attackers which might then be able to steal data or manipulate operations.

6. Attacks on the host country's infrastructure, including water treatment/distribution, power/electricity, transport/airlines, banking, e-government services. Multiple examples of similar activities have been discussed in previous sections, the damage is unbearable, as such services must be guaranteed.

7. Attacks and the manipulation of judges/judging systems, data and/or scoring decisions, can ruin the Games' authenticity and reputation.

8. Attacks and manipulation of contenders' health testing (ie: against performance drugs) or performance monitoring sensors (which are used to enhance their exercise programs and their results) or contender protection (ie: smart airbags). Attacks like these can impact the Games' reputation and authenticity, allowing cheats or even causing the malfunction of contenders' protection systems and therefore threatening their safety.

9. Manipulation of data analytics systems and algorithms (which help predict traffic, population density, weather, water/power/storage demands...). Such manipulation can affect the Games' continuity. Guest attendee experience might also be influenced so they feel confused, not happy or not safe.

10. The spread of rumors via social media can also quickly impact the Olympics. Fake profiles can post fake messages, can start crowd panics or influence a crowd's experience and safety.

11. Jamming attacks can interrupt communications affecting related systems, causing DoS with a huge impact on the many technologies that rely on wireless communications. Many technologies also rely on GPS, which could also be attacked, impacting systems that depend on geolocation.

For more information on developing a safe municipal drones program, refer to previous research paper:
https://securingsmartcities.org/wp-content/uploads/2017/02/municipal_drones_FINAL.pdf

5. Cybersecurity preemptive measures

Today, information technology is integral for the success of any Olympics. The Games rely on technology to channel communications, enhance the user experience, and ensure the success of every event. If there is a major disruption in the use of computing systems at the Games, the events could face difficulties in keeping going and keeping everyone safe.

For example, an attack rendered successful on an associated Industrial Control System (ICS) and within the ICS, perhaps a Supervisory Control and Data Acquisition (SCADA) system. A malicious command may be sent to halt a valid computing function or communication system, hence disrupting normal operations. It might also facilitate an attack on inter-connected systems. The resulting cascade effect could lead to significant disruption of the Olympic Games. As such, the protection of the critical IT infrastructure is vital for any country hosting the Olympics.

The current increase in the number of cybercriminals, state sponsored hackers, terrorists and hacktivists, driven by the desire to steal confidential data, cause disruption of services, or promote certain ideological agenda, cannot be ignored. If a serious cyberattack occurs during the Olympics, it can deteriorate the Games' reputation and lead to loss of critical data. The presence of such risks is necessitating organizers to take strong action to incorporate cybersecurity prevention measures in their planning processes.

A lot of research is being undertaken to identify the latest security threats and come up with robust countermeasures. As a result, the successful strategies used to prevent cyberattacks at the Olympics is normally adopted by various organizations around the world.

Here are some of the key measures the forthcoming Olympics are implementing to fight against malicious hackers.

5.1. Education and readiness

Education and knowledge sharing is the number one strategy that Olympic Games organizers are using to ward off attacks. Appropriate education can instill a security-aware culture that's well prepared and waiting to spring into action. Such readiness helps to deter malicious hackers from exploiting services, and prevents participant naivety and gullibility from compromising confidential data.

Just ensuring users are aware of the strategies used by malicious hackers, is a great way of preventing incidents at the Olympics.

Olympic participants are encouraged to report any cyberattack incidents to the authorities within the shortest time possible. This way, quick action can be taken to prevent a recurrence or escalation of the attack.

Phishing, is one the most common type of cyberattack, and takes place when a malicious hacker convinces a victim to divulge sensitive information. For instance, a visitor attending the Olympics might receive an email purporting to be from the organizers; however, the message might be crafted to trick the visitor into handing out personal financial information.

To prevent this type of attack, Olympics participants, workers, and other people involved in the Games are usually equipped with sufficient skills to identify, and not fall prey to, such incidents.

5.2. Reinforcing the ICT infrastructure

During the 2012 London Olympics, several major cyberattacks were reported, which almost threatened to bring the Games to its knees. For example, there was a denial of service attack on power systems, which continued for nearly one hour. Hacktivists also attempted to bring down the official website of the Games. Similarly, during the Rio Olympics, a number of incidents were also reported.

Smart Olympics technological solutions should comply with basic security requirements such as:

- Strong cryptography to protect data, both at rest and in transit: all wired and wireless communications (data in transit) should be properly protected with strong encryption. Systems dealing with sensitive data should also have a mechanism to encrypt data at rest.
- Authentication capabilities: All systems should require a username and password to access functionality, at a minimum. To enhance authentication capabilities, the solution should support strong authentication mechanisms (one-time passwords, certificate, or biometric-based authentication, etc.).

- Authorization capabilities: All functionality should require and enforce proper permissions before performing any actions.
- Automatic and secure update of software, firmware, etc.: Software/firmware update mechanisms should be available, and updates should be delivered in an automatic and secure way.
- Auditing, alerting, and logging capabilities: All systems should provide mechanisms for auditing and logging security events. Logs must also be saved securely against tampering.
- Anti-tampering capabilities: Devices should have a mechanism to prevent tampering by unauthorized sources.
- No backdoor/undocumented/hardcoded accounts: Some vendors release systems with backdoor/undocumented/hardcoded accounts. Often, these accounts cannot be removed or disabled and have passwords that cannot be changed, allowing anyone to compromise the system using these accounts. Removing or disabling these accounts should be enforced in the service-level agreement (SLA) to ensure vendors will comply.
- Non-basic functionality disabled by default: Only basic functionality should be enabled by default, and the rest should be enabled depending on the organization's needs.
- Fail safe/close: In the case of a system malfunction or crash, the system should remain secure and security protections remain enforced.
- Secure by default: Solutions should come with a secure configuration by default.

A lot of focus has already been placed on the importance of penetration testing, and vulnerability assessments for all systems, people, and devices used in the Games. If any flaws are discovered, appropriate measures should be taken to eliminate the opportunities for hacking into sensitive data, compromising computers, or spreading malware and viruses.

As the forthcoming Olympics brace themselves for more spirited attacks than those at the previous Games, reinforcing the IT infrastructure has been a key priority. For example, Japan will be carrying out more than six cybersecurity drills a year before 2020, to ensure its infrastructure is impenetrable.

With a solid monitoring, response and prevention plan, the chances of hacking critical IT infrastructure like public Internet sources and ticketing systems at the Olympics are well reduced.

For more information on cybersecurity guidelines for smart city technology requirements, refer to our previous research on technology adoption safety in smart cities: https://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf

5.3. Smart crisis management

When an attacker targets an environment, a prolonged process unfolds from the initial intrusion through to an eventual data breach, if the threat actor is left undetected. The impact could be minimized if the attackers are detected in an early stage, reducing the mean time to detect (MTTD) and the mean time to respond (MTTR) where threats are detected and terminated early in their lifecycle, thereby avoiding downstream consequences and costs. A cyber crisis lifecycle typically involves the following steps:

1. Preparing for a cyber incident: This involves typically preparing during the peace times. A smart city should be ready with cyber incident response plans and effectively conduct regular mock drills to ensure stakeholders are fully aware and ready for actual incidents.
2. Detection of a cyber incident: The information security measures should be able to detect and identify a cyber incident or crisis. Notifications about cyberattacks could also come from third parties such as Homeland Security, MI5, and other cybersecurity agencies set up by regional and national governments.
3. Cyber incident response: When a cyber incident is reported, the incident response program is activated, and a response team is assigned to coordinate the investigative processes and an incident response plan.
4. Ongoing investigation: When an investigation is ongoing, reporting on findings should be well coordinated and reported to the relevant parties, and threat intelligence should enable a better understanding of the attacks and their goals. Other local governments may be at risk as well, and mutual aid agreements, as well as non-disclosure agreements, should be established.
5. Involvement of third parties: external experts should be contacted for investigative support. These should be ready to get involved in investigations, and be a point of reference with technological or cybersecurity vendors. External experts can support in validating investigative results, confirming vulnerabilities and supporting remediation measures. Experts could have witnessed similar attacks in the past, and could provide quality advice to accelerate response and recovery.
6. Containment plan: When an investigation reaches a certain understanding of the attack severity and scope, a containment plan should be pushed to isolate affected parties or systems and recover operations.
7. Communication with appropriate government authorities: National security's involvement in incidents could happen in the early stages or the later stages of attack, depending on the case security and support needed. National security agencies can support the Games in different ways: e.g. requesting collaboration from other countries in investigating attacks or tracing attackers...
8. Notification of stakeholders: When the nature and scope of a cyber-attack is known, the city must reach out to affected stakeholders to notify them of the attack and how they have been affected, in addition to other measures required.

9. Full remediation: The smart city would then develop and deploy a remediation plan, customized for the attack case, enabling the full recovery of services and blocking the threat

For more information on smart city cyber crisis management, refer to our previous research: https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-SCCCM.pdf

6. Conclusion

The Olympics are indeed spurring the advancement of technology all over the world. At every Olympics event, we usually witness a showcase of amazing and futuristic technologies.

Because of the extensive use of technology at the Games, they have attracted a high number of malicious hackers trying to find a way of breaking systems and causing havoc. Consequently, at every Games, organizers usually carry out comprehensive security planning to eliminate weak points and make their systems impenetrable.

At the Games, we see innovation in the cybersecurity solutions and controls put in place, in order to get ahead of attackers at both an Olympic and country level. Such measures are important to guaranteeing the safety and experience of the Olympics viewers, attendees, employees, judges, contenders and their crews.

Without the Olympics, there could be no impetus to propel the quick growth of various technologies. With extensive cybersecurity planning, the Olympics are kept safe, and the global deployment potential of technologies are demonstrated.

Nevertheless, the Games are becoming extensively technology dependent and their attack surface is therefore intensively expanding. Can the Olympics keep up with these challenges and maintain technological evolution through the use of effective preventive measures?