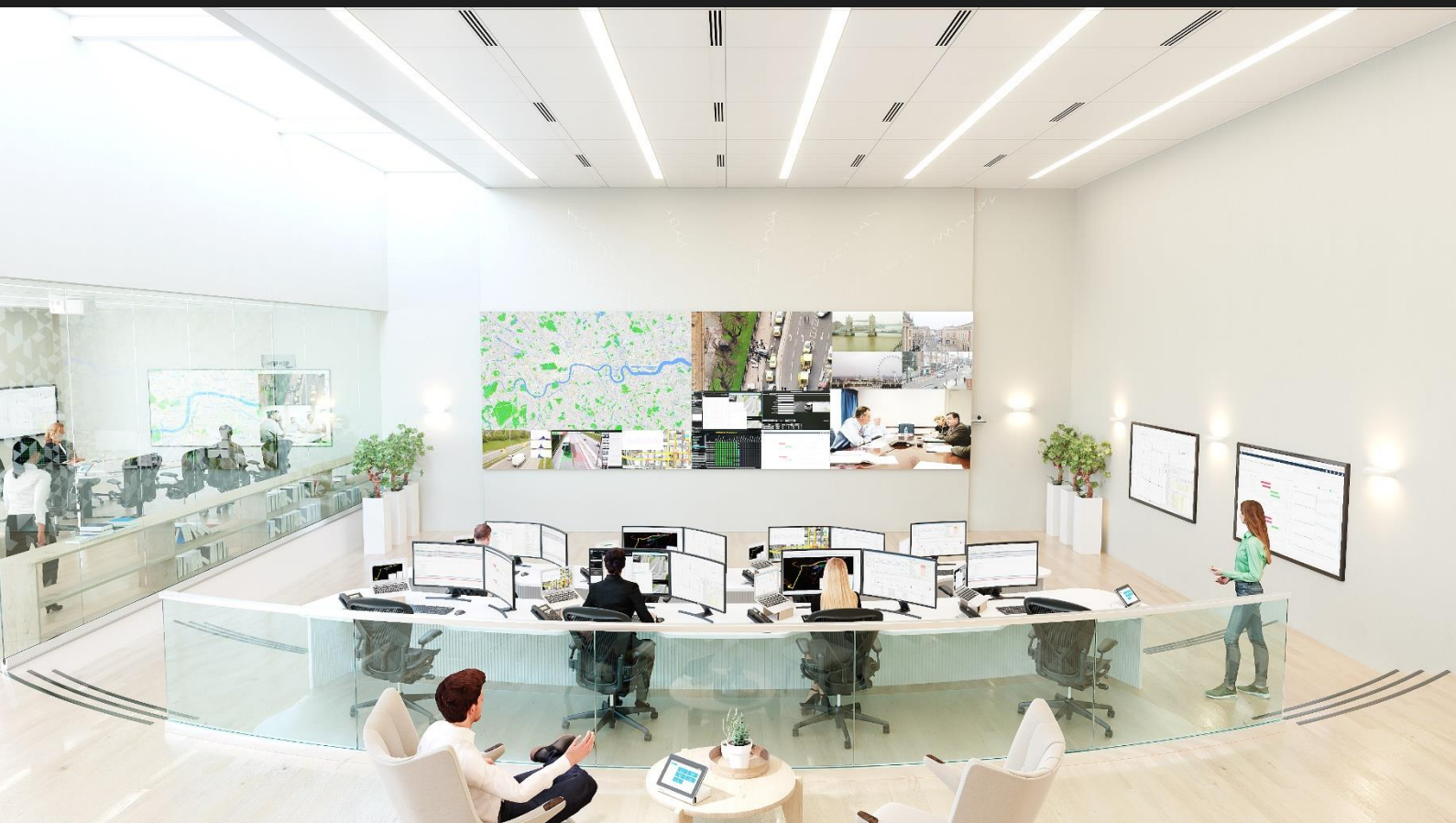
cyviz

WHITE PAPER

# Integrated, dynamic and secure operations centers for Smart Cities

A Smart City is orchestrated by various agencies serving its citizens and businesses.  There is a need to coordinate efficiently and in a timely manner with each other to provide critical services such as emergency and rescue, mobility and transportation, energy, utilities, healthcare, industrial and financial systems.

"There cannot be a Smart City without it being interconnected and secure."



# Executive summary

A Smart City means different things to different people, depending on what aspects of the city we are touching on. Broadly speaking, "being smart" to a large extent can be associated with:

- Having access to better information to make more informed decisions
- Enabling cities to improve the life of its citizens through improved delivery of public services
- Providing solutions to urban growth challenges

Whilst Frost and Sullivan[1] have defined a Smart City as one that has an active presence and plan in at least five of the eight criteria below and has clearly demonstrated projects in place:


Advancement in emerging technologies such as Internet of Things (IoT), Artificial Intelligence (AI) and data analytics opens up tremendous opportunities to create smart solutions and value-added services which were not possible before. According to the research firm Gartner, by 2020 there will be 20.4 billion IoT devices, and approximately 37 percent of those will be used in the enterprise environment including large numbers dedicated to critical infrastructure monitoring and control systems.[2]

While data is the new oil, it also increases risks when shared across various systems to create services and solutions. According to IBM Security and Ponemon Institute 2019 report, across Asia, the average cost of a data breach increased from $2.53 million in 2018 to $2.62 million in 2019 which is the 11th highest cost globally when compared to other regions. Globally, the average cost of a data breach has increased to $3.92 million. [3]

The whitepaper explores the role critical infrastructure plays in allowing a city to function and details the importance of securing such assets. The key high-level challenges faced when implementing a Smart City have been identified with a focus on the growing concern of cyber threats.

An integrated, dynamic and secure operation center is a converged environment where data and intelligence from various devices, systems and applications are collected and analyzed for better planning and management by the various agencies of the Smart City.

In this white paper we have tried to define, identify, and contextualize the needs of an integrated, dynamic and secure operation center in a Smart City. Integrated technologies assist in the efficient delivery of services and there is optimism about their constructive impact on our cities. For research, insights from various policy initiatives, standards, industry use cases in the market have been leveraged.

[1] https://ww2.frost.com/wp-content/uploads/2019/01/SmartCities.pdf

[2] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[3] http://databreachcalculator.mybluemix.net/executive-summary/

# Critical infrastructure in a Smart City

Critical infrastructure plays an important role in ensuring the quality of life of citizens. A Smart City is as smart as the reliable functioning of its critical infrastructure such as public transportation, healthcare, utilities, energy, public safety and emergency. With the adoption of emerging technologies such as IoT, Edge Computing, and AI these services can be integrated to provide seamless and value-added services.

Critical infrastructure is defined as systems, whether physical or virtual, so vital to the city that the incapacity or destruction of such systems would have a debilitating impact on city's physical security, economic security, citizens' health or safety, or any combination of those matters.

In a world that is constantly changing, generating and consuming increasingly larger amounts of data, the approach to decision-making and analyzing complex situations in an operation center is critical. Situational awareness in control rooms and operations centers is imperative. Operations centers have to adapt to new demands and meet the needs of a multi-skilled and multi-generational workforce.

Critical infrastructure and services of a Smart City need to be secure. A clear understanding of the organization's business drivers and security considerations specific to its use of technology across agencies is needed. Because each organization's risks, operational priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the individual framework will vary. Hence a collaborative environment is required to make informed decisions across agencies.

Organizations responsible for the management and operation of critical infrastructure need to have a forward-looking approach to identify, assess, and manage cybersecurity risks not only at a system level, but in an integrated manner with other systems across the city. An emergency scenario such as a cyber-attack on the electric grid can also impact the water distribution, public transportation or health services.

A number of recent high-profile cases can be cited where a disruption to critical infrastructure resulted in widespread economic loss and social challenges for respective governments, businesses and citizens. Argentina, Indonesia and the U.K. all experienced widespread power outages during the year, affecting tens of millions of people and causing a knock-on effect to other critical infrastructure.

In Jakarta, a citywide blackout threw the city into disarray in August 2019, disrupting traffic, communications and businesses. Traffic lights all over the city ceased to operate, causing severe traffic congestion with police unable to manage the flow of traffic. The city's Mass Rapid Transport (MRT) system was brought to a halt, forcing passengers to disembark and walk to the nearest station. With power out in homes across the city, many people sought refuge in shopping malls that had emergency generators, the malls soon became severely overcrowded and presented a security risk in itself. Petrol stations were forced to close and netizens accustomed to cashless payments were forced to search out ATM's to withdraw cash, only to find that none were in operation.

# Challenges in Smart City initiatives

While Smart City initiatives tend to focus on sustainable developments and harnessing digital technologies for integrated citizen-services delivery, it demands that coordination across agencies has a strong focus on the much needed integrated and dynamic operation center in order to manage daily operation and to address emergency scenarios, in addition to taking cybersecurity into consideration.

As we move closer to realizing the vision of a Smart City, the demand for smart technology, integration and IT based problem-solving continues to grow. Some of the common challenges that emerging smart cities are facing include:

- Infrastructure – Sensors are widely used to collect and analyze data with a view to improve the delivery of services and improve the lives of citizens. The infrastructure required to support this can be complex and costly from an installation and maintenance perspective.
- Cybersecurity – As the usage of sensors to collect data used for decision making increases, so does the threat level to security. Due consideration to securing the sensor network is required, with blockchain encryption being widely touted as one possible solution.
- Legislation / Policies / Privacy – With so much information about the lives of residents being collected and analyzed, there is a concern around the “Big Brother” phenomenon. Transparency is required to build trust that solutions are in line with legislation and that citizens are informed about what will be done with data collected.
- Citizen Engagement – As citizens’ wellbeing and participation is paramount to the success of a Smart City, they must be educated about the potential benefits and encouraged to utilize e-services and other offerings.
- Interoperability between stakeholders – It is a requirement to bring together different agencies and organizations to reap the full benefits of a Smart City. Breaking down silos of cultural and political differences is necessary and can be addressed through strong leadership and an inclusive mindset.

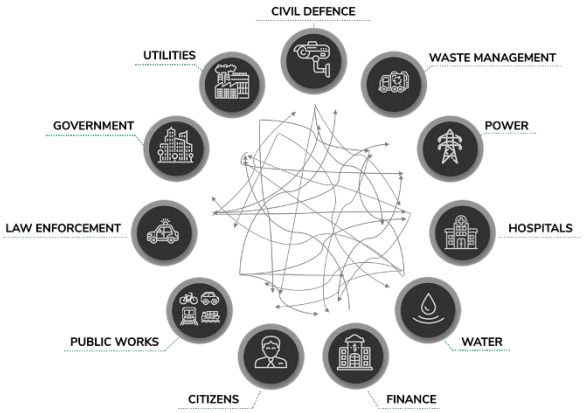
## IoT – A big opportunity with increased risk

The applications of connected IoT solutions have created unprecedented productivity and efficiency gains but have also exposed previously unreachable closed critical infrastructure systems to attack from a range of malicious groups with varying motivations. The information generated by these systems are converged at an organization or city level operation center where the data and insights from various sources are visualized, analyzed and critical decisions are made.

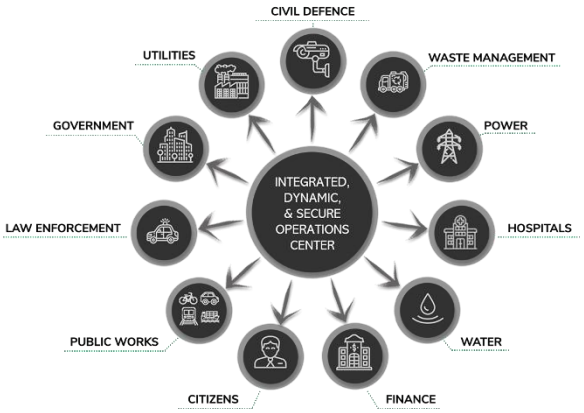
The ground analysis of a few smart cities by PwC suggests that the current technologies powering them are prone to vulnerabilities, which can lead to potential social, health, economic and reputational risks.[4] The growing threat of advanced cyber-attacks on critical infrastructure and interconnected industrial control systems (ICS) presents a unique and complex challenge for organizations, governments and city planners.

The resilience of critical services requires that operations centers be secure and also dynamic in how they respond to risks. This applies not only to information technologies (IT), but also the technologies that are relied upon to operate essential services; also known as cyber-physical systems, operational technology (OT). Many IT and OT systems that were previously segregated, are now becoming increasingly integrated to drive smart critical infrastructure initiatives across various agencies to serve citizens and businesses.

A Smart City operation center shall not be designed for single purpose due to the number of different stakeholders across agencies that are required to support a coordinated response to incidents. The new connected world demands more from these operations centers, they need to be able to visualize large amounts of data, be dynamic and flexible in order to cater to a wide range of situational needs.




*Uncoordinated Response*




*Coordinated Response*

[4] https://www.pwc.in/assets/pdfs/publications/2018/creating-cyber-secure-smart-cities.pdf

# An integrated, dynamic and secure operations center

Smart City operations centers use digital technologies to integrate different service networks. While many agencies may have their own operations centers, a true Smart City framework enables real-time collaboration and coordination across departments such as police, transport, power, water, sanitation, and public safety utilities.

These complex systems and dynamic environments require stakeholders with different skillsets and experiences to come together to share insights and tackle challenges effectively. A true Smart City operation should be **Integrated, Dynamic and Secure**.

## Integrated

> "The whole is greater than the sum of its parts" ~ Aristotle

Integrated Operations (IO) according to Ringstad & Anderson (2006) can be defined as a vision of future operation in the urban planning sector. Parker (2008) defines it as the collaboration across disciplines, companies, and organizational and geographical boundaries, made possible by real-time data and new work processes, in order to reach safer and better decisions faster.[5]

The real value of an integrated operation center does not come from a single standalone solution, but rather from a number of solutions working together across people, processes, tools and technologies. Bringing them together in a single facility, the knowledge sharing and coordination among different agencies within the Smart City ecosystem facilitate a rapid response and improves decision making in emergency situations.

A whole new breed of Gov Tech focussed start-ups and applications are focussed on optimizing government operation to provide better response and improve the services and experiences of citizens. Qlue, a Cyviz Smart City solutions partner, provides a platform with AI, IoT, and data integration, connecting citizens with the Jakarta government agencies to improve work productivity and efficiency in combating of city's problems.

[5] https://www.researchgate.net/publication/310494355_Formulating_an_Integrated_Operations_Centre_in_Johannesburg_A_Smart_City_Initiative

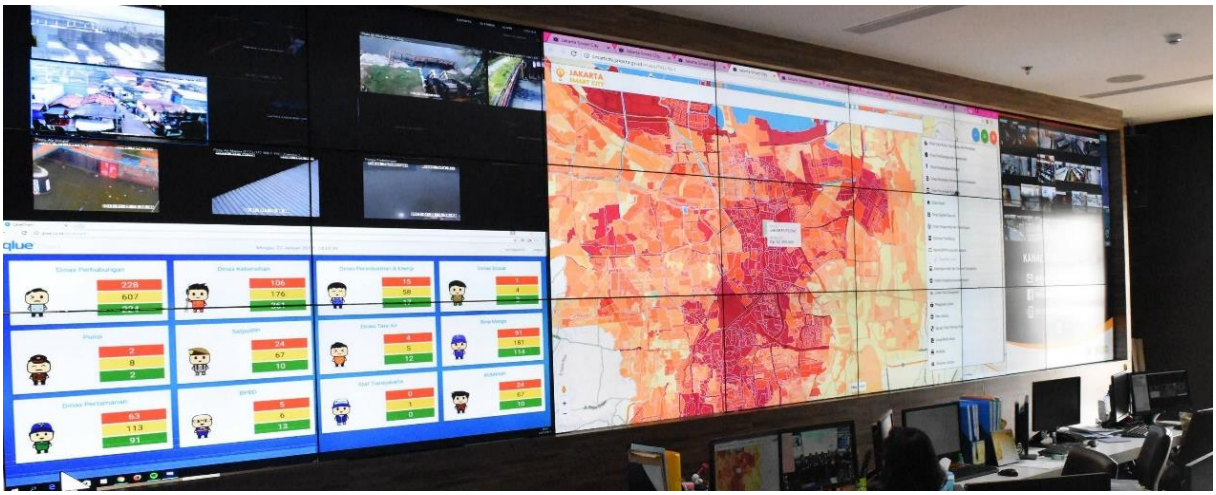



*Image : Jakarta Smart City operation room (Photograph by Qlue)*

Through a geospatial operation center dashboard, Qlue integrates systems from a variety of data sources, such as CCTV and environment sensors, related to public facilities and services. Qlue's analytics platform helps agencies make informed and collaborative decisions, and shape better policies by providing relevant data in real-time. "The pace of technology innovation is providing governments and municipalities increased opportunities to improve the life of its citizens" states Rama Raditya, Founder & CEO of Qlue in Jakarta. "Integrating data from many different sources on an integrated platform provides a powerful tool that enhances a city's real-time decision-making ability."

A Smart City focuses on key fields, such as municipal facilities, urban transportation, environment monitoring, public safety, economy and public opinion. An integrated operational environment acts as the brain of the Smart City and orchestrates the convergence of technologies from the field to help improve the city operation and manage emergency situations.

The need for an integrated operation environment is documented by the learnings from the aftermath of Hurricane Katrina in 2005. A report commissioned by the Committee on Homeland Security and Governmental Affairs[6] recommended the building of a true, government-wide operation center to provide enhanced situational awareness and manage interagency coordination in the event of a disaster. A need was identified for an Operation Center that consolidated into a single entity representative of all relevant federal agencies and provide for one clearly defined, emergency-management line of communication.

*Image: Katrina Hurricane in 2005*

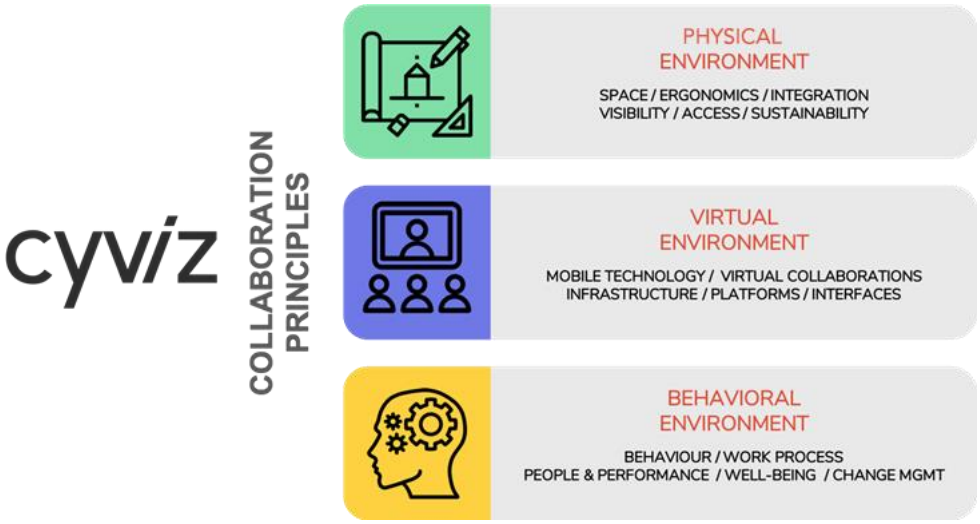
[6] https://www.govinfo.gov/content/pkg/CRPT-109srpt322/pdf/CRPT-109srpt322.pdf

## Dynamic

A Smart City operation center design needs to move away from the static and single-purpose legacy rooms and transform into a dynamic and multi-functional space where the physical and the virtual worlds co-exist. Improved workflow capabilities are possible through seamless integration of standard videoconferencing endpoints and other unified communication platforms such as Skype for Business and Google Hangouts. This allows key government stakeholders in other physical locations to be brought into a conversation ad-hoc and in real-time so decisions can be taken without delay, thus minimising response times and maximizing the efficiency of teams.

Designed as flexible and multi-purpose, these dynamic operations centers drive utilization and deliver a high return-on-investment. A Smart City operation center can be used to optimize work processes to drive efficiencies across sectors such as public transportation, waste management, environment monitoring, and utility services. The same space can be used as an emergency operation center when incidents occur or a cybersecurity response center when the need arises.

When designing dynamic operations centers, the physical, virtual and behavioral environments are three key collaboration principles that will assist designers in ensuring that Smart City operations centers meet the needs of key stakeholders.




The physical environment is concerned with ensuring adequate thought goes into the design of the space and the room ergonomics. There is no one size fits all when it comes to designing a layout for an operation center, the physical design will be based on how the users need to collaborate to support required workflows.

A dynamic operation center supports the convergence between the physical and virtual world, ensuring users can connect with colleagues outside of the space, in other locations or on mobile devices. The right infrastructure design that supports seamless integration between different platforms and technologies and ensures that users have access to the information systems they need is a critical design consideration.

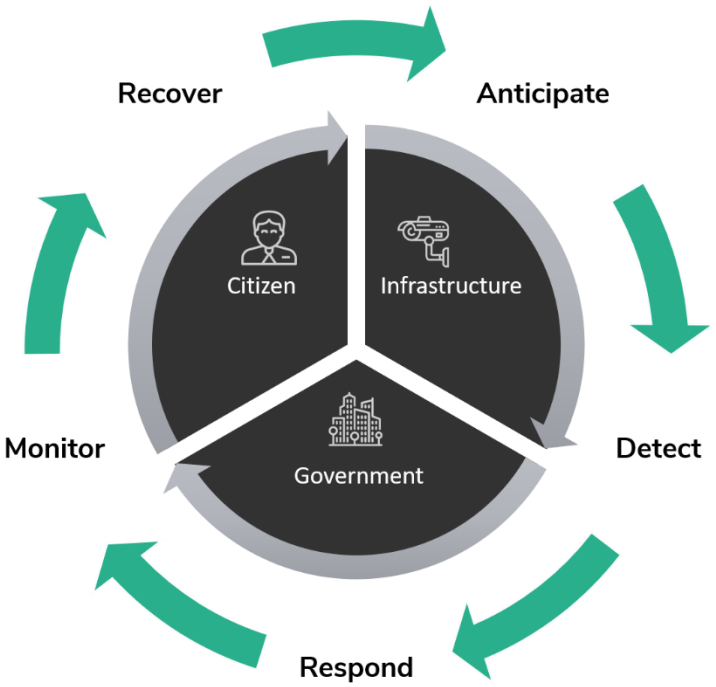
Maximizing wellbeing and focusing on human factors will help to ensure that the operation centre delivers engaging user experiences that are needed to keep teams motivated and attract the next generation of operators. Reducing fatigue, improving health and well-being should be key considertions made possible by ensuring optimal light, acoustics, air quality and ergonomics in the working environment.

## Secure

Smart cities are increasingly relying on emerging technologies to deliver services to its citizens. However, security breaches can impact operational effectiveness and potentially endanger the safety of the citizens. A comprehensive risk management framework that incorporates a proactive approach is therefore required in order for Smart City agencies to prepare for such scenarios.

Funding for cybersecurity personnel should be made as a priority rather than an afterthought. An information security team can be made responsible for monitoring and analyzing a city's security situation on an ongoing basis. The team's goal is to detect, analyze and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes.

Many security leaders are shifting their focus more on the "human element" rather than relying on technology alone to assess and mitigate cyber-related threats. While technology can prevent basic attacks, human analysis is required to put major incidents to rest. Consideration should be given to adopting a framework that allows security analysts to address five key functional activities when designing a cyber threat strategy:




### Anticipate

Understand where and how an attack can take place, that will allow teams to better prepare and protect critical infrastructure

### Detect

Incorporating advanced technologies, such as artificial intelligence and data analytics, to identify early signs of a compromise before it escalates into a serious threat

### Respond

Ensuring teams have the knowledge and access to systems that will allow them to respond in a timely and effective manner

### Monitor

Ensuring teams have situational awareness so they can adapt their response as needs dictate and plan for the recovery phase

### Recover

In the event of a breach, teams shall have access to the tools and processes for recovering data and restoring the affected services and systems

Due to the sophistication of current threats and the need to be able to take immediate action, a comprehensive intelligence picture of threats at a city level need to be made available at the Smart City's operation center. To achieve this, the collaboration between both internal government and external stakeholders is required to integrate cyber intelligence from a variety of sources:

- Government agencies – including national cybersecurity agency and critical national infrastructure (CNI) organizations
- Telecommunications data – from communications service providers and international internet gateways
- Trusted sources – threat intelligence shared between the professional community
- Open sources – intelligence sources collected and shared amongst security professionals
- Social media / dark web – scanning and crawling the internet to find exploits, attacks or malicious entities
- Human intelligence – analysts investigating incidents and discovering vulnerabilities through exploration

To make informed and collaborated decisions, teams must have the right tools to display, visualize and analyze data from multiple sources of cyber intelligence along with information from operational systems to identify and address incoming and potential threats. It is important that team members with different skill sets can collaborate on such intelligence to decide how to best address the specific scenarios.

Whilst much of the focus around cybersecurity is concerned with system threats, such as malware/ransomware, denial of service and man in the middle attacks, Smart City operators can adopt practices from the military agencies in terms of how they go the extra to secure the integrity of their data. In order to meet mission-critical status and operational readiness, military and defense installations have been adopting security standards designed to ensure the integrity of their data and systems at a facility level.

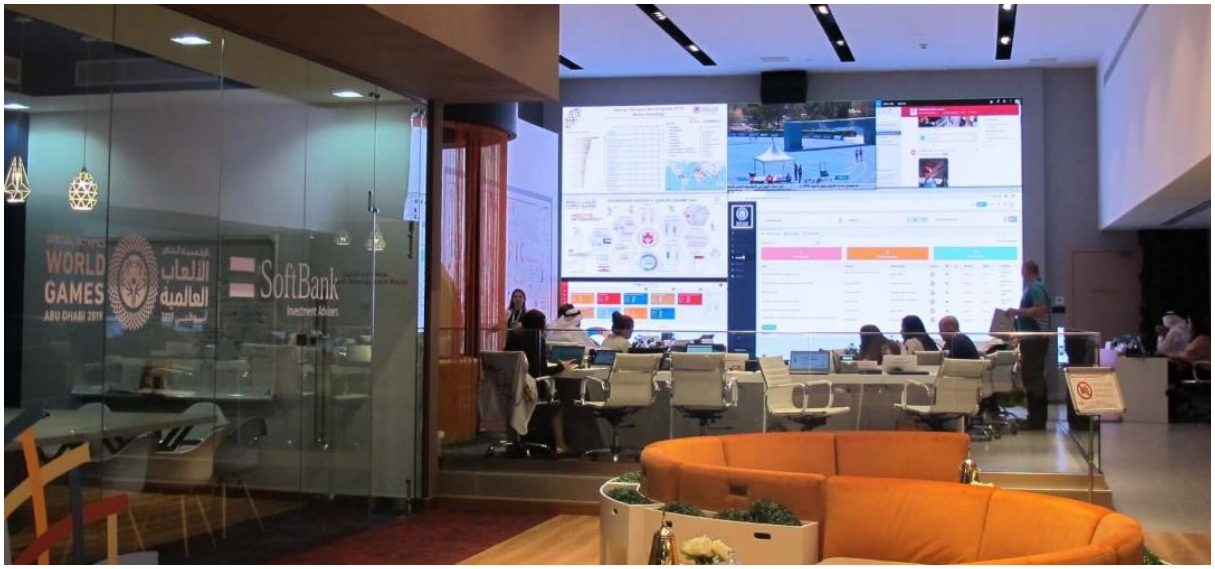
As a practice, one of the "Common Criteria" is an international set of guidelines and specifications developed for evaluating security products, specifically to ensure they meet an agreed-upon security standard for government deployments.

Evaluation Assurance Level (EAL) 4, for example, is the highest level that can be achieved and is accredited against security standards from organizations such as NATO. It evaluates products to ensure they offer the maximum protection against potential weaknesses such as:

- Optical isolation
- Electrical isolation
- Firmware isolation and accuracy

TEMPEST is another (U.S. National Security Agency) specification and a NATO certification referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds and vibrations.

# Special Olympics World Games master operations center




One of the most highly-regarded global sporting events in 2019, the Special Olympics World Games – which took place from March 14th to 21st at Zayed Sports City Stadium in Abu Dhabi – saw a record number of more than 200 nations represented, as 7,500 athletes of determination arrived in the UAE to compete for the winning title in more than 24 Olympic-style sports over seven days. With 500,000 spectators accommodated at nine world-class venues across Abu Dhabi and Dubai, and more than 20,000 volunteers assisting its 1,500 refereeing officials and 3,000 coaches, the event was the largest sports and humanitarian event in the world in 2019. Praised for its truly inspiring display of inclusivity, unity, respect, and sporting achievement, it made stars out of the athletes and captured hearts across the globe, all while aligning with the values of the UAE's Year of Tolerance.

To make the event of this scale successful the organizers built a mini-city to orchestrate operation, and provide the best services to the athletes, spectators, volunteers and officials. Well-handled logistics can make or break such an event – particularly one where many of the attendees had special needs – so having seamless medical, transportation, scheduling, and accommodation support were paramount. Here, data and analytics challenges were monitored in the master operation and command center and beyond, with information and apps supporting every part of the event playing a key role as vital elements in a production of this scale.

Cyviz engaged with the Special Olympics organization to help solve their data and analytics monitoring and visualization challenges in the master operation and command center for the World Games. Through Cyviz' support, all digital assets for the event fed information and data to the data hub, acting as a visual aggregator for all related intelligence. Another important part of the experience was the World Games app, which helped visitors and athletes to navigate through Augmented Reality, and share volunteer schedules, venue information, and medical incident application to manage any emergencies. It also provided a chatbot, as well as sports information, from scheduling and awards to profiles and live updates.

Cyviz' understanding of how visualization and a dynamic control room can contribute to public safety and reduce risk through the management of real-time and real-life situations, ensured an efficient delivery of services. As the center of monitoring and control of all data and analytics related to the Games, the master operation center was at the heart of the event's successful execution. Cyviz was the organizers' preferred choice – and the only solution that could deliver the versatility and adaptability needed to deliver a successful event.

# Secured and intergrated healthcare systems


Healthcare systems and services are examples of critical infrastructure for any city. The sensitivity associated with patient data makes the digitalization more challenging similar to other smart cities agencies and functions. The goal for hospitals and clinics is ultimately to better serve patients. To protect the hospital infrastructure and data, a Network Operation Center and a Security Operation Center allow teams to react quickly to cyber threats and provide a global view of critical IT systems required to maintain a high degree of uptime. It also allows them to securely connect with other agencies as required.

Cyviz was selected by Memorial Hermann Hospital in Houston as a key component of the new 6,000 S.F. Integrated Technology Command Center (ITCC). The ITCC houses Memorial Hermann's IT Help Desks, IT NOC Engineering and the technical operation team for the health system. The largest not-for-profit health system in Southeast Texas, Memorial Hermann has 14 hospitals and 200 other locations located throughout the Greater Houston area, and employs approximately 24,000 people. Today, the combined departments field over 30,000 calls per month.

"Cyviz is the centerpiece of our new ITCC," commented Brandon Hall, director of Technical Services at Memorial Hermann. "The 32 foot ultra-wide, ultra-high resolution video wall inside the ITCC will be used by our L3 NOC engineering team as well as the command conference center, or 'War Room.' If we have a major problem due to weather, or an outage of some sort, we will use the video wall to display critical information needed for our executives and people actually working on the problem. We've also integrated some additional panels on the opposite side of the building for our engineering teams. Our L3 engineering team will have a view on their walls to see what's happening in the environment in real time," Hall concluded.

"Memorial Hermann's commitment to a digital-centered environment means that it's critical to keep their systems available at all times," states Peter Stewart, President of North America for Cyviz. "Their new ITCC is an excellent example of how to utilize today's cutting-edge collaboration and visualization solutions to ensure everyone is able to respond to any technology issue quickly and proactively."

# Conclusion

A Smart City can be built by leveraging the best of emerging technologies in sensor networks, communication technologies, innovations in hardware infrastructure and software applications. An integrated, dynamic and secure command and control center is the spinal cord of a Smart City, required to analyze massive amounts of data from various agencies and systems to help stakeholders make efficient, informed and coordinated decisions.

The efficiency of a Smart City heavily relies on its interconnected network availability and any delay in coordination and response increases risks. A Smart City needs to prioritize issues and make informed decisions for mission-critical applications. A well-designed command center helps stakeholders serve its citizens and businesses in the most efficient way, whilst leveraging the power of emerging technologies such as Artificial Intelligence, Internet of Things and data analytics.

Organizations designing an operation center to manage critical infrastructure must ensure they are addressing cyber threats across systems, facility, operation and integrated processes throughout the solution lifecycle. Operators of critical services must manage risks by implementing appropriate and proportionate security measures required to notify the relevant national or city authority of incidents. Operators of critical services are responsible for the compliance within their partner network too, so due consideration should be given to the way third party solutions are evaluated, selected and procured.

## References

1. NIST Cybersecurity for IoT Program.
   https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
2. Framework for Improving. Critical Infrastructure Cybersecurity
   https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
3. GSMA IoT Security Guidelines
   https://www.gsma.com/iot/iot-security/iot-security-guidelines/
4. Baseline Security Recommendations for IoT
   https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

## About AllThingsConnected

AllThingsConnected is a Digital Transformation organization based in Singapore with global touch points. AllThingsConnected works with its clients and solutions partners to help them build their transformation journey strategy, roadmap, solutions and adaptive ecosystem. www.athingsc.com

## About Cyviz

Since 1998, Cyviz has designed and delivered global technology solutions. Now, we bring you the Dynamic control rooms and operations centers. Robust and multipurpose solutions built for use in secure, mission-critical environments. www.cyviz.com

Visit one of our Cyviz Experience Centers to get a demonstration of our solutions for the Dynamic control room:

## EUROPE

**Stavenger**
Vestre Svanholmen 6
4313, Sandnes
Norway
+47 51 63 55 80

**Oslo**
Strandveien 15
1366 Lysaker
Norway
+47 96 62 27 19

**London**
St Clare House
30-33 Minories
London EC3N 1DD
+44 203 475 00 90

## NORTH AMERICA

**Washington DC**
900 N. Glebe Road
Suite 200
Arlington, VA 22203
+1 571 858 3370

**Houston**
5555 San Felipe
Suite #1700
Houston, TX 77056
+1 713 350 6700

**Atlanta**
Parkside Terrace West
Suite 320
3780 Mansell Rd
Alpharetta, GA 30022
+1 678 744 6185

## ASIA PACIFIC

**Singapore**
80 Anson Rd #11-07
079907 Singapore
+65 6814 1000

**Jakarta**
Foresta Business Loft 2
No. 28 BSD City
Indonesia 15339
+62 81287868786

## MIDDLE EAST

**Dubai**
Dubai Internet City
Office Park 116
Building C, 3rd floor
PO box 502782
Dubai, UAE
+971 4 375 4747

**Riyadh**
Tamkeen Tower
19th Floor
King Fahad Road
Yasmeen Area
Riyadh
Kingdom of Saudi Arabia
+966 112030262

---

CYVIZ DESIGNS AND DELIVERS DYNAMIC CONTROL ROOMS & OPERATIONS CENTERS

 INTEGRATED

 DYNAMIC

 SECURE

GLOBAL
SUPPORT CENTER
support@cyviz.com

CYVIZ
SALES
sales@cyviz.com
www.cyviz.com

cyviz