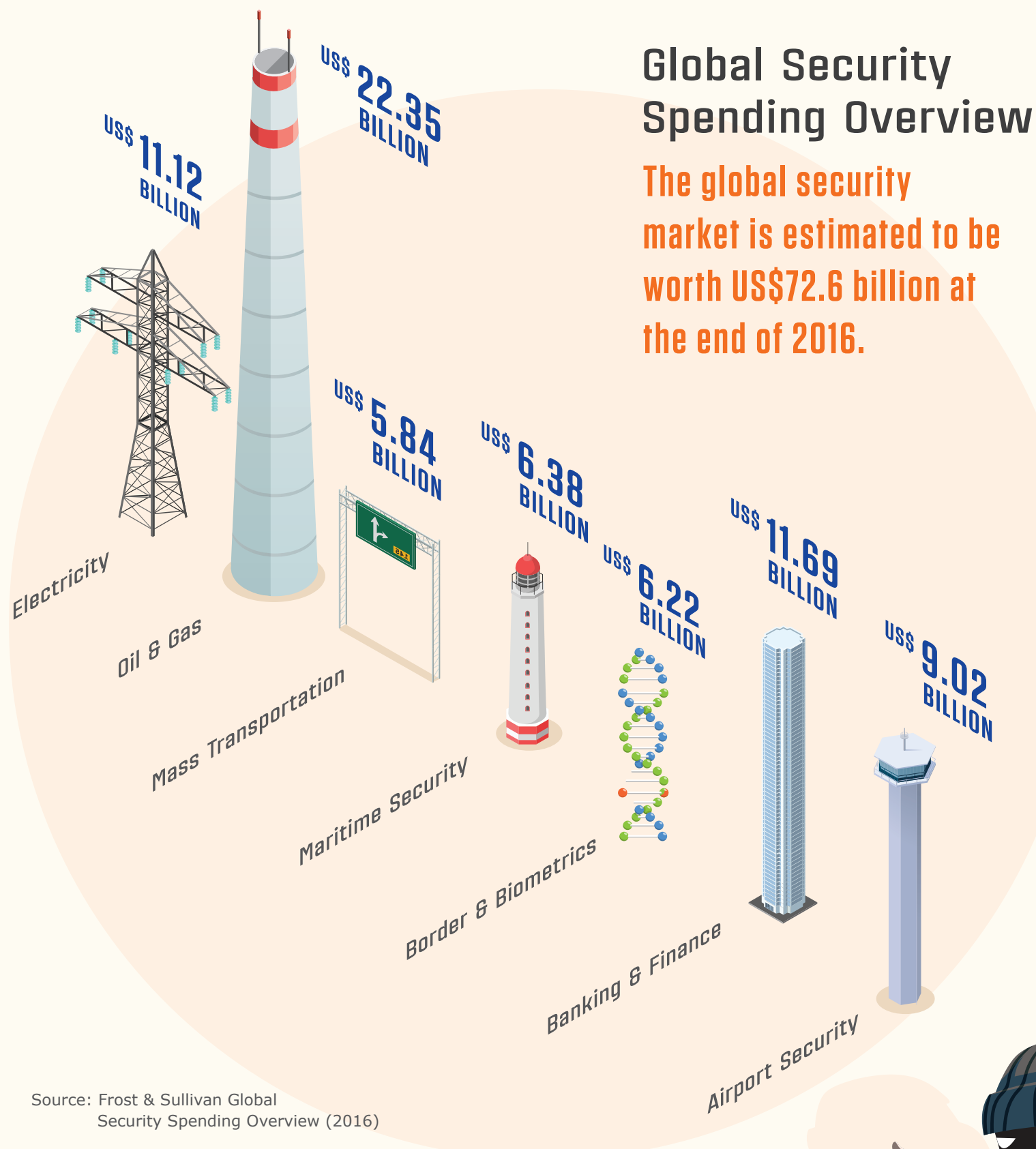


INTEGRATING CYBER-PHYSICAL SECURITY FOR A SAFER CITY

Addressing the Emerging Risks to Critical Infrastructure with Cyber-Physical Solutions



Source: Frost & Sullivan Global Security Spending Overview (2016)

Why Security is a Key Priority for Smart Cities

Connected infrastructure

Convergence of operational technology and information technology

Disconnect between physical security and cyber security

Cyber-attacks potentially disrupting critical services

DDoS* Attacks: A Growing Threat



240% increase in botnet activity, traced mostly to 900 compromised CCTV cameras

25,513 IP cameras compromised in a DDoS attack, including 24% from Taiwan, 9% from Indonesia, and 6% from Malaysia (2016)

152,000 IoT devices (e.g., CCTV cameras and personal video recorders) compromised in a 1Tbps DDoS attack

*Note: Distributed denial-of-services

Security Technology Forecast: Key Areas To Watch

AIRPORTS



ELECTRICITY



OIL & GAS



Source: Frost & Sullivan

AIRPORTS

Physical
Long screening queues at security checkpoints

Cyber
Automated check-ins, baggage drops, and ID scans

KEY TECHNOLOGIES

- Multimodal biometrics
- Facial recognition algorithms
- Network-wide multilayer defenses
- Advanced protection gateways for SCADA networks

NATURAL DISASTER MANAGEMENT

Physical
Lack of disaster planning and recovery practices

Cyber
Remote attacks on critical infrastructure

KEY TECHNOLOGIES

- Environmental sensors in risk-prone areas
- Advanced predictive analytics
- Emergency Incident Response
- Vulnerability identification, mitigation and management system

CITIZEN SAFETY

Physical
Physical threats in densely-populated areas

Cyber
Data breaches in public domain

KEY TECHNOLOGIES

- Behavior Analysis
- Video Data Analytics
- Incidence Reporting
- Cyber security forensics

CRITICAL INFRASTRUCTURE OPERATIONS: TOP 6 AREAS OF VULNERABILITY

Stadium/ Big Events

Physical
Hostile-aggressive individuals/crowds

Cyber
Attacks on networks to cripple operations and cut power

KEY TECHNOLOGIES

- High-resolution cameras
- Behavioral analytics
- Real-time networking monitoring
- Next-generation firewalls

ELECTRICITY

Physical
Vandalism/terrorism of plants/critical facilities

Cyber
Connected devices as new grid invasion access points

KEY TECHNOLOGIES

- Multi-layered defence for SCADA
- Intrusion Detection
- High-resolution cameras
- Behavioral & Video Data Analytics

GOVT SERVICES

Physical
Vandalism, theft, and/or disruption of services

Cyber
Cyber-attacks motivated by political dissent

KEY TECHNOLOGIES

- Multimodal biometrics for access control
- Behavior Analysis
- Detection of cyber threats and data leaks, and identification of cyber-attack patterns
- Intrusion Detection

Capture key insights on securing cities in an increasingly connected world



SCAN HERE TO READ THE WHITE PAPER OR VISIT nec.com/safecity