CASE STUDY: HOW CYBERSECURITY AND DEVELOPING TECHNOLOGIES ARE REDEFINING THE SECURITY OF GLOBAL EVENTS IN THE TWENTY-FIRST CENTURY

Paul Burnham, *Protect and Prepare Ltd*

ABSTRACT: *As technology becomes increasingly advanced and widely accessible the threat of cyberterrorism grows exponentially. Whilst technologies such as drones, centralised intelligence and digital procedures were initially used to enhance security and aid organisation managers in designing, constructing and securing global events, over time this technology is becoming increasingly weaponised and is now considered one of the most severe global terrorism threats. Testing, planning and strategising has already begun for the 2024 Summer Olympics in Paris, with a focus on how to best respond to drone threats in particular in a swift and safe manner, whilst India has previously experienced incidents in which drones have been used to remotely deliver and detonate explosive devices. The proliferation of technological capabilities and cyberterrorism 'training' has resulted in threats that are hard to detect, track, and stop. This article will explore best practice in how to effectively respond for the MENA region, and how protocols for global events has shifted to meet new technological threats, and the implications for those planning large-scale events. Whilst technological developments may offer the greatest of advantages in warfare, they have come to represent one of the greatest threats of global terrorism and understanding how 'over the counter' technologies are contributing to this is essential for ensuring future sporting events in the region are delivered securely.*

Key Learning Objectives:

- To identify the risks presented to mega events by cybercrimes/terrorism
- To identify the risks of drone technology for incorporation into event planning
- To analyse the complex balance of utilising technology to aid security, without creating new areas of vulnerability
- To identify strategies and recommendations for the Qatar 2022 World Cup, and the implications for the MENA region

INTRODUCTION

As rapid and exponential growth of technology has redefined many aspects of modern-day society, the growth of cloud services, security software and new physical technologies have enabled new systems and protocols to develop and enhance security for mega events. What this has also produced, is a new weapon for those with sinister intent, be that from a criminal or terrorist perspective. Indeed, the nature of cyberthreats is particularly difficult to manage, due to the 'unclear and problematic' understanding of what this term means.[1] The challenge of addressing cybersecurity was perhaps best explained by former FBI Director James Comey in 2015;

> *'Let me start by telling you what you know, which is that everything has changed in ways that are so fundamental that it's difficult to describe what it means when we say the world is changing because of cyber. Now, I find that in all things cyber there's a lot of nodding and I worry there's not a lot of understanding behind the nodding at times.'*[2]

The fact is that cyber security has been used to refer to such a range of issues, and that new cyber software, technologies and methods are evolving at a rate at which it is becoming impossible to maintain one encompassing definition. Similarly, the use of 'cloud-based technology' has evolved rapidly, whilst the security and safety of these systems has not kept pace.[3] For the purpose of this case study, we will be focusing primarily on the security of data held in 'the cloud.' The definition of cloud-based computing will be used as follows:

> *the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.*[4]

[1] Giulianotti R, Klauser F. Sport mega-events and 'terrorism': A critical analysis. International Review for the Sociology of Sport. 2012;47(3):307-323. doi:10.1177/1012690211433454

[2] Comey J, Director of FBI, Addressing the Cyber Security Threat, Speech delivered to International Conference on Cyber Security, Fordham University New York City, New York January 7, 2015, Transcript available at https://nsarchive.gwu.edu/sites/default/files/documents/5986971/National-Security-Archive-Department-of-Justice.pdf

[3] Takeshi Takahashi, Youki Kadobayashi, and Hiroyuki Fujiwara. 2010. Ontological approach toward cybersecurity in cloud computing. In <i>Proceedings of the 3rd international conference on Security of information and networks</i> (<i>SIN '10</i>). Association for Computing Machinery, New York, NY, USA, 100–109. DOI:https://doi.org/10.1145/1854099.1854121

[4] Definition provided by Oxford Languages, hosted by Google.com

This case study will also examine the impacts of developing drone technologies, and the potential uses for securing events through this new technology, and the risks it poses when used with malintent.

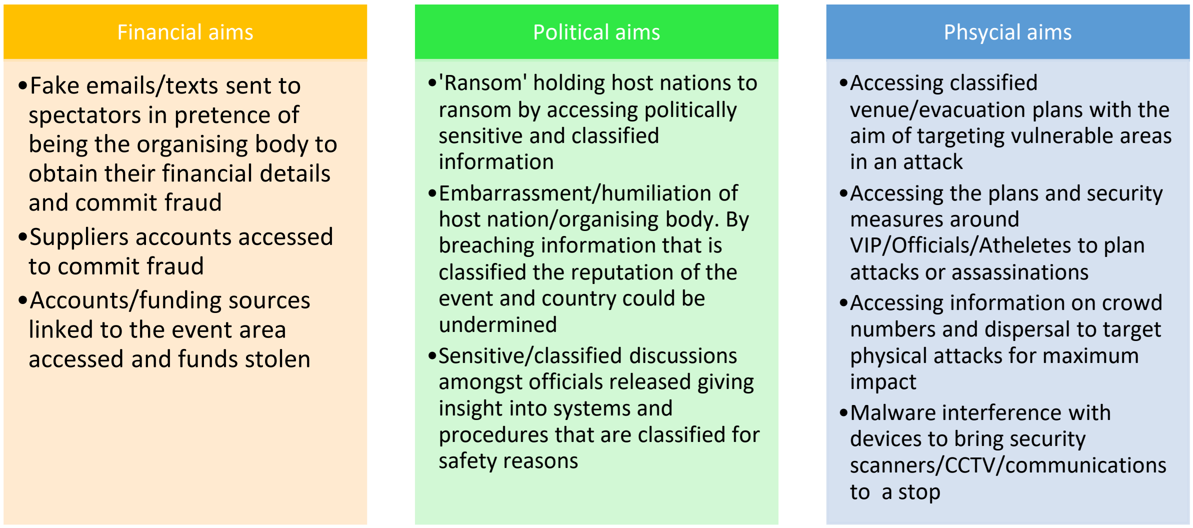
It is widely acknowledged that mega-events have become huge targets for a range of criminal and terrorist activity; everything from the threat of physical violence to the violation of sensitive documents in increased by the size and status of events. Indeed, the security implications of hosting such an event have been identified by some as a contradiction of the peaceful and cooperative message intended behind global sporting events.[5] Traditional planning for elements such as venue design, evacuation routes and emergency service protocols have become assumed starting points for hosts, and alongside this in the modern day sit plans and systems for securing the sensitive data which is now stored digitally.[6] This has inevitably driven the focus on cybersecurity currently taking place in Qatar, as they aim to secure the vast quantities of data associated with hosting the Qatar 2022 FIFA World Cup.[7]

The threat posed by cyber-attacks include financial, political and physical threats, all made possible through illegal access and theft of sensitive data. Attacks may be targeted at the events hosts or suppliers themselves, or at attendants, whose data has been collected and processed during the event organisation process. Examples of each type can be found below in Figure 1, although these are by no means exhaustive, they serve to give a sense of the scale and range of cybercrime that target global events.

[5] Handelman, Don. 2016. "Prologue: Olympic surveillance as a prelude to securitization." In Bajc, Vida (ed.). Surveilling and securing the Olympics. London: Palgrave Macmillan: 5.

[6] Ibid.

[7] Tabassum, Aliya & Mustafa, Mohammad & Maadeed, Ali. (2018). The Need for a Global Response Against Cybercrime: Qatar as a Case Study. 10.1109/ISDFS.2018.8355331.



Financial aims

- Fake emails/texts sent to spectators in pretence of being the organising body to obtain their financial details and commit fraud
- Suppliers accounts accessed to commit fraud
- Accounts/funding sources linked to the event area accessed and funds stolen

Political aims

- 'Ransom' holding host nations to ransom by accessing politically sensitive and classified information
- Embarrassment/humiliation of host nation/organising body. By breaching information that is classified the reputation of the event and country could be undermined
- Sensitive/classified discussions amongst officials released giving insight into systems and procedures that are classified for safety reasons

Phsycial aims

- Accessing classified venue/evacuation plans with the aim of targeting vulnerable areas in an attack
- Accessing the plans and security measures around VIP/Officials/Atheletes to plan attacks or assassinations
- Accessing information on crowd numbers and dispersal to target physical attacks for maximum impact
- Malware interference with devices to bring security scanners/CCTV/communications to a stop

Figure 1:Varying aims of Cyberattacks

Perhaps the most concerning aspect of cyber threats for mega-events lie in the ability to carry out a huge number of successive attacks in a very small time period. It is estimated that during the Beijing 2008 Olympic Games there were on average 12 million attempted cyberattacks every day.[8] In the build up to the Tokyo 2020 Summer Olympic Games organising bodies analysed the cyber '*environments and systems of the previous three Olympic games, using this understanding to inform their own policy specific to the Olympic event*'.[9] This heightened emphasis on the cybersecurity of global mega-events is not only appropriate in resisting breaches of security, but also in utilising the possibilities modern technology offer in consolidating it.

An exacerbating factor for cyberthreats and the upcoming Qatar 2022 FIFA World Cup has been the Covid-19 pandemic.[10] Ongoing research has identified that the number, frequency and uniqueness of cyberattacks carried out since the onset of the global pandemic have increased and, whilst the underlying causes of this may still be unknown, this will be an important consideration for cyber-preparedness when hosting events in the near-future.[11] As

[8] Ormsby A (2010) London Olympics 'unavoidably attractive' for cyber attacks. Reuters, 25 November, available at: http://uk.reuters.com/article/idUKTRE6AO2QY20101125 (accessed 20 January 2011).

[9] Polak-Rottmann, Sebastian. (2020). Security for the Tokyo Olympics. 10.4324/9781003033905-32.

[10] Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, Xavier Bellekens, Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyberattacks during the pandemic, Computers & Security, Volume 105, 2021, 102248, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102248

[11] Ibid.

events have moved to provide increasing focus on both virtual and hybrid experiences and the use of apps and digital documentation to reduce contact between people, there have been created extra opportunities for malicious cyber activity.

BUILDING FOUNDATIONS OF DATA SECURITY FROM ABOVE; THE IMPORTANCE OF REGULATION AND COMPREHENSIVE LAWS

Frequently identified as the biggest challenge in ensuring data security is maintaining policy which keeps up with the technology, complexity and transient nature of the field. Regulators face a constant battle to update legislation and are often reacting to new threats and thus playing 'catch-up' with those looking to access sensitive data[12]. The challenge is heightened for mega-events as organisers are handling data from across the globe, where policy between nations may vary vastly.[13] Cross-border cloud security complicates the process of processing data, and organising bodies are required to uphold the data rights of the end-user in their domestic location.[14]

Research carried out in the lead-up to the Qatar FIFA 2022 World Cup has indicated a high public confidence in the hosts ability to secure the cyber element of the games, and perceptions of policymakers tend to acknowledge the nation as becoming more proactive in addressing cybersecurity as the games approach.[15] Qatar has shown a focus on increasing the reach of data policy, from adopting Law No. 13 in 2016 (Protection of Personal Data Privacy; the Data Protection Law), to the 2021 update on Personal Data Privacy Protection Law (the Guidelines).[16] The update has provided great guidelines for organisations in securing data, but does not go so far as binding required practices as legal obligations, instead serving more as clarification of data protection methods and expectations.[17] As the first country in the Middle-East to enact such policy relating to data protection, Qatar is undeniably at the forefront of policymaking for cybersecurity in the MENA region.[18]

[12] Kaufman L. M., "Data Security in the World of Cloud Computing," in IEEE Security & Privacy, vol. 7, no. 4, pp. 61-64, July-Aug. 2009, doi: 10.1109/MSP.2009.87.

[13] Berry, R. and Reisman, M., 2012. Policy challenges of cross-border cloud computing. *J. Int'l Com. & Econ.*, *4*, p.1.

[14] Owens J, Project Manager - Cloud, Cyber Security and Information Security, Interviewed by Protect and Prepare Ltd.

[15] Khalifa, N. A.-D. (2020). Identification and prevention of expected cybersecurity threats during 2022 FIFA World Cup in Qatar. *Journal of Poverty, Investment and Development*, *5*(1), 49 – 84. https://doi.org/10.47604/jpid.1135

[16] Lusardi R, Khaled A, Qatar Data Protection Guidelines: Update, The National Law Review, April 26 2021, K&L Gates, https://www.natlawreview.com/article/qatar-data-protection-guidelines-update

[17] Ibid

[18] Higham E, Keane L, Ooijevaar M, Wilkinson D, New regulatory guidelines on the Qatar Personal Data Protection Law, Clyde & CO March 2021 https://www.clydeco.com/en/insights/2021/03/new-regulatory-guidelines-on-the-qatar-persona-1

The next step for policy on Qatar will be on the process of enforcement of their new regulations, and collaboration with FIFA regarding how data is handled regarding the 2022 World Cup. It is vital that all stakeholders and organisations involved in the process of the games protect any data relating to the event, and this would be best done through policy that was both nationwide and compulsory for all those interacting with Qatari organisations.[19] No involvement is too small to be considered, as the security of data relies upon a thorough and complete securitisation of the cloud and all data pertaining to the event. Suppliers, service providers, staff and government departments all hold important data in their roles, and a blanket law which is strongly and effectively enforced would ensure all are meeting the same standards of security.

For more detail of current data laws in Qatar see:
https://www.lexology.com/library/detail.aspx?g=459eefaa-b2c2-454d-9d6e-c9a8ff3fd072

FIFA has extensive and transparent policy regulations outlined for a range of groups on a targeted site for data protection information.[20] Qatar could use the collaboration as an opportunity to develop best practice through international collaboration, using FIFAs existing framework to develop their own policy which can continue beyond the 2022 World Cup itself. As the organising nation there will be a strong expectation and focus on Qatari cybersecurity, and failure to protect the information of the hundreds of thousands involved in planning and attending the games could result in severe damage to the reputation of Qatar as a host nation.

[19] Scoular M, Protect and Prepare Ltd. Interviewed 23/10/2021

[20] FIFA Data Protection Portal, Accessed 23/10/2021 https://www.fifa.com/data-protection-portal

WHAT DATA DOES PLANNING FOR A MEGA-EVENT INVOLVE, AND WHAT ARE THE RISKS OF BREACHES?

The obvious sensitive data involving hosting mega-events are perhaps the ones which we link to terrorism and physical threats, venue plans, evacuation routes, security systems and emergency services intelligence. It is also worth noting the enormous range of individuals involved in organising the games; when you consider the number of staff, construction workers, service provides and members of the organising body there are thousands of potential ‘leak points’ in the data. Each individual has access to, or knowledge of, sensitive information, and if they do not handle this properly it makes mega events an attractive target for criminals.

Whilst these are of course pieces of data that need unbreachable security, there is a plethora of other data that needs to be kept safe alongside this information. Again Figure 2 serves to give an idea of the range of data held but is by no means exhaustive. Each example given in Figure 2 could be dangerous if in the wrong hands, and there are two main strains of intent for mega events to be concerned about; criminal activity and terrorism.[21] The terrorism strain encompasses the possibility that those who access sensitive data may use it to exploit vulnerabilities in the event itself, and to carry out acts of terrorism in a physical sense. The criminal strain is the use of hacking into to data with the intention of committing fraud, theft or extortion, and may target attendants or the organisers themselves.[22]

[21] Owens J, Project Manager - Cloud, Cyber Security and Information Security, Interviewed by Protect and Prepare Ltd.

[22] Ibid

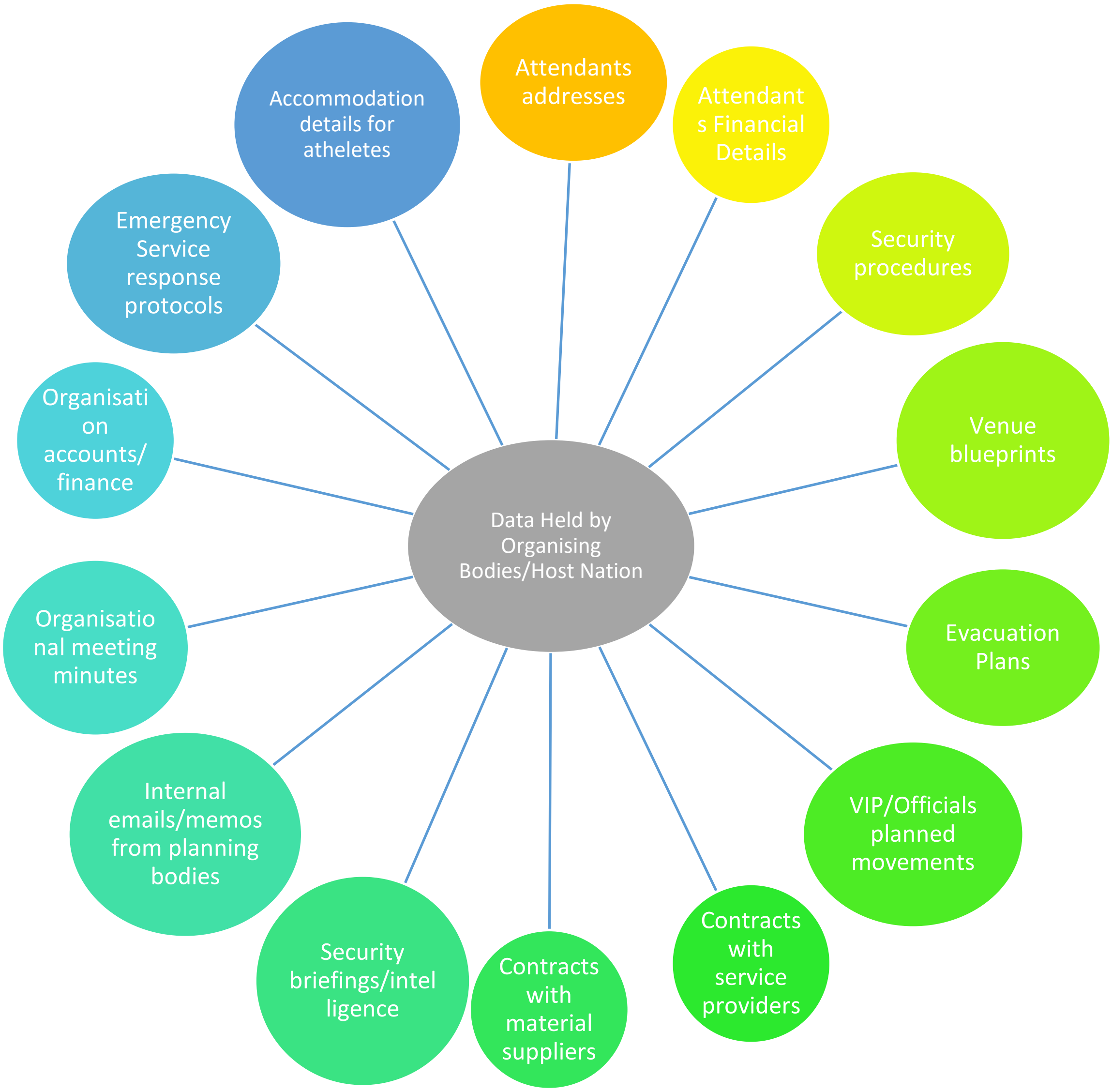

Data Held by Organising Bodies/Host Nation
Attendants addresses
Attendant s Financial Details
Security procedures
Venue blueprints
Evacuation Plans
VIP/Officials planned movements
Contracts with service providers
Contracts with material suppliers
Security briefings/intel ligence
Internal emails/memos from planning bodies
Organisatio nal meeting minutes
Organisati on accounts/ finance
Emergency Service response protocols
Accommodation details for atheletes

Figure 2: Examples of data held by host organisations

Criminal intent and mega-event data

The nature of planning an event means that within the cloud there is a huge quantity of sensitive data stored not only about the event itself, but also those in attendance. This makes criminal activity easier to carry out as hackers can choose to target individuals directly, through 'phishing' or malware links sent in emails. An example of this could be emails sent to spectators under the guise of information sent from host organisations, which then capture sensitive personal or payment information, and go on to use this to commit fraud. The Covid-19 pandemic, whereby attendance at events has required frequent collection of data from attendants has been a requirement, has created an acceptance and expectation of such emails from hosts and thus increased the 'believability' of these scams.[23] The other potential uses range from holding a list of homes likely to be empty on specific dates whilst they attend the event, to personal details that can be used to open new credit accounts in an individual's name.[24] Criminal intent can continue to take place over a prolonged period of time, as the data that has leaked may be shared and passed on between cybercriminals, and therefore cybercrime in relation to mega events can be long-lasting as well as far-reaching.[25]

Similarly, criminals may gain access to financial details of organising bodies by accessing documents such as contracts or accounting documents stored in the cloud and carry out cyber-attacks on the organisation's own finances.

Once criminals have access to a database of ticketholder information, they have an enormous pool of targets for which cybercrime can be committed. In this instance the host organisations would be held accountable for the data breach, as they are expected to responsibly secure and protect such data, as explored in the previous section.

Terrorism intent and mega-event data

The opportunity for terrorists to utilise classified information is widely known, and the implications of a terrorist breaching the cloud could be catastrophic for an event.[26] The focus of this strain is on accessing data which could expose the vulnerability of venues and safety protocols, creating a 'chink in the armour' in which harm could be done.[27] For example the venue plans may enable those wishing to carry out attacks to identify best points of entry, or areas with maximum impact on human life. Similarly, information pertaining to the evacuation of venues or the multi-agency response protocols may enable terrorists to maximise the loss of human life through deliberately disrupting these plans.[28] This is a particular vulnerability where new venues have been constructed specifically for events, as

[23] Ibid

[24] Scoular M, Protect and Prepare Ltd. Interviewed 23/10/2021

[25] Owens J, Project Manager - Cloud, Cyber Security and Information Security, Interviewed by Protect and Prepare Ltd.

[26] Ibid

[27] Scoular M, Protect and Prepare Ltd. Interviewed 23/10/2021

[28] Ibid

the amount of planning documents in the cloud is increased, and their systems and protocols are less ‘tried and tested’ than pre-existing venues.[29]

Additional targets for attack are present at mega events due to the very large number of high-profile officials, celebrities and athletes in attendance. If potential attackers gained access to the planned protection, itinerary and location of such individuals, they could target attacks at specific individuals for political or symbolic killing. [30] This information, once stolen, can be shared between terrorist individuals or organisations across cyberspace, making it impossible to know who has seen such documents.[31] Like criminal activity, the internet itself has become a hive for recruitment and organisation of terrorist groups, and this sharing of stolen information would pose a real threat to the physical security of the games.[32]

Whilst the uses described above address the risk posed by those planning a physical attack at the event, this does not mean the threat passes after the game ends. Once sensitive information about venues and security protocols is leaked there continues to be a threat for future events, and for the organising bodies involved in the games.

[29] Owens J, Project Manager - Cloud, Cyber Security and Information Security, Interviewed by Protect and Prepare Ltd.

[30] Ibid.

[31] Bieda, D., & Halawi, L. (2015). Cyberspace: A Venue for Terrorism. *Issues in Information Systems, 16*(3). Retrieved from https://commons.erau.edu/publication/304

[32] Ibid

PHYSICAL TECHNOLOGIES AND IMPLICATIONS FOR SECURITY AT MEGA-EVENTS

The development of new technologies, and the increased accessibility of advanced devices has had huge implications for mega-events. Access to devices that can host apps, be used aa a payment method and hold important documentation have revolutionised the processes surrounding event entry. Mobile phones, I-pads and other portable devices have visibly altered the way we access and experience events and have added new layers to security considerations when hosting a global event.

Less widely known to the public has been the development of drone technology; and it is this specific technology this case study will consider when discussing the impact of technological advancements on event security.

Accessibility:

Perhaps the biggest driving force behind use of drone technology is the rate at which it has become accessible on the 'high street.'[33] Equipment that is a 'decent drone' can be picked up from high street stores for around £500, meaning that proliferation of the technologies has been rapid and far-reaching.[34] Private sales, or a lack of monitoring by sellers mean that large numbers of drones are owned privately 'off-record' in the UK, making it very hard to monitor their usage and ownership.[35] The Civil Aviation Authority have developed regulations and laws for the registration of drone devices using expert advice, but they have been on 'the back-foot' at times, trying to catch up with technology already out there.[36] The devices themselves are fairly easy to track, and central authorities such as the CAA can detect nefarious activities relatively easily.[37] What is proving more difficult is when people are buying

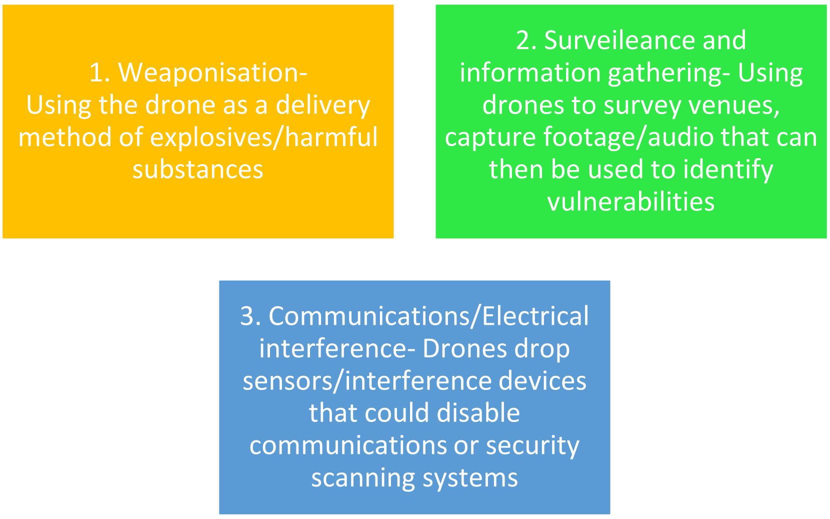
[33] Rainford C, Drone Pilot and Specialist, Advised UK Fire Brigades, MoD, Police Forces to establish dedicated Drone Security teams, Interviewed by Protect and Prepare Ltd.
[34] Ibid.
[35] Cashmore A, Retired Group Commander National CBRN Centre, Previously Unmanned Aerial System (UAS) Manager within the Technical and Operations Support Directorate of West Midlands Fire Service, Interviewed by Protect and Prepare Ltd.
[36] Ibid.
[37] Ibid.

the elements of a drone and then self-building devices, making them harder to register and track.[38]

The impact of this for modern-day organisers is an added ‘sphere’ of required understanding and preparation when planning a mega event. Where previously the main areas of planning were on logistics such as venue plans and staffing, organisers now must be equipped with adequate technological knowledge to understand drones and mitigate the risks they pose. The knowledge of the technologies, the intent behind their usage and the methods by which they can be utilised to damage an event are now fundamental for all aspects of planning, from data or information leaks all the way to physical threats.

Risks:

The use of drones to threaten the security of an event can be identified as 3 core usages.



1. Weaponisation- Using the drone as a delivery method of explosives/harmful substances

2. Surveileance and information gathering- Using drones to survey venues, capture footage/audio that can then be used to identify vulnerabilities

3. Communications/Electrical interference- Drones drop sensors/interference devices that could disable communications or security scanning systems

Weaponisation:

Using drones as a direct physical weapon is an increasingly explored area of technology both from the perspective of those fighting against terrorism, and the terrorists themselves.[39]

[38] Ibid.

[39] Pledger T, THE ROLE OF DRONES IN FUTURE TERRORIST ATTACKS, Association of the United States Army, February 2021 https://www.ausa.org/publications/role-drones-future-terrorist-attacks

Weoponising a drone is expensive, and requires very technical knowledge, making it more likely to be a method used by organised terrorist groups, and less likely to be used by standalone 'lone wolf' attacks.[40] There have been previous uses of drones for violent means by non-government organisations, such as the attempted assassination of the Venezuelan President in 2018, or the attack on Russian military bases in 2018.[41][42] In these instances the drone itself is carrying out the attack, enabling the attacker to remain away from the event, increasing the possibility of attracting attention prior to the attack, and evading detection after the attack.[43] This can make reacting to a drone threat complex; in the UK the CAA regulations mean it is illegal to simply shoot down or destroy a drone threat as there are implications for potential casualties when it lands/explodes. Therefore, a huge consideration for event organisers is on how to detect weaponised drones early, giving time to consider evacuation/lockdown of areas to mitigate the threat.[44] Those in charge of event security must possess and up-to-date and in-depth knowledge of drone technologies and how they have been weaponised, in order to fully inform safety planning for all possible methods of attack.

<u>Surveillance:</u>

The use of drones as surveillance equipment presents a huge threat to the security of global events. Drones equipped with cameras and listening devices can capture information pertaining to venue layout, security scans and procedures and can be used to help identify areas of vulnerability both within and surrounding event locations.[45] Similarly to weaponization the ability for the perpetrator to remain distant from the location of the information gathering offers them enhanced protection from being identified by security services, and this 'over the fence' information can go on to inform physical threats for terrorist related intentions.[46] Drones are widely used by security/military organisations as surveillance

[40] Rainford C, Drone Pilot and Specialist, Advised UK Fire Brigades, MoD, Police Forces to establish dedicated Drone Security teams, Interviewed by Protect and Prepare Ltd.
[41]https://www.bbc.co.uk/news/world-latin-america-45073385
[42] https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html
[43] Scoular M, Protect and Prepare Ltd. Interviewed 23/10/2021
[44] Cashmore A, Retired Group Commander National CBRN Centre, Previously Unmanned Aerial System (UAS) Manager within the Technical and Operations Support Directorate of West Midlands Fire Service, Interviewed by Protect and Prepare Ltd.
[45] Ibid.
[46] Rainford C, Drone Pilot and Specialist, Advised UK Fire Brigades, MoD, Police Forces to establish dedicated Drone Security teams, Interviewed by Protect and Prepare Ltd.

tools, informing targeted killing of enemies.[47] It is perhaps not surprising then that those with violent intend toward an organisation or civilians are utilising the technologies in the same way. Event managers now need to consider not only who is in the room during sensitive discussions or planning, but also whether there could potentially be devices present which place that information at risk of leaking. Good practice would be to utilise counter-surveillance technologies such as scrambling devices throughout planning stages, and organisers should be made aware of the importance of sensitive data being stored and discussed within specified areas, or at specified times whereby checks have been taken place prior to discussion.

Interference:

Drones as tools of interference would be particularly problematic for mega events. If a drone could access an area and use malware/hardware that interfered with the communications or electronic systems of a venue it could generate disruption, or indeed mass panic.[48] Terrorists primarily seek to spread terror, and even the presence of a drone which then disrupted event systems could incite mass panic and stampedes from venues.[49] In these instances if response agencies are unable to communicate due to their systems being disrupted, you can maximise the harm done by delaying emergency service collaboration. Drones as a means of 'scrambling' the technology within the stadium could go as far as disabling security scanning equipment, cutting off both internal and external communication networks (both walkie-talkies and mobile phone signal) and generate an environment whereby the panic produced couple with the obstacles for responders generates a physical harm threat.

Geofencing and preventing drone threats:

Given the aforementioned potential use of drones, it is not an exaggeration to state that mega event host nations need to have rigorous and carefully considered counter-drone policies and

[47] Matthew Ayamga, Selorm Akaba, Albert Apotele Nyaaba,
Multifaceted applicability of drones: A review, Technological Forecasting and Social Change, Volume 167, 2021, 120677, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2021.120677

[48] Rainford C, Drone Pilot and Specialist, Advised UK Fire Brigades, MoD, Police Forces to establish dedicated Drone Security teams, Interviewed by Protect and Prepare Ltd.

[49] Ibid

technologies in place. Geofencing is the most widely used counter drone technology and involves creating 'safe zone' areas where drone technology is unable to operate.[50] Geofencing is a preventative measure, which seeks to mitigate the risks drones pose before they are able to gain access to either the intended information or venue they are targeting. A combination of drone detection and interference technologies combined can be used to create a barrier around venues and locations which require protection, measures that in the current technological age are deemed as a necessity for high profile locations and events.[51]

Mega event locations will need to be 'smothered' in this preventative technology, and also maintain a continuous monitoring an information feed of the surrounding airspace, carried out by specifically trained drone-specialist staff.[52] Specialist trained drone units are increasingly becoming embedded into emergency services around the world, and their presence at mega events can help inform the wider security protocols in relation to drones, and also provide effective and efficient reactive protection if a drone threat is detected. Organisers should thoroughly research the uses of geofencing and understand how to deploy such technologies and maintain their integrity.

[50] Rainford C, Drone Pilot and Specialist, Advised UK Fire Brigades, MoD, Police Forces to establish dedicated Drone Security teams, Interviewed by Protect and Prepare Ltd.

[51] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," in IEEE Communications Magazine, vol. 56, no. 4, pp. 68-74, April 2018, doi: 10.1109/MCOM.2018.1700430.

[52] Rainford C, Drone Pilot and Specialist, Advised UK Fire Brigades, MoD, Police Forces to establish dedicated Drone Security teams, Interviewed by Protect and Prepare Ltd.

RECOMMENDATIONS FOR THE QATAR FIFA WORLD CUP 2022:

Implicit Policy and Laws

Perhaps the most important action to be taken is in consolidating existing policies and laws, and creating new ones where gaps are identified. Whilst Qatar has led the MENA region on data policy, there remains a need for explicit policy that dictates the must have/have nots of handling cyber security and data. Enforcement of these policies must be consistent and real repercussion for non-compliance should be made clear in future laws pertaining to this area. Policymakers need to liaise with the event specialists (FIFA) as well as experts in the cybersecurity field to ensure laws secure the vast cyberspace surrounding the 2022 World Cup and continue to provide security for Qatari events in the future. Recommendations and checklists are a good starting point for outlining the expectations of cybersecurity and the responsibilities private organisations have but moving forward there need to be 'black and white' regulations which can be nationally and internationally applied to all those operating in or alongside Qatari organisations.

In relation to drone technologies policy needs to be informed with the most up-to-date information from both a technological, and intelligence perspective. Current drone policy uses subjective terminology such as 'do not fly over crowds/ respect privacy of others and this general approach can create grey areas or loopholes by which drone activity is not as closely monitored as necessary.[53] Whilst the Qatari CAA does require registration of drone pilots and technologies, the actual regulations on the usage of drones is less specific. These policies will need 'tightening' up to leave no room for movement in drone usage, and enhanced screening by the CAA when granting licenses will help ensure the 2022 World Cup faces a lessened threat from drones.

Education that filters through

The need for education by specialist advisors is obvious; but perhaps the filtering down of this information is less so. Policymakers and event organisers will need to be educated on the most current technologies and their risks, and how to mitigate them. What is necessary for

[53] https://drone-laws.com/drone-laws-in-qatar/

mega events, is for education beyond this. When dealing with specific threats like drones, specialist on-site teams and response units should become embedded into the practices of Qatar when hosting mega events. These units can be drawn from existing agencies such as military/police/fire brigade and can receive specialist training from external agencies.[54]

Similarly, event staff right down to steward level will need to be educated on not just response to physical technology threats, but also the securitisation of their own data and information relating to their work. Organising bodies should ensure that all staff are aware and educated on the protocols surrounding sensitive information (e.g., use of internal email addresses only) and that they know how to quickly report any potential breach in event cybersecurity.

Finally, the education needs to reach the public. There is no doubt that 'Phishing' scams, fraudulent activity and illicit theft of personal data is intensified for those attending a mega event. Educating spectators of these risks, clarifying what legitimate communications will be and how to identify any fraudulent ones will not only help protect customers, but also raise the profile and reputation of the organising body. Reducing the number who fall victim to these scams through education help build trust in the organisations processes, and also provide reassurance of the capabilities of the host nation for future events. This is an especially important opportunity for the Qatari government as they move to the forefront as cybersecurity pioneers in the MENA region and offer a template of good practice for others to follow. The use of national programs funded by the governments of host nations could best spread this message, through awareness campaigns delivered across multimedia channels. Organisers should also take an active role in the process; clarifying upon purchase of tickets how to identify genuine communications and offering tips/hints upon booking confirmation to help the public avoid common phishing/hacking strategies.

<u>The need for frequent review and update</u>

An ongoing theme in the cybersecurity and physical technology space is the pace of change. Regulators are constantly seen as 'one step behind' the latest threats and trends. Methods, tools and legal complexities in cybersecurity are constantly evolving, and policy needs to be

[54] Rainford C, Drone Pilot and Specialist, Advised UK Fire Brigades, MoD, Police Forces to establish dedicated Drone Security teams, Interviewed by Protect and Prepare Ltd.

both reactive and rigorous. Both the FIFA organisation, and Qatari authorities need to be carrying out frequent review of systems and policies, ensuring they reflect the most recent threats and challenges. Regular ‘health checks’ of systems and security enforcements needs to take place, with any identified areas of weakness addressed at the earliest possible chance by leading experts. This will inevitably require investment into the digital infrastructure of the 2022 World Cup, and this investment should continue into the wider Qatari digital environment. Where shortfalls are happening there is an opportunity for learning, so Qatar should ensure analysis and investigation into potential breaches is thorough. It is not enough to ‘fix the hole in the wall’ as a long-term strategy, and instead finding the root cause of these issues will serve both the event itself, and the Qatari authorities best in securing their data and venues.

CONCLUSION

Overall, the cybercrime and technological threat presented to the Qatar 2022 FIFA World Cup reflects the global struggle against such activities. The risks to mega-events that are both created and enhanced by cybercrime and terrorism include data theft, financial and political threats, remote drone attacks and cyberwarfare. These areas are experiencing continuous growth and change and meeting this threat with defence can be daunting and expensive. The threats posed by technology are perhaps unusually complex in that they straddle so many categories of threat from intelligence, data theft through to physical harm. Drone technology in particular has seen significant advances in capabilities and availability in recent years and presents new threats to mega-events, particularly the risk of remote explosive-based attacks.

Ultimately it will take huge investment of time and energy into this space, and this needs to be maintained long after the games have finished. Specialist research into this space, informed by the successes and areas of development ahead of the 2022 FIFA World Cup, should be a priority, and will enable Qatar to continue their positioning as the leader of cybersecurity in the MENA region. Collaboration with experts within existing organisations, and the establishment of specialist teams will be key to success and will help continue what has thus far been a thorough and considered approach to securing data in the country.

The utilisation of advanced technologies to aid the security of events is an undeniably powerful tool in the arsenal of organisers, although it is perhaps ironic that these can create new vulnerabilities and areas of risk for those with negative aims. Ultimately the host organisation will need to remain several steps ahead, both in terms of technology and education, then those using technology to threaten such events, a challenge which may seem impossible in a space where rapid change and development have defined the nature of the threats posed.

Teaching Notes

***Introduction**: The following activities are designed to help you achieve the objectives of this case study. They encourage you to develop your thinking around technology, cybersecurity and drones in relation to event planning, and require application of analytical thinking and careful evaluation. Try to remember that the topics covered in this case study form only one element of the considerations organisations need to take when planning a mega event, and that the reality of planning such events is a huge complex and multi-layered task.*

What are the motives behind cyberattacks targeted at organisers of mega events?

- *Financial:*
    - *Theft of personal data of spectators to open accounts in their name/commit fraud*
    - *Theft of financial data of spectators to steal funds directly*
    - *Ransom; stealing valuable or private information with the intention of holding the organising body to ransom and demanding payment*
- *Political:*
    - *Unauthorised access to political documents/discussions/communications to gain intelligence on host nation/organisation*
    - *Humiliation/exposure of organising bodies or nations. Using classified information to undermine their reputation/status*
    - *Hold sensitive political information to use as leverage/threat against a nation or organisations*
- *Physical:*
    - *Obtaining venue/event information that would aid the planning of a terrorist attack*

      Obtaining the plans/documents relating to VIP or high-profile attendants to target attacks at specific individuals
    - *Using malware to infect/disrupt security equipment and enable physical threats to enter a venue*

Why is it difficult for nations to prevent cybercrime?

- *Pace of change; the technologies and methods used by cybercriminals are constantly evolving, and unique threats emerge at a very frequent rate.*
- *Complexity of policy; policies are required to be all encompassing and consistent for a region, but also flexible enough to adapt and change at short notice. This constant moving of goalposts makes it difficult to maintain a consistent approach*
- *Cloud based services; whilst the cloud has enabled globalisation, information sharing and improved accessibility to data it has also meant the same for those with nefarious intent. There is no longer a need for the thief to be close to their target, allowing them to operate from a distance and evade detection*

Why are mega events so attractive as a target for cybercrime?

- *They hold such a wide range and large quantity of data. This can range in meeting the needs of low-level criminals such as phishing scammers, all the way through to terrorist agencies looking to inflict mass suffering. The requirement of events to hold data from such a range of sources (attendants, suppliers, venues, staff, sponsors, investors, VIPS) mean there is also a range of interested parties who would access the data*
- *They are often the launch of new systems/venues/processes/technologies. These are less well tested/protected than established systems and may be easier to find a vulnerability to exploit.*
- *The number of individuals required to maintain data security; the thousands of staff and workers involved at all levels of planning represent an individual potential leak point.*

What is the nature of threats presented by drone technology?

- *Weaponization*
  - *Using the drone as a delivery method of explosives/harmful substances*
- *Surveillance and information gathering*
  - *Using drones to survey venues, capture footage/audio that can then be used to identify vulnerabilities*

- *Communications/Electrical interference*
  - *Drones drop sensors/interference devices that could disable communications or security scanning systems*
- *Generating an environment of terror*
  - *The very presence of a drone without explanation would be enough to instigate panic and fear in a mass crowd area*

<u>What are the most important next steps for Qatar to secure the 2022 FIFA World Cup from cyber AND technological threats?</u>

- *Education: ensuring that organisers, staff and attendees are all fully educated in the risks posed by cybercriminals, and that this education informs their decision making and actions before the games*
- *Clarifying and enforcing a rigorous and thorough legal stance for both drone technology and data handling. Laws that go beyond recommendation need to be established and enforced at a consistent, nationwide level.*
- *Investing in a sustainable digital infrastructure. Ensuring Qatar has a fortified core for data and cybersecurity built upon expert advice, that is frequently reviewed and maintained with specialist input and updates. Research in the area needs to continue as a priority, as the cybercrime threat grows exponentially, so too should the defences.*

<u>In a group imagine you are the team in charge of planning protocols for preventing the theft of data/intelligence relating to the event. Draw up a list of 5 'Golden Rules' you will be putting in place to secure the event technologically. Be specific when talking about actions you would take/technologies you would use.</u>

Bibliography

- Bieda, D., & Halawi, L. (2015). Cyberspace: A Venue for Terrorism. *Issues in Information Systems, 16*(3). Retrieved from https://commons.erau.edu/publication/304

- Comey J, Director of FBI, Addressing the Cyber Security Threat, Speech delivered to International Conference on Cyber Security, Fordham University New York City, New York January 7, 2015, Transcript available at https://nsarchive.gwu.edu/sites/default/files/documents/5986971/National-Security-Archive-Department-of-Justice.pdf

- Giulianotti R, Klauser F. Sport mega-events and 'terrorism': A critical analysis. International Review for the Sociology of Sport. 2012;47(3):307-323. doi:10.1177/1012690211433454

- Handelman, Don. 2016. "Prologue: Olympic surveillance as a prelude to securitization." In Bajc, Vida (ed.). Surveilling and securing the Olympics. London: Palgrave Macmillan: 5.

- Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, Xavier Bellekens, Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyberattacks during the pandemic, Computers & Security, Volume 105, 2021, 102248, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102248

- Higham E, Keane L, Ooijevaar M, Wilkinson D, New regulatory guidelines on the Qatar Personal Data Protection Law, Clyde & CO March 2021 https://www.clydeco.com/en/insights/2021/03/new-regulatory-guidelines-on-the-qatar-persona-1

- Kaufman L. M., "Data Security in the World of Cloud Computing," in IEEE Security & Privacy, vol. 7, no. 4, pp. 61-64, July-Aug. 2009, doi: 10.1109/MSP.2009.87.

- Lusardi R, Khaled A, Qatar Data Protection Guidelines: Update, The National Law Review, April 26 2021, K&L Gates, https://www.natlawreview.com/article/qatar-data-protection-guidelines-update

- Matthew Ayamga, Selorm Akaba, Albert Apotele Nyaaba, Multifaceted applicability of drones: A review, Technological Forecasting and Social Change, Volume 167, 2021, 120677, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2021.120677

- Ormsby A (2010) London Olympics ‘unavoidably attractive’ for cyber-attacks. Reuters, 25 November, available at: http://uk.reuters.com/article/idUKTRE6AO2QY20101125 .

- Owens J, Project Manager - Cloud, Cyber Security and Information Security, Interviewed by Protect and Prepare Ltd.

- Pledger T, THE ROLE OF DRONES IN FUTURE TERRORIST ATTACKS, Association of the United States Army, February 2021 https://www.ausa.org/publications/role-drones-future-terrorist-attacks

- Polak-Rottmann, Sebastian. (2020). Security for the Tokyo Olympics. 10.4324/9781003033905-32.

- Scoular M, Protect and Prepare Ltd. Interviewed 23/10/2021

- Tabassum, Aliya & Mustafa, Mohammad & Maadeed, Ali. (2018). The Need for a Global Response Against Cybercrime: Qatar as a Case Study. 10.1109/ISDFS.2018.8355331.

- Takeshi Takahashi, Youki Kadobayashi, and Hiroyuki Fujiwara. 2010. Ontological approach toward cybersecurity in cloud computing. In <i>Proceedings of the 3rd international conference on Security of information and networks</i> (<i>SIN '10</i>). Association for Computing Machinery, New York, NY, USA, 100–109. DOI:https://doi.org/10.1145/1854099.1854121

X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," in IEEE Communications Magazine, vol. 56, no. 4, pp. 68-74, April 2018, doi: 10.11