CYBERSECURITY OF HYBRID THREATS TO ORGANIZATIONS USING GEOSPATIAL TECHNOLOGIES

AN INNOVATIVE APPROACH TO PROTECTION AGAINST MODERN HYBRID THREATS THROUGH THE INTEGRATION OF GIS TECHNOLOGIES AND INTELLIGENT MANAGEMENT

Ph.D., Associate Professor, Department of Cybersecurity and Information Technology

TETYANA NALIVAYKO

Purpose of the article

- To develop an innovative geospatial model that combines GIS capabilities with intelligent forecasting and dynamic resource management to ensure proactive resilience of organizations against hybrid threats.

- Geographic information systems (GIS) are an ideal tool for raising awareness among all management personnel within an organization, as they are capable of modeling both physical and virtual environments.

- GIS is an automated system that collects, stores, integrates, and graphically represents spatial information in the form of diagrams or maps.

The purpose of creating a GIS for organizational cybersecurity

- A comprehensive GIS platform will ensure early detection and rapid response to cyber intrusions into information and data. The GIS platform can be used to combine location and cyber activity data, as well as other information, for better forecasting, detection, response, and recovery from cyber incidents. GIS technologies also make it possible to provide relevant information to other management entities within the organization for effective decision-making and coordination of joint actions, thereby promoting business continuity and resilience.

- GIS enables organizations to protect their electronic resources, quickly detect and prioritize cyber threats, and create a geospatial solution that integrates all available data to reduce uncertainty.

Challenges of hybrid threats to organizations

Cyberattacks

Targeted attacks on critical infrastructure and communication systems

Disinformation

Spreading false information through social media

Physical impact

Combining digital and kinetic methods of influence

Levels of geospatial integration in GMDS

GMDS uses a GIS platform to overlay and correlate data from five dynamic layers:

- 1. Physical/kinetic layer (P-layer): Reflects the physical location of critical ITCS and their dependence on support systems (e.g., power supply and environmental control). Takes into account the impact of non-digital, kinetic events (weather, land use, population density) on electronic systems to predict the risk of critical facilities being taken out of service.
- 2. Critical data flow level (CSL layer): Inherits the CSL model, identifying all devices that allow priority data types to be transferred from source to destination. The organization's mission performance directly depends on the correct operation of devices in the CSL. In military and special networks (NPM, BSM), this layer includes monitoring quality indicators (bandwidth, delay, packet loss).
- 3. Cyber layer (C-layer): Collects and intelligently analyzes traditional cyber indicators, event logs, and anomalies. The central element here is the application of genetic algorithms and methods of reducing the dimensionality of the feature space to identify the invariant component in the behavior of a polymorphic or metamorphic malware. This allows identifying the vector of destructive influence of malware, even if its code is constantly changing.
- 4. Reputation and trust level (T-layer): Focuses on user safety and cross-domain interaction. Geolocates sources of information threats (e.g., activity in social

Dynamic management mechanisms in the DRM layer

Spatial risk modeling	Intelligent network management	Cyber security adaptation
Uses cognitive modeling to quantitatively assess hybrid threat levels and predict losses. This allows the GIS platform to visualize high-risk spatial-temporal zones (e.g., areas where the convergence of data from the P-layer (physical vulnerability) and C-layer (cyber activity) is highest)	Adaptive algorithms are applied in high-risk areas to increase resilience (which is an integral indicator of survivability, reliability, interference immunity, and cyber security)	The DRM layer uses the results of the C-layer analysis of invariant behavior of the network infrastructure to automatically update security policies (e.g., SIEM systems or intrusion detection mechanisms) and firewall configurations, focusing on preventing new modifications of known threats

Structure of GMDS integration levels

The model consists of five interacting levels that are displayed on a single geospatial map, allowing cyber indicators to be correlated with physical and social factors

Level	Main threat vector	Integrated geospatial assets
I. Physical/Kinetic (P-layer)	Anthropogenic, natural, intentional, and accidental threats	Physical ITCS objects, support infrastructure (power supply, environmental control), terrain data (3D maps)
II. Critical Data Streams (CSL layer)	Risks to data availability and integrity	All devices that provide priority data transmission for mission execution
III. Cyber Level (C-layer)	Cyberattacks, viruses, hacker attacks, polymorphic malware	Localized cyber indicators, SIEM system event logs, network traffic anomalies
IV. Reputation and Trust (T-layer)	Disinformation, social engineering, authentication attacks	Geolocation of users and devices, PKI certificates, reputation mechanisms
V. Dynamic Resource Management (DRM layer)	Insufficient response speed and suboptimal resource allocation	Intelligent forecasting results and dynamic management decisions tied to space and time

Intelligent forecasting (proactive component)

GMDS uses the DRM layer for forecasting and risk assessment. The task of predicting dangerous actions is complex and requires knowledge in various fields. A hybrid approach is used:

- 1. Cognitive and expert modeling: Expert assessments are used to understand the context, and cognitive maps are used to quantitatively assess the impact of hybrid threats on national security and predict losses. This allows us to determine indicators of dangerous actions (security risks, system vulnerability, potential damage).

- 2. Analysis of the invariant component of the C&I: To counter polymorphic/metamorphic C&I, the DRM layer integrates machine learning with genetic algorithms. The method is based on reducing the dimensionality of the feature space to select a subset of features that describes the invariant (unchanging) behavior of malware, regardless of its constant modification. This allows for proactive updating of defense strategies even before new malware mutations are classified by traditional antivirus tools.

Dynamic adaptation and reconfiguration (management component)

After identifying spatial-temporal risk zones, the DRM layer automatically adjusts protection:

- Communication system resilience management: communication system resilience is an integral indicator that includes survivability, reliability, interference protection, and cyber protection. In the context of hostilities in Ukraine, where the enemy widely uses electronic warfare (EW) means, the DRM layer calculates resilience based on the combat capabilities of troops and the predicted degree of fire damage (FD).
- Intelligent routing (NMP): to ensure continuous and adaptive real-time control, the DRM layer uses hierarchical intelligent NMP control systems based on reinforcement learning (RL). If there is a threat of kinetic damage (P-layer) or radio silence (CSL-layer), the DRM layer applies optimized multi-threaded algorithms, such as MBD-RRT*FFT, to quickly plan the optimal path for UAVs or UAVs in a dynamic urban environment.
- Communication interference protection: to counteract interference, the DRM layer controls Smart antennas (e.g., ring antenna arrays) to form a dip in the directional pattern in the direction of the interference source. In critical cases, the DRM layer switches communication to highly secure terahertz networks using algorithms such as M-SO-NOMA, which increases the reliability of data transmission even when line of sight is blocked.

Geospatial perimeter protection model (enhanced component)

Within GMDS, cybersecurity activities are viewed as a sequence of measures aimed at reducing risks and vulnerabilities. The GIS platform provides data to answer five key questions:

- 1. Was there an attempt to compromise the organization's ICT? (SIEM systems are used that can integrate fuzzy models for detecting cyber incidents with weighted antecedents of rules to improve effectiveness in conditions of uncertainty).
- 2. If so, was it successful? (Comparison of perimeter defense data with geospatial data, including geolocation of vulnerable access points).
- 3. What are the technical consequences of the incident? (Classification of consequences related to the risk of critical data).
- 4. How did the compromise affect the organization's missions? (Assessment integrating the CSL layer).
- 5. How should the organization respond to the incident? (Decisions are made taking into account DRM layer forecasting).

Conclusions

The proposed geospatial model of dynamic stability (GMDS) is an innovative approach that systematically integrates geospatial awareness with the needs of proactive RCS security management in the context of hybrid threats.

- 1. The GDSM provides systematic integration of cyber (C-layer), physical (P-layer), logistical (CSL-layer), and social (T-layer) threats using a single geographic framework, which is necessary to counter combined hybrid methods.
- 2. The key innovation of the model lies in the creation of a Dynamic Resource Management Layer (DRM-layer), which uses intelligent methods (AI/ML) for: a) Predicting spatial-temporal risk zones. b) Adaptive protection against cyber threats by identifying the invariant component of their behavior. c) Optimizing the resilience of critical networks (NPM, SSZ) through dynamic routing (MBD-RRT*FFT) and the use of interference-resistant communication technologies (THz, Smart antennas, M-CO-NOMA).
- 3. Thus, GMDS enables the transition from reactive threat assessment to proactive security management, allowing organizations not only to have a comprehensive operational picture, but also to automatically adapt protective mechanisms to constantly changing threats.