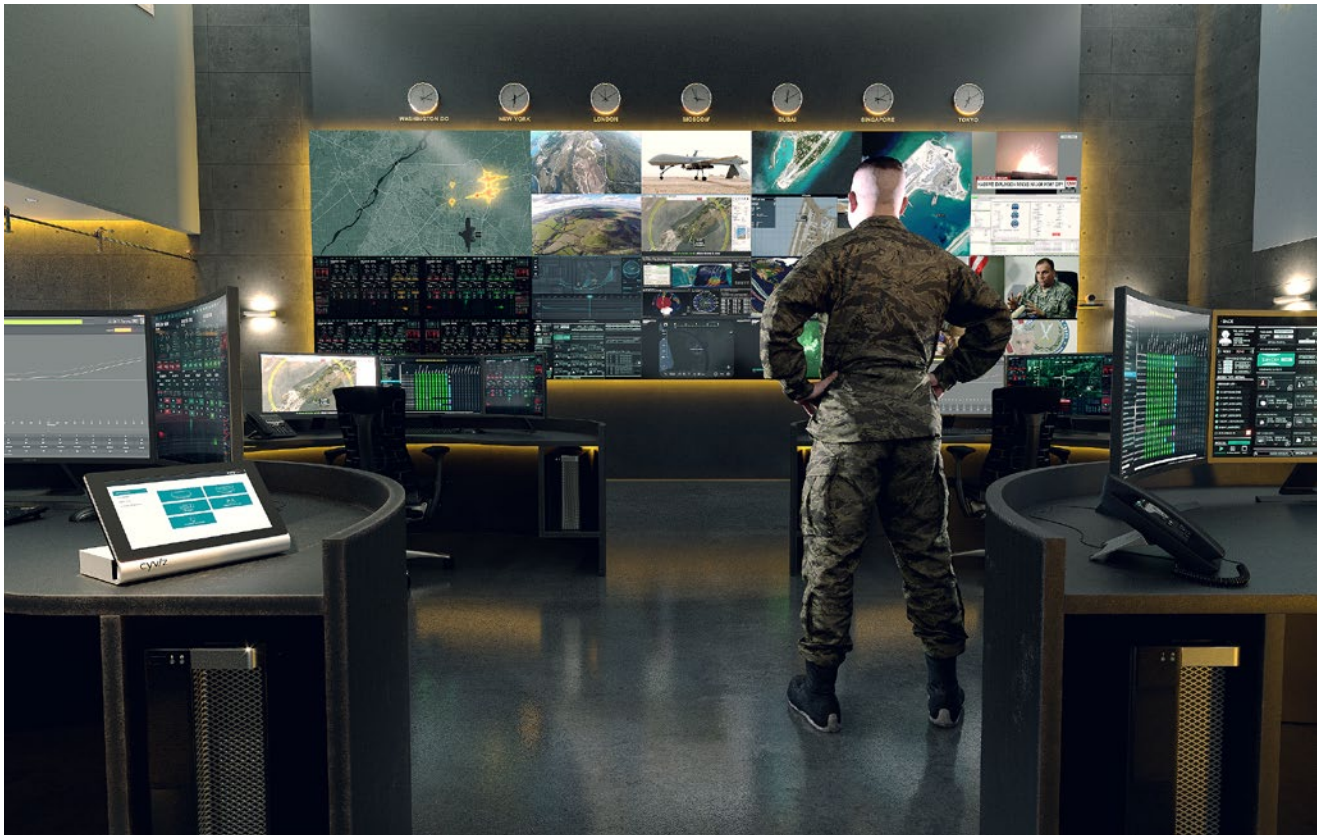
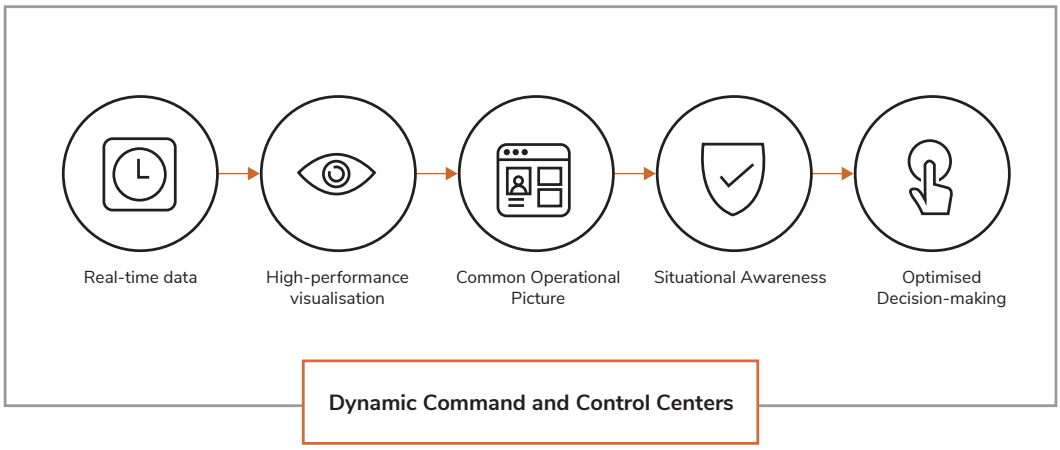
Building the next generation of secure and dynamic Command & Control centers

Governments face an ever increasing number of challenges - foreign, domestic and natural. Advances in information technology require governments at all levels to protect their operational networks and citizens from cybersecurity threats in ways never imagined just a few years ago. These constantly shifting challenges require Command and Control centers to have content visualization technologies that offer multi-domain security, access to a wide variety of content sources, and help leaders make decisions quickly during fast moving situations.



A Flexible Common Operational Picture (COP)

Defense operations need a Common Operational Picture (COP) to establish situational awareness. The COP acts as the single shared source of truth for direction and coordination, and ultimately decision-making. Leaders need to see and quickly grasp the changing realities within a highly dynamic combat or emergency environment. Therefore the technologies presenting that data must instantly present relevant information and be able to change how that content is displayed across the wall or within an individual display. Innovative leaders use this technical advantage to create a more adaptive mission command approach to utilizing assets on the ground, the seas, the air and out in space to achieve their missions. Constantly changing multi-domain threats ranging from cyber criminals to geopolitical power dynamics, civil discord, and climate change demands a more flexible approach to using audio visual technologies to enable the FCOP in complex control center settings.



> The use of presets saves valuable time in critical situations and make it possible to transform and 'personalize' the user experience..."
>
> – Peter Stewart, Cyviz

Immediate scenario switching using presets

A great way to technically facilitate this ease of mode switching and dynamic workflows, is to use scenario presets. As missions constantly evolve, it is critical for the video control system to change how the information is displayed in a quick manner. End-users and customers cannot facture in to wait for a programmer, but instead be able to switch modes as missions unfold. A new set of experts might need to be brought in, a new security clearance might be required for the rest of the mission, or the location or objectives might change completely and require new settings and content sources to be pulled in quickly.

Also, in an operation center, the senior staff will change over the course of the day, and when the new commanding officer starts, he or she will usually want to change the way the information is displayed. The use of presets saves valuable time in critical situations and make it possible to transform and 'personalize' the user experience at the click of a button. The dynamic approach automatically computes the user's requirements for the environment and the mission to deliver the right common operational picture for that user and that particular mission.

Multi-classification

The next generation of dynamic Command & Control centers should also cater for multiple security configurations within the same system. This flexible approach should differentiate between security levels as they apply to different individual clearances and different networks. This flexibility in network source configuration is a significant advantage in Cyber Security Operations centers, Joint Operations centers and in Command & Control environments where multi-level security is a requirement. Computer sources from different networks and security classifications can be surely connected to the system, so content from multiple sources can be combined into an optimal representation of mission-critical information. In many instances, end users need to switch between two or more computers, at different classification levels, introducing data vulnerabilities. Strict security rules for the protection of classified information dictate data processed solely in trustworthy red networks is never transferred to black networks, where unauthorized personnel would have access to it.

Another focus is to ensure that authorized users only gain access to those parts of the system they are authorized to access. For instance, KVM systems are often designed to access multiple sources across multiple domains with different security classification levels. It is critical that a breach does not occur between these two domains, even though they may exist as part of the same KVM infrastructure. Typically, there are two design approaches to manage issues like these: partitioning and restriction.

Partitioning refers to the ability to dedicate resources within the system to isolated groups, with no chance of unintentional crossover, within a router, switch or system of routers and switches. Essentially, partitioning creates several routers within a router. Restriction addresses the idea of limiting access on a user-by-user, source-by-source basis. A strong KVM system design will allow the system manager to determine which users gain access to which sources, and perhaps more importantly, which users are denied access to which sources. The result is a secure system architecture engineered from the ground up results in a scalable solution, which doesn't compromise the system administrator's ability to perform configuration management easily across the entire facility. The objective of physical separation is to prevent the threat (people) from physically accessing the content or the system. A common approach is to prevent unauthorized users from entering the physical location of the system, by restricting access through card readers, biometric readers, etc. The physical separation between Information Processing Units (IPU) of various classifications is maintained in a remote location(s) accessible by the system administrator and out of the way of the mission operator. This greatly minimizes attack vectors and the insider threat as compute resources and the IP network are no longer in the operating environment.

High-performance visualization to solve complex problems

The human aspect to complex decision-making within Command & Control centers is crucial. The way images and content will be displayed, and their resolution could make the difference between life or death in mission critical environments. To solve complex problems and take informed decisions, operators and senior staff need to visualize information in an ultra-wide canvas at a superior resolution. Depending on the room's layout, the wall space, the required number of inputs and content sources, but also the viewing distance for operators and staff chief need to be taken into considerations before choosing a video wall solution. Aspect ratio, pixel density and light constraints will also help inform the choice between LCD, LED or blended projections display technologies.

The trend in many Cyber Security Operations centers is the adoption of 4K video source resolution or at least address the need to be 4K ready. This resolution needs to be carried to the display wall and even to multiple targets that are also 4K resolutions each. A target display is one or more displays to the left, rear and/or right of the main operations center wall. Higher resolution in cyber yields the advantage of increased identity of artifacts that could be critical to the defense of the network and other layers. This means the resolution requirements for an operation center must be considered at the initial stages of design, and in many circumstances, additional display surfaces can be added later.

Future-proof solutions

With the digital transformation well under way and the use of Augmented Reality (AR) and Artificial Intelligence (AI) picking up rapidly; government entities will require a future-proof Command & Control room that adapts to these new needs and will be a long-term investment. Dynamic control room solutions must be application agnostic, standardized and configurable to stand the test of time, regardless of changing underlying technology. Existing systems must be easily upgradeable with features and functions. The best Command & Control environments should offer the reliability and flexibility needed to meet the changing landscape of technologies, and remain relevant, powerful and reliable. An agile installation and maintenance

An agile installation and maintenance expertise

Due to their sensitive and critical nature, Command & Control centers must maintain 100% uptime especially during real-world operations but also when executing planned exercises. Installation and maintenance have often been pain points for these environments, demanding experienced support from their vendor. Support staff will need to come with the appropriate clearances and minimize disruptions in workflows to ensure 24/7 operations do carry on.

> The best Command & Control environments should offer the reliability and flexibility needed to meet the changing landscape of technologies, and remain relevant, powerful and reliable."
>
> **– Peter Stewart, Cyviz**

cyviz

Cyviz Command & Control centers highlights

Operational structure that supports remote services delivery model

Cyviz is reinventing central support management and monitoring with the Cyviz Easy Server which is an all-in-one control platform for centralized support and management of all Cyviz systems. It is designed to improve user experience while reducing resources spent on management and support.

Configurable control

- The Cyviz Easy Controller communicates with other system components via TCP/IP or serial protocols and can be integrated with a CATx based extension receiver. The unit has two RS232 ports, which can be extended using an (USB-RS232) adapter.
- Built-in support for a selective list and heavily vetted list of well-proven A/V components and is designed to control systems built on the Cyviz Solution design model.
- Feature controls and menus can be password protected by a system administrator.
- Multiple configurations available.

Multi-classification and secure KVM integration

Cyviz seamlessly integrate with Thinklogical, which provides the only fiber optic KVM extension and Video Display System (VDS) solution to achieve Common Criteria, NATO (NIAPC) Green Status, JITC UCR and TEMPEST accreditations. It is also the only remote extension system approved to switch multiple security domains through a single chassis. Thinklogical's products follow strict User Data Separation policies in which there is no data flow between Transmitter Port Groups or Receiver Port Groups and any other physical port on Thinklogical routers unless an authorized.

- Non-blocking, protocol agnostic Layer 1 switching. 10Gbps/6.25Gbps bandwidth per port and no latency or lost frames.
- Uncompressed video up to 4K60 (4:4:4, 10-bit) across distances of up to 80km.
- Can be configured and deployed as a "Closed VDS System" per section 9.2 of the DoD UCR 2013.

Unique Video Processing

The Cyviz video wall processor called the XPO (4 or 5), is designed to be used in conjunction with the Cyviz Easy Controller to achieve maximum efficiency and usability in the Command & Control space. This integration forms the basis of the consistent Cyviz system architecture based on IT principles. The Cyviz approach is to create a separate A/V net that moves video one-way to the display wall.

- Network access not required.
- Cyviz XPO applies proprietary video processing algorithms to the incoming video signals in DVI single link, DVI dual link, HDMI or Display Port 1.2, and outgoing video signals in either DVI single link.
- All video signals coming to the Cyviz video processors are one-way, subsequently passed along to the display wall.
- Creates Picture-in-Picture (PiP) images for individual sources and distributes the resulting image across multiple display units in real time when used in conjunction with the Cyviz Easy Controller.
- Proprietary algorithms for edge blending of multiple solid-state projectors, LCD flat panels, and small pitch LED displays.

About Cyviz

Cyviz is a global technology provider for standardized conference rooms, control rooms and experience centers. Since 1998, Cyviz has empowered the digital workforce to connect, visualize, and collaborate on their critical data. The IT-driven turnkey solutions are easy to deploy, manage and support. Cyviz serves global enterprises and governments with the highest requirements for usability, security and quality, that engage people, encourage collaboration, and accelerate decision-making. Cyviz is listed on Euronext Growth at Oslo Stock Exchange since 2020.

With the right technology, we believe that leaders from any industry can leverage the power of digital collaboration to keep distributed workforces motivated, satisfied, and productive.