The Geospatial Approach to Cybersecurity: An Executive Overview

An Esri® White Paper
January 2014

380 New York Street
Redlands, California 92373-8100 USA

800 447 9778
info@esri.com

esri.com

The Geospatial Approach to Cybersecurity: An Executive Overview

An Esri White Paper

Contents **Page**

The Geospatial Approach to Cybersecurity: An Executive Overview

Introduction

With organizations' increasing reliance on electronic communications comes the inherent risk of cyber attacks and cyber-enabled espionage. Realizing this, US President Barack Obama issued an executive order that cyber systems (computers and related technology) be considered critical infrastructure to the United States and its people and be protected as such.

The role of geospatial technology in the support of physical security is well known and understood. It is used for situational awareness, data management, multiple intelligence (multi-INT) fusion, analysis, and information sharing. Physical security is interdisciplinary and relies on multiple sources of information. Yet cybersecurity remains cloistered in information technology (IT) departments, separated from the rest of the organization.

Cyber defense should be assessed in terms of its direct contribution to the successful execution of an organization's primary mission. Cybersecurity should be integrated with the various business functions it is protecting. However, in the past, this tight integration has been difficult to achieve. Arguably, the reason for its difficulty is the lack of a common framework that can align the activities of mission specialists with experts in all the other security-related activities required to provide full mission assurance.

This paper introduces an approach to creating a geospatial framework that provides shared situational awareness (SSA) for the many activities associated with cyber defense. The goal of this framework is to enable a cross-disciplinary approach to providing organizational mission assurance and resilience by maintaining the availability of priority IT devices during and after a cyber attack. The key concept that makes a common framework possible is that cyberspace is a mechanism to deliver digital data where it is needed. If the data isn't delivered (or if it is inaccurate), then missions fail. By organizing network data, physical security systems, and other multi-INT sources such as weather, threats and warnings, and social media, Esri® ArcGIS® can provide the integrative framework for cybersecurity data.

Problem

Organizational leaders are increasingly concerned about the threat posed by cyber attacks. However, they generally aren't focused on the technical aspects of the event; they want to understand the impacts to their mission.

Before a cyber event occurs, leaders will ask

- What is the risk posed by a device malfunction?
- What can be done to mitigate the risk?

After the event, leaders need to know

- What is the mission impact of the event?
- Was this an attack?
- How do we recover our capability?
- How do we strengthen our ability to be resilient to future events?

Answering these questions can be a challenge for IT departments. Their work is predominantly focused on devices, and the mission-to-device relationship isn't always clear. IT divisions take action in prevention, protection, response, and recovery to operate and maintain the network. They must maintain the ability to respond to technology-driven maintenance requirements; however, there should be a way to prioritize prevention and monitoring activities based on current, short-term mission requirements. To respond to these challenges, leaders need a way to incorporate cyber data into their SSA tools to show the impact of cyber attacks on the organization's many other functions.

Cybersecurity Defined

Cybersecurity is a broad area that encompasses the protection of assets from cyber crime, cyberterrorism, and other network service disruptions that affect operations. Cybersecurity is achieved through active monitoring, detection of malicious activity, and timely reaction to threats. While security in the cyber world is different from that of the physical world, many similar security concepts can be applied to both. A key concept is that location is the foundation to which all activity can be organized.

Cyber Supply Line

Cybersecurity involves the coordination of many (sometimes disparate) departments including those involved in IT, system design, operations, network analysis, and maintenance, as well as industrial control and supervisory control and data acquisition (SCADA). Because of the complexity of these interwoven systems and applications, cybersecurity actions must be prioritized according to the organization's mission and activities. This requires understanding an organization's specific method of protection and, in the event of an attack, the response. Both protection and response require the coordination and sharing of information between operations, IT, and other departments based on an approach that Esri calls the cyber supply line (CSL).

Each organizational device exists within a geospatial context and can be affected by both physical and cyber disturbances. Protecting each device from all disturbances requires the unified effort of personnel from a variety of departments including operations, IT, security, utility, and civil engineering. Multiply this effort by the number of devices included in a typical organization and it is clear that the challenge to management is significant. The CSL provides a methodology to identify the most critical devices for the data flow of a specified mission. This reduces the number of devices being managed from thousands to a few dozen that are focused on the organization's most important missions at a particular time.

The direct coordination of all involved departments when responding to a cyber attack is generally not possible. Therefore, personnel must coordinate their responsibilities and activities indirectly by working from a common operational picture (COP) with visualizations customized for their specific needs. Those responsible for maintaining the flow of data must be able to identify and assess the impact of all potential disturbances and have the ability to contact individuals supporting the mitigation efforts as required.

From an architecture perspective, cybersecurity is simply a configuration of the ArcGIS platform's current capabilities; software development is not required. New customer data can be added to existing infrastructure data to quickly establish a more robust SSA capability.

ArcGIS is widely used within the national security community (defense, national intelligence, critical infrastructure protection, and emergency management). The ArcGIS platform is an out-of-the-box solution that provides the technology to fuse the logical, physical, and geographic data layers to provide comprehensive situational awareness.

The ArcGIS platform is able to model the behavior of cyberspace. ArcGIS Network Analyst and other Esri tools can be used to display the various data flows involved in sending organizational data between two locations. However, the real advantage in cybersecurity is the ability of ArcGIS to model effect propagation between layers. For example, a device outage caused by a flood could have a significant negative impact to organizational operations half a world away.

Conclusion

The ArcGIS platform can be used to fuse location data, cyber activity data, and other information to better anticipate, detect, respond to, and recover from cyber incidents while providing SSA of cyberspace and associated activities.

The platform includes tools, workflows, and applications that can be implemented with an organization's existing cybersecurity data and technologies to improve

- Data management (big data from various sources including security logs and social media).
- Analysis and fusion (incident analysis, pattern analysis, predictive analysis and multi-INT fusion).
- Visualization for situational awareness (real-time visualization of network/node status, incidents, current network traffic, and continuity of operations).
- Information sharing (dashboards for a COP of the network, data traffic, and incidents).

If you would like to know more about the use of ArcGIS for cybersecurity and the implementation of the cyber supply line, we welcome the opportunity to discuss your requirements and provide a demonstration of the power of ArcGIS for cybersecurity. Please contact us at cybersecurity@esri.com.

Esri inspires and enables people to positively impact their future through a deeper, geographic understanding of the changing world around them.

Governments, industry leaders, academics, and nongovernmental organizations trust us to connect them with the analytic knowledge they need to make the critical decisions that shape the planet. For more than 40 years, Esri has cultivated collaborative relationships with partners who share our commitment to solving earth's most pressing challenges with geographic expertise and rational resolve. Today, we believe that geography is at the heart of a more resilient and sustainable future. Creating responsible products and solutions drives our passion for improving quality of life everywhere.

Contact Esri

380 New York Street
Redlands, California 92373-8100 USA

1 800 447 9778
T 909 793 2853
F 909 793 5953
info@esri.com
esri.com

Offices worldwide
esri.com/locations

Printed in USA