The 2014 FIFA World Cup and 2016 Olympics in Brazil: Lessons Learned

DYNAMIS EUROPE

Executive Summary

Goal: The goal of the Brazilian military was to guarantee the safety of athletes and spectators against possible security threats to the 2014 FIFA World Cup (FWC) and 2016 Olympic and Paralympic Games.

Challenges: The unique nature of the events presented numerous security challenges. For the 2014 FWC, these included the need to monitor 12 stadiums in 12 cities and the immense number of spectators, which reached almost 3.5 million in total.[1] The Olympic and Paralympic Games entailed a much greater number of events in a more concentrated area, as nearly all competitions took place in Rio. In the latter case, the military was tasked with ensuring the security of 15,253 athletes for the duration of the event.

Results/Solution: The Brazilian military achieved its goal via a Common Operating Picture (COP) that enabled it to integrate GPS, chemical and radiological sensor, incident, photographic and weather data into a single map and dashboard, securely accessible anywhere and on any device. This allowed them to track the real-time location of undercover security operatives, respond to real-time alarms triggered by sensor readings that appeared on the COP map, and monitor all venues simultaneously from a remote location.

Background

Since 2012, the Brazil Army Command (BAC) Centro Tecnologico do Exercito (CTEX) has employed Dynamis' COBRA software as its comprehensive security solution and Common Operating Picture provider for High Visibility Events (HVEs) throughout the country. These events include the 2012 Rio +20 UN Conference, the 2013 Rio visit of Pope Francis, the 2014 FIFA World Cup, and the 2016 Olympic and Paralympic Games. CTEX also utilizes COBRA for all HVE planning, training and exercises.

Case-Specific Security Challenges: 2014 FIFA World Cup

Major international sporting events such as the 2014 FIFA World Cup (FWC) are vulnerable to a unique set of security threats, including:

- Complex, coordinated terrorist attacks
- Violence between antagonistic, overzealous fan groups
- civil unrest/public disorder

All were identified as potential threats to public safety in the months preceding the event.[2]

Several case-specific security challenges also complicated the effort, including:

- The need to monitor 12 stadiums in 12 cities remotely and simultaneously
- The immense population of spectators at each match (average of 53,592)[3]
- Limited mobility within individual venues

1. Kevin Moore (2017) A second 'Maracanazo'? *The 2014 FIFA World Cup in historical perspective*, Sport in Society, 20:5-6, 555-571
2. Donna Wong & Simon Chadwick (2017) *Risk and (in)security of FIFA football World Cups—outlook for Russia 2018*, Sport in Society, 20:5-6, 583-598
3. Moore, *A second 'Maracanazo'?*

DYNAMIS EUROPE

Quick Facts: 2014 FWC

Stadiums: 12

Cities: 12

Total Matches: 64

Average Spectators/Match: 53,592

Total Spectators: 3,429,873

Country Teams & Training Facilities: 32

Volunteers: 15,000

Journalists: 15,000

Case-Specific Security Challenges: 2016 Olympics and Paralympics

The Brazilian military produced a new threat assessment for each HVE, so the primary security threats identified for the 2016 Olympic and Paralympic Games were slightly different from those associated with the 2014 FWC. Of the many possibilities considered, the military evaluated an increase in organized criminal activity in the Rio region and attacks ordered or inspired by prominent, global terrorist organizations such as the Islamic State as the two most likely threats facing the event. Several factors made ensuring security for all stakeholders a major challenge, including the…

- High number of events (65 total championships relative to 1 championship for the 2014 FWC)
- Geographical concentration of athletes and events (all events took place in Rio except a few football matches in 5 cities)
- High number of athletes (total of 15,253)
- Length of the event (17 days for Olympics, 12 for Paralympics)
- Huge number of event-related personnel, including 70,000 total volunteers, 32,300 journalists and 4,500 officials (referees and assistants)

In general, the demand for first responders, equipment and other resources was much greater for the 2016 Olympics and Paralympics than for the 2014 FWC.

Results/Solutions

COBRA's client-based software and web-based platform enabled Army and Navy security personnel to create and monitor a shared Common Operating Picture, empowering them to exercise the following capabilities:

- Track precise, real-time location of undercover security operatives.
- Connect hundreds of Commercial-Off-The-Shelf (COTS) handheld chemical and radiological sensors, carried by security operatives, to the GIS-driven COP. Data was sent to the Emergency Operations Center (EOC) via mobile phones and other web-enabled devices.
- Gather and collate over 2,000,000 real-time GPS-tagged chem/rad sensor readings (mobile and fixed site), displayed in the COP.
- Respond to real-time alarms based on multiple chemical, radiological and weather sensor readings. Sensor readings triggered alarms when they exceeded a certain pre-set threshold. Alarms appeared as color changes on the COP dashboard and updates on the COP map.

5. Ibid.

DYNAMIS EUROPE

Quick Facts: Olympics and Paralympics

Total Championships: 65

Total Athletes: 15,253

Event Length (Olympics): 17 days

Event Length (Paralympics): 12d

Total Volunteers: 70,000

Total Journalists: 32,300

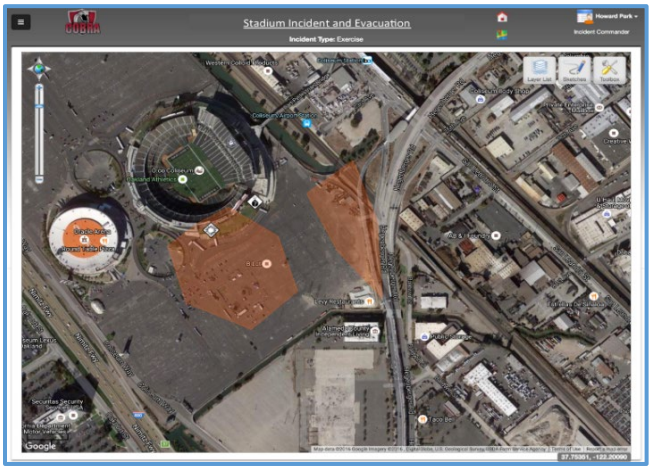
Total Officials: 4,500

Total Countries Participating: 200+

- Gather and upload real-time remote GPS-tagged photographs to the COP.
- Generate and collate real-time operation logs for all participating security elements, allowing for shared incident data in the COP.
- Display all data from multiple venues in real time (simultaneously) on a single COP map and dashboard, accessible anywhere and from any web-enabled device.
- Archive all data and export to common file formats (Excel, Google Earth).
- Utilize numerous response plan/Standard Operating Procedures (SOP), database, checklist, responder data, after-action report and analytic tools provided by COBRA. These aided Army/Navy personnel in conducting capabilities assessments, threat analyses, vulnerability analyses and risk assessments, as well as developing priorities, joint plans and exercises, SOPs and consequence management plans for multiple scenarios.
- Instantaneously sync data across multiple devices (including iPhone, Android, Blackberry and Windows Mobile platforms) and with servers.
- Utilize Stand-Off chemical surveillance tools, in combination with Joint Hazard Assessment Teams (JHATs) strategically positioned around the city, to protect public spaces such as subway stations, hotels and airports from chemical attacks.
- Monitor all facilities in several cities remotely from multiple locations.
- Divide Rio into 4 "clusters" during the 2016 Olympics, each with individual commanders and resources. 3 clusters were under Army control and 1 under Navy command.

In addition to exercising these capabilities, the military also trained thousands of hotel, subway and airport workers in terrorist threat perception in order to enhance the safety of public spaces.

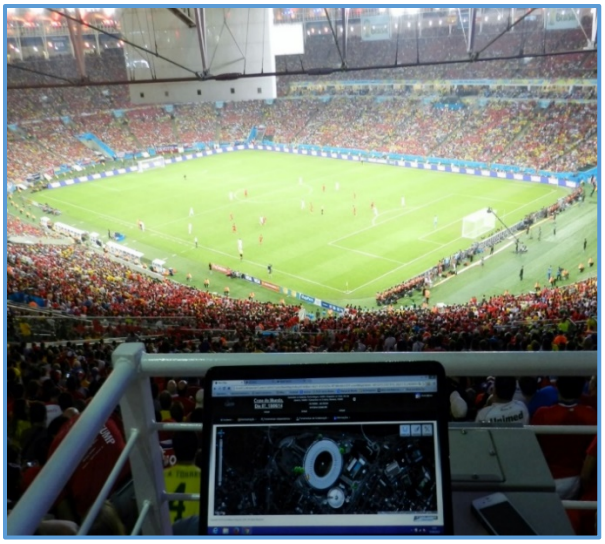
These capabilities allowed CTEX personnel to effectively respond to the daunting security challenges posed by the events. These challenges, including the vast, widespread operational areas that spanned multiple cities and the enormous number of spectators involved, were overcome with the instantaneous communication, remote monitoring and meticulous data collection provided by the COP. A radiological alarm set off in the city of Manaus and a chemical alarm triggered in the city of Maceio during the 2014 FWC demonstrated the effectiveness of the system. Both events ended without any major public safety hazards or security breaches.[5]



Lessons Learned

The Brazilian military applied numerous lessons learned from the 2014 FWC to the 2016 Olympic and Paralympic Games. Many of these lessons concerned the use of chemical and radiological detectors. In many cases, these sensors triggered alarms when there was no real threat, though they were functioning correctly. These false alarms were subsequently attributed to discrepancies in chemical background and other local particularities between the temperate climates where the devices were manufactured and Brazil's tropical climate. These issues were resolved in advance of the 2016 Olympics by updating SOPs and notifying the device manufacturer, who adjusted the devices' chemical libraries. In general, Brazilian security forces also learned the importance of precise calibration and maintenance of these instruments. Another major lesson learned was the paramount importance of interagency collaboration for ensuring safety for large-scale events—that is, coordinating protocols, plans and actions across the armed forces, federal police, health ministry, regulatory agencies, civil defense, security agencies, and intelligence agencies.

Broadly speaking, the ability of the Brazilian military to cover all events during the World Cup was strained due to the large number of sensors and personnel employed, as well as the wide geographic areas involved. To address this concern, Brazil added additional sensors, augmented Army personnel with additional Navy personnel, and deployed updated versions of the software and sensors to enhance radiological identification capacity during the 2016 Olympic Games in Rio. The experience also demonstrated the importance of designing detailed response plans and Standard Operating Procedures in advance of major events. In sum, the Brazilian military came away from the 2014 FIFA World Cup with a greater appreciation for the security value of real-time, remotely monitored sensor networks accessed via a comprehensive, national-level Common Operating Picture for large-scale events.



"During the World Cup, all stadiums were monitored using COBRA software by the Army in ten cities and Navy in two cities. The flexibility of COBRA provided us the capacity to monitor our CBRN sensor networks and deployed response teams at local Command and Control centers as well as the National C2 center in Brasília, providing real time information about the largest CBRN defense operation ever deployed by the Brazilian MoD."

-Cel Paulo Malizia, Chefe da Divisão de Defesa QBN, Centro Tecnológico do Exército