New Technologies for National Security Situation Centres

New Technologies for National Security Situation Centres

By

Anatoly Alekseevich Morozov
and Vitaliy Aleksandrovich Yashchenko

Cambridge
Scholars
Publishing

New Technologies for National Security Situation Centres

By Anatoly Alekseevich Morozov and Vitaliy Aleksandrovich Yashchenko

This book first published 2026

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-0364-6604-6
ISBN (Ebook): 978-1-0364-6605-3

CONTENTS

PREFACE

Digital Shield: New Technologies for National Security Situation Centers is a comprehensive study of modern situation centers (SCs), key tools for management and decision-making in the complex challenges of the 21st century. The authors take a detailed look at SC architecture, including centralized and decentralized structures, hardware and software, as well as data protection and system integration issues. Special attention is paid to decision-making processes, the role of big data, artificial intelligence (AI) and cognitive technologies in improving management efficiency.

Separate chapters are devoted to the application of SC in military operations, revealing the peculiarities of their technological equipment, strategic and tactical planning, and the use of simulation and analysis. The book explores the interaction between humans and AI in SC, including the problems of individual and collective decision-making, as well as the prospects for the development of androids and neural networks as the basis of artificial intelligence.

In the context of cybersecurity, the authors analyze threats in the digital space and methods of information protection, emphasizing the importance of SO resilience to external attacks. The final sections look to the future: quantum computing, blockchain, virtual situation centers and their integration with national security systems. The book concludes with a discussion of ethical issues and responsibilities when using new technologies in decision making.

The publication is supplemented with a glossary, list of acronyms, recommended reading, and case studies, making it a valuable resource for national security, governance, AI, and cybersecurity professionals, as well as anyone interested in the technological future.

ABOUT THE AUTHORS

Anatoly Alekseevich Morozov is a doctor of technical sciences, professor, and academician of the National Academy of Sciences of Ukraine. One of the leading experts in the field of cybernetics, automated control systems, and situational center technologies.

He was born on May 9, 1939 in Kyiv. In 1961, he graduated from the Kiev Polytechnic Institute, and in 1972, he completed his postgraduate studies at the Institute of Cybernetics of the Academy of Sciences of the Ukrainian SSR. He began his scientific career under the guidance of the famous cyberneticist, academician Viktor Glushkov, whose scientific directions he continued and developed.

Professor Morozov is the author of more than 500 scientific publications, including fundamental works on information and analytical systems and technologies for making situational decisions. Under his supervision, 16 doctoral and 43 candidate dissertations were defended.

He was one of the pioneers in the development of early automated enterprise control systems in the USSR, including the Lviv system, which was awarded the State Prize of the Ukrainian SSR in 1970. He also contributed to the creation of the Mission Control Center in Korolev, Russia, for which he was awarded the USSR State Prize in 1977. Following the Chernobyl

disaster, he led the development of a water safety assessment system for the Dnieper River, which was critical to public health and recovery efforts.

From 1983, he served as director of the Special Design Bureau of Mathematical Machines and Systems; in 1992, he founded and became director of the Institute for Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine. Since 1991, he has been president of the Academy of Technological Sciences of Ukraine.

Professor Morozov has received numerous awards, including several State Prizes of the USSR, the Ukrainian SSR, and Ukraine, as well as the Order of the Red Banner of Labor and the Order of Merit (III degree). He has made significant contributions to the development of digital technologies for the needs of public administration and government agencies. He was the chief designer of the electronic voting and document management system "Rada". His work on the "Rada" system, which supports legislative decision-making, was implemented in more than 20 government agencies in Ukraine and abroad. His research interests include system modeling, situational management, cognitive technologies, artificial intelligence, and the development of sustainable digital infrastructures.

Vitaliy Aleksandrovich Yashchenko is a Candidate of Technical Sciences and a researcher in the field of intelligent information technologies, neuro-like systems, and cognitive computing. He was born in 1941 in the city of Pyatigorsk, Stavropol Krai, Russia, into a military family.

He graduated from the Kyiv Geological Exploration Technical School (1958), the Odesa Institute of Patent Studies (1971), and the Faculty of Automation and Telemechanics of the Odesa Polytechnic Institute (1972). He earned his Candidate of Technical Sciences degree in 1989 at the Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine. In 1999, he defended his doctoral dissertation at the Institute of Mathematical Machines and Systems Problems (IMMSP) of the NAS of Ukraine (not approved by the Higher Attestation Commission of Ukraine).

Since 1974, he has worked within the National Academy of Sciences of Ukraine system: first at the Institute of Cybernetics, then at its Special Design Bureau, and since 1992 — at the IMMSP, which was established on the basis of that bureau. Since 2016, he has been a corresponding member of the Academy of Technological Sciences of Ukraine.

Many of his scientific developments were carried out in close collaboration with academician Anatoliy A. Morozov. His solutions are based on original ideas and have often been ahead of their time, earning recognition as inventions. Among the most notable are an intelligent diagnostic system for

general practitioners and a system for monitoring patient motor activity, which was implemented in medical institutions in Crimea.

Over the past three decades, his main research focus has been the development of neurallike networks as a new information processing technology. He is the creator of a new type of neural network — multidimensional receptor-effector neuro-like growing networks, which exhibit strong capabilities for self-learning, adaptation, and efficient processing of complex structured data.

He is the author of 23 inventions, more than 100 scientific publications and three monographs.

INTRODUCTION

Situation centres (SCs) are vital instruments for governance, security, and resilience in a world characterized by intricate and rapidly evolving challenges. Powered by advancements in information technology, big data analytics, and artificial intelligence, these centres facilitate real-time monitoring, crisis response, and strategic decision-making across diverse sectors, from national security to urban infrastructure management and emergency response. This book offers a comprehensive analysis of situation centre technologies, organizational frameworks, and applications, establishing them as essential pillars for the stability and sustainability of modern states and societies. By synthesizing theoretical insights with practical applications, it seeks to advance scholarly and professional understanding of SCs as critical socio-technical systems.

The genesis of situation centres can be traced to the 20th century, when military and governmental entities grappled with the complexities of operational management and burgeoning information flows. Originally developed to monitor strategic threats and coordinate military operations, SCs provided unparalleled real-time situational awareness. Their efficacy led to their adoption in civilian contexts, such as disaster management, environmental monitoring, and urban traffic control. This adaptability underscores the versatility of SCs, positioning them as integral to contemporary governance frameworks.

Technological progress has dramatically enhanced the functionality of situation centres. The shift from analog to digital data streams, combined with the integration of diverse data sources, has enabled rapid and sophisticated analysis. By the early 21st century, SCs had become central to state and municipal governance, supporting real-time oversight of critical processes, including crisis response, public safety, and public health monitoring. In addressing global challenges—such as cyberattacks, climate change, migration crises, and geopolitical instability—SCs demonstrate their capacity to foster coherence and resilience in governance structures.

This book provides a rigorous examination of situation centres, encompassing their theoretical underpinnings, technological foundations, and practical applications. It explores how SCs leverage big data analytics, artificial intelligence, and machine learning to process extensive datasets and deliver actionable insights, thereby enhancing decision-making in high-uncertainty environments. The study also investigates the organizational flexibility of SCs, which can operate as centralized hubs for coordinated control or as distributed systems for decentralized management. Through detailed case studies and conceptual frameworks, the book illuminates the strengths and limitations of these models in addressing varied operational needs.

A central contribution of this work is its focus on the strategic role of SCs in navigating uncertainty. By employing advanced analytical tools to identify patterns, predict outcomes, and propose optimal strategies, SCs empower decision-makers to tackle complex challenges effectively. Equally significant is the emphasis on data security, with the book examining technologies such as quantum cryptography, blockchain, biometric identification, and multi-factor authentication as critical for ensuring secure SC operations in an era of globalized cyber threats. These discussions highlight the necessity of robust security frameworks to maintain the integrity of SCs.

Written for an international audience of researchers, practitioners, and policymakers, this book bridges cutting-edge scholarship with practical guidance. It provides insights into the design, implementation, and security of situation centres, drawing on interdisciplinary perspectives from information technology, governance, and security studies. By underscoring the strategic importance of SCs, the book contributes to global discussions on how socio-technical systems can enhance resilience and safety in an interconnected world.

The role of situation centres is set to expand with the emergence of transformative technologies, such as quantum computing, neural networks, and advanced data analytics. These innovations promise to revolutionize the analytical and predictive capabilities of SCs, opening new avenues for their application. This book equips readers with the knowledge to engage with these developments, encouraging contributions to the ongoing evolution of

situation centres as vital tools for governance and security. In doing so, it aims to inspire further research and innovation in this dynamic and critical field.

CHAPTER I

FUNDAMENTALS OF SITUATION CENTRES

1. Situation Centres

Situation centres (SCs) are advanced socio-technical systems designed for centralized monitoring, control, and management of critical infrastructure and processes (Grigoryev, 2020). As defined by Bellow and Ivanov (2019), a situation centre is "*a specially equipped facility, such as a control room, hall, or office, fitted with communication technologies, including videoconferencing and interactive data visualization tools, to support operational decision-making, control, and monitoring of various objects and situations*". This definition underscores the role of SCs as integrated environments that facilitate real-time situational awareness and governance.

SCs vary significantly based on their purpose, scale, and application, reflecting their adaptability to diverse operational contexts. This chapter provides a systematic classification of SCs, examines their decision-making structures, and proposes a refined definition to account for modern technological advancements, contributing to a deeper understanding of SCs as pivotal tools for governance and crisis management.

1.1 Classification of Situation Centres

SCs can be categorized according to several criteria, reflecting their diverse functions and operational requirements. These classifications are outlined below.

By Purpose

- Situational Information Display Systems (SIDS): These systems prioritize data visualization in user-friendly formats to enable real-time monitoring of operational conditions. SIDS are critical for

environments requiring immediate situational awareness (Bellow & Ivanov, 2019).

- Dynamic Situation Modelling Systems (DSMS): DSMS facilitate the development of predictive models to simulate event progression and forecast outcomes, widely used for risk analysis and preventive measures (Petrov & Sidorov, 2021).
- Analytical Situation Systems (ASS): ASS focus on in-depth data analysis to identify patterns, trends, and correlations, supporting strategic decision-making in long-term planning (Smirnov & Petrov, 2022).

By Functionality

- Observation SCs: These centres emphasize the aggregation and visualization of data from multiple sources, such as sensors and databases, to provide comprehensive situational overviews.
- Analytical SCs: These centres concentrate on processing large datasets to generate actionable insights, often leveraging artificial intelligence and big data analytics (Smirnov & Petrov, 2022).
- Full-Featured SCs: Combining observation, modelling, and analytical capabilities, full-featured SCs offer a holistic approach to situational management.

By Scale

- Local SCs: Deployed at the level of individual enterprises or units, local SCs address specific operational needs.
- Regional SCs: Operating across cities or regions, these centres coordinate broader infrastructure and resources.
- Federal SCs: Functioning at the national level, federal SCs oversee country-wide operations, often addressing national security or large-scale coordination (Bellow & Ivanov, 2019).

By Industry Application

SCs are employed across various sectors, including:

- Security and Defense: Agencies such as the Ministry of Emergency Situations (MChS), Ministry of Internal Affairs (MVD), and Federal Security Service (FSB) utilize SCs for crisis response (Lebedev & Kuznetsova, 2023).
- Energy: Power plants and grids rely on SCs for infrastructure management.
- Transportation: SCs support aviation, railway, and maritime operations.
- Industry: Manufacturing enterprises use SCs to optimize production.
- Finance: Banks and stock exchanges employ SCs for market monitoring.
- Healthcare: Hospitals and clinics leverage SCs for patient and epidemic monitoring.

By Decision-Making Structure

SCs can be classified based on decision-making processes into two types:

- Centres with Sole Decision-Making Authority: Decisions are made by a single individual with ultimate responsibility.
- Centres with Collective Decision-Making: Decisions are formulated collaboratively by a group of stakeholders.

These models are integral to SC operations, warranting detailed examination.

1.2 Situation Centres with Sole Decision-Making Authority

A situation centre with sole decision-making authority is a centralized structure designed to deliver analytical information to a single decision-maker, typically a high-ranking official (Grigoryev, 2020). These centres employ advanced technologies—such as real-time data analytics and predictive modelling—to provide comprehensive situational awareness, enabling rapid responses in high-stakes contexts like crisis management or military operations (Lebedev & Kuznetsova, 2023). An exemplar is the Presidential Situation Centre, which supports the head of state in addressing national security, defense, foreign policy, and crisis response (Bellow & Ivanov, 2019). This centre integrates data from intelligence agencies,

security services, and operational units, with analytical teams working in real time to ensure responsiveness and accuracy.

The president, as the sole decision-maker, relies on the SC to provide consolidated insights. While consultation with experts may occur, final authority rests with the president, ensuring a streamlined process. The decision-making cycle includes:

- Data Collection: Information is gathered from intelligence reports, ministerial updates, and monitoring systems.
- Data Analysis: Specialists use analytical tools to identify risks and issues.
- Situation Assessment: The situation is evaluated, with scenarios and consequences outlined.
- Decision-Making: The president makes the final decision, informed by data and recommendations.
- Implementation: The decision is executed by relevant agencies, with oversight.
- Monitoring and Adjustment: Outcomes are evaluated, with adjustments as needed.

This structure supports rapid, authoritative decision-making under time-sensitive conditions.

1.3 Situation Centres with Collective Decision-Making

A situation centre with collective decision-making facilitates collaborative analysis and decision formulation by a group of experts or stakeholders (Kovalyov & Semyonov, 2021). These centres integrate data to enable real-time collaboration, supporting consensus-driven solutions in complex, multifaceted scenarios. The Situation Centre of the Verkhovna Rada of Ukraine exemplifies this model, supporting the legislative process by providing analytical insights to parliamentary deputies.

It monitors political and socio-economic conditions, prepares legislative proposals, and forecasts policy outcomes, with decisions made through

majority voting. The SC provides data and scenarios without advocating for specific choices, leaving final decisions to the collective body (Figure 1.1).

Figure 1.1 Operational framework of the Verkhovna Rada Situation

The collective decision-making cycle includes:

- Data Collection: Information is sourced from committee reports, monitoring data, and consultations.
- Data Analysis: Experts synthesize data to identify challenges and opportunities.
- Situation Assessment: Scenarios and implications are outlined.
- Collective Discussion: Deputies and stakeholders discuss options.
- Decision-Making: A decision is reached through majority voting.
- Implementation: The decision is executed, with coordination ensured.
- Monitoring and Adjustment: Outcomes are evaluated, with adjustments as needed.

This approach ensures diverse perspectives are considered, fostering balanced decisions.

1.4 Comparative Analysis of Sole and Collective Decision-Making SCs

The Presidential Situation Centre and the Verkhovna Rada Situation Centre highlight distinct decision-making dynamics:

- Centralization vs. Collectivity: The Presidential SC is centralized, directing all information to the president, while the Verkhovna Rada SC supports collective decision-making through voting.
- Responsiveness vs. Deliberation: The Presidential SC prioritizes rapid responses to crises, whereas the Verkhovna Rada SC supports deliberative legislative processes.
- Functional Objectives: The Presidential SC focuses on strategic, urgent decisions, while the Verkhovna Rada SC addresses legislative and socio-economic initiatives.

Both are high-level analytical situation systems, sharing common features:

- Scale: Operate at a national level.
- Functionality: Combine visualization, modelling, and analysis.
- Data Sources: Integrate economic, social, political, and military data.
- Objectives: Support informed decision-making for national leadership.

However, the Presidential SC emphasizes strategic security, while the Verkhovna Rada SC focuses on legislative activities.

1.5 Redefining Situation Centres

Traditional definitions of SCs, which emphasize physical spaces and basic communication functions, are increasingly outdated given modern technological advancements. This chapter proposes a refined definition: *"A situation centre is an integrated socio-technical system of software-hardware complexes, equipped with artificial intelligence and decision-support technologies, operating in both collective and individual modes to manage complex systems."* This definition highlights the role of advanced technologies, such as AI, and the integration of human and machine

capabilities, aligning with contemporary standards for automated control systems.

SCs are organizational systems implementing situational management technologies, distinguishing them from mere meeting rooms with display equipment (Lebedev & Kuznetsova, 2023). Key roles in SCs include:

- Decision-Maker (DM): A domain expert responsible for final decisions, participating in collective discussions.
- Analyst: A specialist modeling alternative solutions without decision-making responsibility.
- Expert: An experienced professional contributing to discussions without decision-making authority.

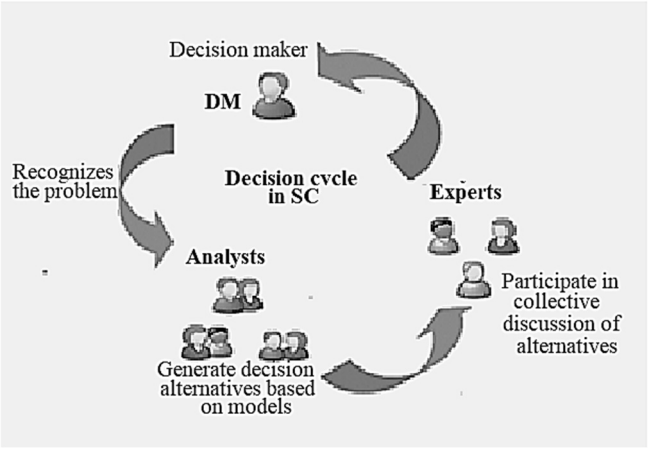

Figure 1.2 Simplified decision-making cycle in a situation centre, highlighting roles and processes.

The simplified decision-making cycle, illustrated in Figure 1.2, underscores the collaborative interplay of these roles in achieving effective situational management.

2. Situation center architecture

A situation center architecture is an integrated ecosystem of hardware and software solutions designed to collect, process, analyze, and visualize data critical to informed decision making (Deloitte, 2022; Schneider Electric, 2024). These centers serve a variety of applications, including government, business, and military operations, providing rapid and accurate responses to emerging threats or challenges (MITRE Corporation, 2021). The architecture varies depending on operational objectives, with the main difference being the distribution of data processing functions in centralized or decentralized structures (Eurofunk, 2023).

2.1 Centralized SC Structure

A centralized situation centre structure consolidates all key processes—data collection, processing, analysis, and decision-making—within a single control hub, ensuring unified coordination and oversight (Deloitte, 2022; Eurofunk, 2023). This model establishes a central authority through which all data streams and decisions flow, facilitating streamlined management of complex systems (MITRE Corporation, 2021). Centralized SCs are particularly effective in environments requiring strict operational control, such as public safety, military operations, or government crisis response (Schneider Electric, 2022).

The primary advantage of a centralized structure is its ability to maintain robust control over operations. By centralizing functions, the SC minimizes inconsistencies across units and standardizes protocols, enhancing monitoring and management efficiency (Deloitte, 2022). This unified approach ensures consistent performance standards, optimizing system performance in high-stakes scenarios (Eurofunk, 2023). For instance, centralized EOCs in the United States integrate data from regional agencies to coordinate disaster response, ensuring alignment with national priorities (Deloitte, 2022).

Technically, the central hub is equipped with advanced infrastructure, including high-capacity servers, redundant data storage systems, high-speed communication networks, and interactive visualization tools (MITRE

Corporation, 2021; Schneider Electric, 2022). These resources enable real-time processing of diverse data sources—such as sensors, surveillance feeds, field reports, and mobile units—critical for time-sensitive decision-making. A central data centre manages these streams, leveraging parallel computing to handle large datasets efficiently, as seen in military C2 systems processing intelligence data (MITRE Corporation, 2021).

Centralized structures are effective for scenarios prioritizing organization and coordination but may face challenges like single-point failures, necessitating robust redundancy measures (Eurofunk, 2023). Nevertheless, this model remains a cornerstone of SC architecture in high-control environments.

2.2 Decentralized SC Structure

A decentralized situation centre structure distributes data processing and decision-making functions across multiple autonomous centres, each capable of operating independently while coordinating through secure communication networks (Eurofunk, 2023; Everbridge, 2022). Unlike centralized models, which rely on a single hub, decentralized systems enable regional or specialized centres to collect, process, and analyze data, making decisions tailored to local conditions (Fraunhofer IIS, 2023). This architecture enhances flexibility and adaptability, making it ideal for dynamic environments such as crisis management or distributed enterprises (Bryghtpath, 2023).

The primary advantage of decentralization is enhanced system resilience. If one centre fails—due to natural disasters, cyberattacks, or conflicts—others continue functioning, preventing systemic collapse (Eurofunk, 2023). For example, decentralized crisis management platforms, like those used in U.S. corporate security operations, allow regional teams to respond swiftly to localized threats while maintaining network-wide coordination (Everbridge, 2022). This autonomy enables rapid decision-making, accounting for regional specifics without requiring central approval, which is critical in large-scale crises (Fraunhofer IIS, 2023).

Decentralized SCs rely on robust network communications to ensure interoperability. Secure, high-speed channels facilitate real-time data exchange, enabling centres to share situational updates and coordinate with higher authorities when needed (Eurofunk, 2023). Such systems are prevalent in global commercial organizations, such as retail chains or logistics networks, where regional branches operate autonomously but align with corporate objectives through integrated platforms (Bryghtpath, 2023). For instance, distributed supply chain systems use decentralized data spaces to maintain operations during disruptions, enhancing resilience (Fraunhofer IIS, 2023).

Despite its strengths, decentralization may introduce coordination challenges, requiring standardized protocols to prevent fragmentation (Eurofunk, 2023). Nevertheless, the model's flexibility, resilience, and rapid response capabilities make it well-suited for high-risk, fast-changing scenarios demanding local autonomy.

2.3 Hardware infrastructure

Situation Center hardware infrastructure forms a complex, high-tech ecosystem that integrates various technical components to ensure seamless operations and effective information management (McKinsey & Company, 2023). Key elements include high-performance servers, redundant storage systems, advanced communications networks, and interactive visualization technologies (Schneider Electric, 2025). These interconnected systems provide a robust platform for processing extensive data sets from sources such as sensors, surveillance feeds, and field reports, enabling real-time decisions critical to management, safety, and crisis response (CBRE, 2025; Vantage Data Centers, 2023).

The hardware infrastructure of situation centres forms a sophisticated ecosystem integrating servers, storage systems, communication networks, and visualization technologies to enable real-time data processing and decision-making (Deloitte, 2022; Schneider Electric, 2023). High-performance servers, equipped with advanced processors and substantial RAM, leverage parallel and distributed computing to process large datasets from diverse sources, such as surveillance cameras, sensors, social media,

and field reports (MITRE Corporation, 2021). High-capacity storage systems, including storage area networks (SANs) and distributed file systems, ensure rapid data access and reliable archiving, critical for operational continuity (Schneider Electric, 2023).

Communication systems, encompassing local area networks (LANs), high-speed internet, satellite links, and specialized secure networks, facilitate seamless data exchange with external sources, including field devices and cloud services (Atos, 2022). Redundant links and failover mechanisms enhance reliability, ensuring system resilience during crises, such as natural disasters or cyberattacks (Deloitte, 2022). Visualization systems, including video walls, multi-monitor workstations, and augmented reality (AR) interfaces, transform complex data into accessible formats—such as graphs, maps, and 3D models—enabling operators to monitor and respond to dynamic situations effectively (MITRE Corporation, 2021; Atos, 2022).

Integration of these components is achieved through specialized software platforms that synchronize servers, storage, networks, and visualization systems, minimizing latency and ensuring continuous operation (Schneider Electric, 2023). This cohesive infrastructure underpins the SC's ability to deliver rapid, informed decisions in high-stakes environments, though regular maintenance is required to sustain performance (Atos, 2022).

Thus, the hardware infrastructure of situation centers is a complex and highly efficient system, where each component plays its own important role in ensuring smooth operation and prompt decision-making. Proper integration of all elements and their reliability is the basis for successful operation of a Situation Center, which must be ready to respond quickly under any conditions.

2.4 SC Software Infrastructure

The software infrastructure of situation centres orchestrates data collection, processing, analysis, and visualization to support real-time decision-making in dynamic environments (Juvare, 2025; Rostelecom, 2023). Comprising data management systems, analytical platforms, and visualization software,

this infrastructure integrates diverse components into a cohesive ecosystem, enabling operators to respond effectively to crises (Atos, 2022).

Data Management Systems form the foundation, aggregating and processing information from sources such as sensors, surveillance cameras, social media, and emergency service channels (Kaspersky, 2022). These systems utilize relational databases (e.g., SQL) for structured data and non-relational databases (e.g., NoSQL) for unstructured or semi-structured data, ensuring scalability and accessibility (Rostelecom, 2023). Real-time data streaming technologies, such as Apache Kafka, enable immediate processing, critical for rapid response during crises like natural disasters or security incidents (Deloitte, 2023). Integration tools harmonize heterogeneous data formats, enhancing security and availability through robust encryption and access controls (Kaspersky, 2022).

Analytical Platforms leverage statistical methods, machine learning (ML), artificial intelligence (AI), and predictive analytics to derive actionable insights (Springer, 2024). ML algorithms analyze historical and real-time data—such as incident records, weather patterns, or traffic flows—to forecast potential crises, enabling proactive risk management (Juvare, 2025). For example, AI-driven platforms in U.S. EOCs predict flood risks by modeling hydrological and population data, optimizing resource allocation (Deloitte, 2023). Predictive analytics employs statistical models to anticipate scenarios, supporting strategic planning and consequence assessment in uncertain conditions (Springer, 2024). These platforms enhance SCs' ability to not only react to events but also anticipate their progression, as seen in Russian public safety systems forecasting urban incidents (Rostelecom, 2023).

Data Visualization Software transforms complex data into intuitive formats, facilitating rapid situational awareness (Atos, 2022). Geographic information systems (GIS) display real-time event locations on interactive maps, aiding response coordination during crises like wildfires or terrorist incidents (Juvare, 2025). Charts and graphs, ranging from linear trends to multivariate analyses, highlight anomalies and trends, supporting operational decisions (Springer, 2024). Advanced visualization, including augmented reality (AR) and virtual reality (VR), provides spatial context for emergency

management, enhancing decision accuracy in European C2 systems (Atos, 2022). For instance, AR interfaces overlay data onto real-world environments, improving operators' perception of critical infrastructure risks.

Integration ensures seamless interaction among these components, achieved through application programming interfaces (APIs), data buses, and specialized platforms (Rostelecom, 2023). These tools create a unified ecosystem where data flows continuously, enabling operators to act on accurate, up-to-date information (Kaspersky, 2022). However, integration complexity may pose challenges, requiring standardized protocols to prevent latency or data silos (Deloitte, 2023). By combining robust data management, advanced analytics, and intuitive visualization, SC software infrastructure empowers operators to make informed decisions, anticipate threats, and mitigate risks effectively in high-stakes scenarios.

2.5 Data Security and Protection

Data security in situation centres is critical for safeguarding sensitive information in government, military, and critical infrastructure contexts, where breaches or cyberattacks could lead to severe security, economic, or political consequences (CISA, 2024; Rostelecom, 2023). A robust SC architecture integrates advanced cybersecurity measures with comprehensive physical security to ensure the confidentiality, integrity, and availability of data and systems (Secure I.T. Environments, 2024).

Cybersecurity

SCs process vast datasets, including classified security, citizen, or military information, necessitating sophisticated cybersecurity defenses (Kaspersky, 2022). Firewalls, deployed as hardware or software, filter inbound and outbound network traffic, blocking unauthorized access and mitigating vulnerabilities (Splunk, 2024). For example, U.S. critical infrastructure SCs use next-generation firewalls to protect against ransomware and network intrusions (CISA, 2024). **Intrusion Detection and Prevention Systems** (IDS/IPS) monitor network traffic for malicious activity. IDS identifies threats through signature-based or behavioral analysis, alerting administrators,

while IPS actively blocks suspicious activities, such as distributed denial-of-service (DDoS) attacks, before they cause harm (Atos, 2022). Russian SCs employ IDS/IPS to secure government networks against state-sponsored cyber threats (Kaspersky, 2022).

Data encryption ensures confidentiality during storage and transmission, rendering intercepted data unreadable without decryption keys. Protocols like SSL/TLS secure communication channels, critical for military SCs handling sensitive operations (Rostelecom, 2023).

Authentication and access control systems, including multi-factor authentication (MFA) combining passwords with biometrics or smart cards, restrict access to authorized personnel, reducing risks of insider threats or credential theft (Secure I.T. Environments, 2024). For instance, European public safety SCs implement MFA to protect real-time crisis data (Atos, 2022).

Physical Security

Physical security is equally vital, as unauthorized access to SC facilities can compromise even the most robust cybersecurity measures (Splunk, 2024). Access control systems employ biometric identification (e.g., fingerprint or iris scanning), smart cards, or PINs to restrict entry to sensitive areas, such as server rooms, ensuring only authorized personnel gain access (Rostelecom, 2023). Video surveillance, including closed-circuit television (CCTV) and motion sensors, monitors indoor and outdoor areas, enabling rapid detection of suspicious activity. UK data centres integrate CCTV with AI-driven analytics for real-time threat identification (Secure I.T. Environments, 2024).

Server and computing rooms are fortified with metal doors, environmental controls (e.g., temperature, humidity), and redundant power supplies to protect against physical tampering or natural disasters (Splunk, 2024). Russian SCs for public safety use climate-controlled server rooms to ensure operational continuity during crises (Rostelecom, 2023). Backup systems, such as uninterruptible power supplies (UPS) and emergency cooling, maintain functionality during power outages or extreme conditions, critical for U.S. EOCs managing disaster response (CISA, 2024).