The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations

An Esri® White Paper
June 2015

380 New York Street
Redlands, California 92373-8100 USA

800 447 9778
info@esri.com

esri.com

The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations

An Esri White Paper

Contents **Page**

The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations

Introduction

Cyber threats affect more than just the information technology (IT) infrastructure of a company or command. These threats cause disruptions to its entire network that can impact its principal business functions and mission. As such, cybersecurity should be assessed in terms of its direct contribution to the successful execution of an organization's primary mission.

Organizations can no longer ignore cyber threats or delegate security to the information technology department. Cyber defense must be integrated into traditional security activities, such as physical and personnel security as part of an overarching effort to protect business operations from both external and internal threats. Cybersecurity activities must be prioritized and aligned to strategic business activities.

Geographic information system (GIS) technology is the foundation needed to establish shared situational awareness for interdisciplinary activities.

This paper describes the implementation of the ArcGIS® platform as the GIS solution that can deliver shared situational awareness for the various activities associated with cybersecurity. The goal of this solution is to improve cyber defense and to enable a cross-disciplinary approach to providing organizational mission assurance by maintaining the availability of IT systems.

Problem Definition

In the 2013 edition of its Data Breach Investigation Report, Verizon summarized 10 years of data relating to cybersecurity (Verizon 2013). The report explains how over time, cybersecurity incidents have become more frequent and more damaging to their targets.

Of particular concern, it noted that while approximately 90 percent of successful cyber compromises are executed in a matter of hours, less than 25 percent are quickly detected. Most successful intrusions aren't discovered until months after the compromise. Additionally, 70 percent of compromises are only discovered when third parties report finding the victim's data "in the wild."

During the same 10-year period, there were huge increases in the amount of resources dedicated to improving cybersecurity. So why hasn't progress been made? When the Business Software Alliance (BSA), a group of the world's leading software companies,

created a task force in 2002 to research this question, it reached the following conclusions (Business Software Alliance 2003):

- There is already a broad consensus on the actions necessary to remedy the problem.
- Information security is often treated solely as a technology issue when it should also be treated as a governance issue.
- The lack of progress is due in part to the absence of a governance framework.

Since the release of the BSA report, additional cybersecurity legislation was ratified and more cyber frameworks were created, which include Control Objectives for Information Technology (COBIT) 5; Information Technology Infrastructure Library (ITIL) Framework; International Organization for Standards (ISO) 27001; and most recently, the National Institute of Standards and Technology (NIST) Cybersecurity Framework. These frameworks are all authoritative, extensive, and detailed. So the question remains, why haven't we made more progress?

Unfortunately, these frameworks are incomplete in a critical way. Each does an outstanding job of describing

- What tasks should be accomplished to improve cybersecurity.
- Who should accomplish the tasks.
- Why the tasks should be undertaken.
- How to accomplish the tasks.

What's Missing

What is missing is an indication of when and where the tasks should be implemented. No organization is sufficiently resourced to maintain all controls, on all devices, at all times. Not having a means to prioritize necessary actions could result in the implementation becoming reactive and ad hoc, leaving exploitable holes in an organization's cyber defenses and responses.

A mechanism is needed to determine the *where* and *when* that enables execution of the tasks described so well in the various cyber frameworks. This mechanism must be more than just a framework. It must be able to model an organization's entire environment, both physical and cyber; assign collected data to the model; quickly identify threats; and empower planners to determine the optimal courses of action.

By combining traditional cyber indicators with a geospatial platform, organizations can quickly discover and prioritize all manner of cyber threats, both natural and man-made, intentional or accidental, by creating a comprehensive model that integrates all available data. The result is organization-wide agility that combines physical and cyber activities when responding to service interruptions and complex intrusions. It also prioritizes preemptive actions that can prevent disruptions or mitigate their impact.

G69472

Cyberspace Reconsidered

The primary motivation for modern organizations to rely so heavily on cyberspace is that it allows them to efficiently, effectively, and economically coordinate activities across dispersed locations in near real time. Cyberspace is critically dependent on electromechanical devices and personnel that make up its components in the physical domain or layer. The Department of Defense Joint Publication 1-02 defines *Cyberspace* as "The interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

The virtual environment includes four layer types: data, device, network, and geographic.

It is clear that cyberspace consists of a complex mix of data, devices, and people. The US Army Training and Doctrine Command (TRADOC) states the virtual environment consists of four different types of network layers, each of which has nodes that are locatable in space-time. These include the data, device, network, and geographic layers.

Data layers are often assigned based on the type of node used, whether a person or device. However, it is useful to think of each node layer as being defined by its type of dataflow. For information to be exchanged at the social level, documents must flow in the device layer. For documents to be exchanged, packets must flow at the network layer. And for packets to be exchanged, electromagnetic energy flows between two specific points in space-time, represented by the geographic layer.

Device status is the mechanism that couples the various layers. If a router fails at the network level, some subset of hosts at the device level will be denied required packets. The loss of packets results in the devices being unable to exchange documents and some users being denied required information. It is the loss of information, not devices, that directly impacts a mission. This analysis demonstrates that cyberspace is not virtual; it is hierarchical. This vertical analysis adds rigor to the mission impact assessment of cyber disruptions. Without this structure, mission-impact assessment has often been ad hoc.

The Geographic Layer and the ArcGIS Platform

The geographic layer serves as the common integrating framework for all the layers previously discussed. Integration is achieved by geolocating all nodes, including people, user devices, and infrastructure devices, and the edges that connect them within a layer and between layers. Geospatially enabling the common operational picture (COP) allows users to consider the effect of noncyber, kinetic events in relation to cyber devices. Traditional geospatial datasets, such as weather, land use, and population density, can provide value to cyberspace operators when assessing risk to their communications networks. Regardless of the cause of the disruption, cyber operators must be able to anticipate the risk of failure for certain, critical devices and then determine the mission impact of those device failures.

Mapping all the layers to the geographic layer provides the common baseline from which comprehensive shared situational awareness can be achieved. A comprehensive GIS platform must be able to support user workflows, collaboration, and dynamic situational awareness to meet a variety of mission requirements. The technology is available on many devices and networks, providing personnel with access to information and data to support decisions for awareness, prevention, protection, response, and recovery. Information can be quickly accessed, understood, and shared to support coordinated actions.

The GIS platform can be used to fuse location and cyber activity data and other information to better anticipate, detect, respond to, and recover from cyber incidents. It is easily integrated into an organization's existing command and control structure to ensure that leadership has access to complete and accurate data for decision making. GIS platforms are already widely used within national security including defense, national intelligence, critical infrastructure protection, and emergency management organizations. Extending this capability to incorporate cyber alongside more traditional domains is incredibly powerful and allows for improved synchronization of security efforts.

Cyber Operations Defined

The Department of Defense Joint Publication 1-02 defines *Cyberspace Operations* as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." Operations conducted in cyberspace can be divided into three activities based on the process being affected and the location of the network on which the activities are being conducted. These activities include network operations (NETOPS), defensive cyber operations, and offensive cyber operations.

NETOPS involves the design, installation, operation, and maintenance of computer networks to make an organization's processes more efficient. In a physical comparison, it can be said that NETOPS organizations create the terrain on which defensive and offensive cyber units act.

Defensive cyber operations involve physical, personnel, and network security measures which are conducted on one's own network and intended to ensure the availability and reliability of IT resources, capabilities, and data. Offensive activities are those in which operations are conducted on the network of an adversary to disrupt its processes.

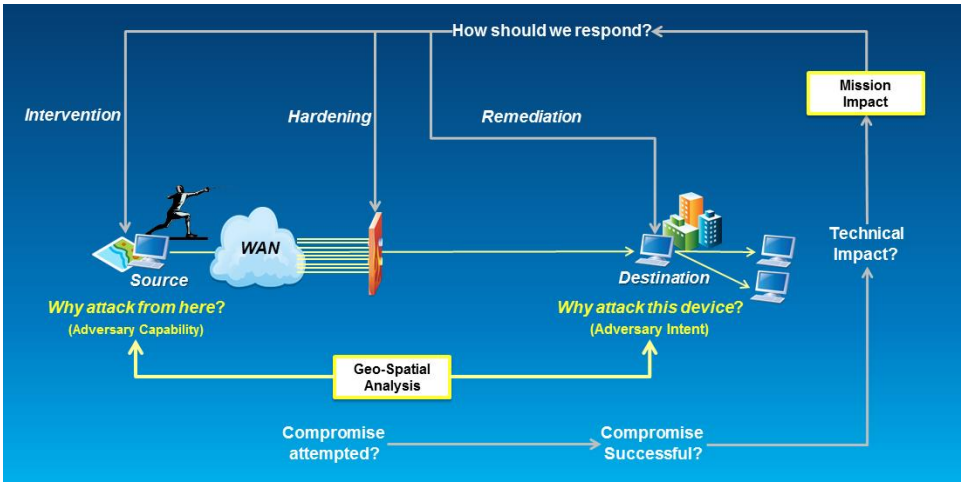
This paper focuses on defensive cyber operations; however, the solution can be applied to offensive operations where permitted.

A Geospatial Solution to Cybersecurity

Cybersecurity is a broad area that encompasses the protection of assets from cyber-crime and terrorism and other network service disruptions that affect operations. Cybersecurity is achieved through active monitoring, detection of outages or malicious activity, and the timely reaction to disruptions. 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 on which all activity can be organized, visualized, and shared for efficient decision making. 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. GIS enables organizations to apply these concepts to the protection of cyber resources to quickly discover and prioritize cyber threats by creating a geospatial solution that integrates all existing data to reduce uncertainty. The goal is to enable early detection and organization-wide agility when responding to cyber intrusions. Figure 2 depicts the cyber defense process as a series of five assessments which must be made (in order) for each suspect event. Geospatial analysis can support two of these assessments: (1) the geospatial model for perimeter defense to assist with an assessment of whether or not a compromise was attempted and (2) Cyber Supply Line (CSL)-based mission impact assessment.

Organizational leaders are increasingly concerned about disruptions to cyber resources and the coordinated actions needed to ensure operations, business continuity, and resiliency. Configuring the ArcGIS platform for cybersecurity enables organizations to better align their business operations with those of facilities, IT, and security to be part of a broader, organization-wide effort to mitigate cyber threats. A GIS platform provides tools that allow personnel to coordinate maintenance, response, and recovery activities indirectly by working from a COP with visualizations customized for their specific needs. Those responsible for maintaining the flow of data are able to identify and assess the impact of potential disruptions and have the ability to contact individuals supporting the mitigation efforts, as required.

G69472



This graphic depicts the cyber defense process and highlights Esri's two focus areas: the geospatial model for perimeter defense and the Cyber Supply Line (CSL)-based mission-impact assessment.

Geospatial Model for Perimeter Defense

Defensive cyber activities include detecting specific adversaries that pose a threat to an organization's network and preventive measures that focus on mitigating risks and vulnerabilities.

Cyber defense is best understood as a sequence of five questions. Any suspicious activity, regardless of the organization or discipline that attempts it, can be grouped according to the response to the following questions. Organizing cyber defense by response provides an open system in which any new technology/techniques can be easily incorporated. These questions assume there is an existing network that is instrumented in various ways to provide data:

- Is a compromise being attempted?
- If so, was the compromise successful?
- What is the technical impact of the compromise?
- What is the mission impact of the compromise?
- How should the organization respond?

Technologies such as firewalls and intrusion detection systems can be used to determine if an organization's network is being threatened. Many of these devices face limitations such as high false alarm rates or the inability to identify novel attack vectors, for example, viruses and vulnerable access points. Determining whether a compromise was successful involves comparing data from both perimeter security and host-based security devices. The defense team must then determine the technical impact for all confirmed compromises. There are usually three outcomes: (1) The compromise puts critical data or functionality at risk, (2) the compromise provides access to other machines that put critical data or functionality at risk (i.e., a pivot attack), or (3) the compromise is limited to the victimized device. If either of the first two cases is true, a mission-impact assessment must be conducted to determine which organizational functions/missions are at risk. The final step is to determine the most appropriate mix of response options: (1) remediation, (2) network hardening, or (3) intervention at the source.

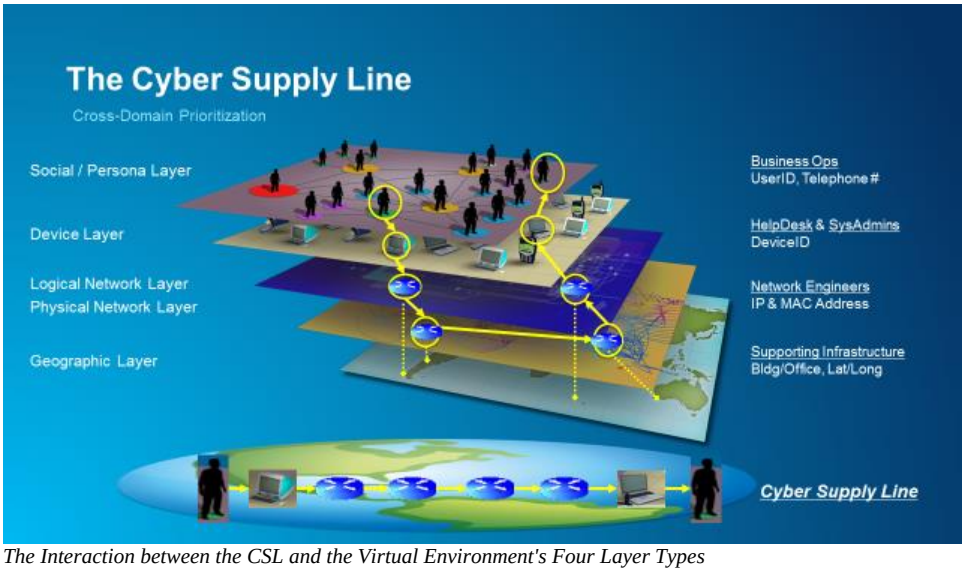
Based on the results of Verizon's data breach investigation, it seems that the IT and cyber defense communities are well positioned for prevention and response activities. What is difficult to determine is which network connections pose the greatest risk and how to assess the potential mission impact of those threats. Most organizations include perimeter security devices, such as intrusion detection systems, in their arsenals.

Cyber Supply Line-Based Mission Impact Assessment

The key concept that makes a common framework possible is that cyberspace is just a mechanism for delivering data to where it is needed. If the data isn't delivered or is wrong, then missions fail. Cyber mission assurance isn't about maintaining the entire network; it is about protecting the critical portions that are needed to deliver information from one particular source location to a specific destination in support of critical missions.

When prioritizing critical destinations, certain devices are deemed critical under all conditions. For example, authentication servers and databases containing sensitive data will always be critical. However, extending the static approach too far will limit an organization's agility and ability to prioritize responses. Some devices are only critical under certain conditions. The cyber supply line was designed to address this dynamic aspect of cyber defense.

Esri defines the CSL as all devices that enable a particular kind of data to be moved from one source to one destination. If multiple destinations are designated for a given dataflow, a cyber supply line exists from the common source to each user location because each will transit a different subset of the cyberspace infrastructure. In a packet-switched network, each CSL will be between 16 and 18 hops in length. A hop is defined as two devices composed of a combination of routers, switches, clients and servers, and the circuit that connects them. A circuit is simply an identifiable transmission media such as a length of cable, a satellite downlink, or a connection in a wireless network. Each device has a defined location in space-time, each is owned by an organization, and each has strict dependencies on support systems such as electrical and environmental control. If a device is on a CSL, a mission depends on its working correctly.



The Interaction between the CSL and the Virtual Environment's Four Layer Types

CSLs provide a common solution for business specialists and technologists to exchange requirements, priorities, and reports. To establish operational focus, an organization's leadership must prioritize the dataflows that are most critical, given existing business conditions. These requirements must be communicated to planners who may be widely dispersed across an organization. For example, leadership may state that secure voice communication between headquarters and a tactical command post be maintained throughout the duration of a humanitarian assistance operation on a different continent.

The NETOPS team takes each of the prioritized dataflows verified by leadership and identifies the mission network over which the data will likely flow. The mission network is created by identifying the shortest path then purposely failing each device to determine all likely routes the packets can take. Each route is a possible CSL. The goal of the NETOPS team is to prioritize its resources to ensure that priority data flows remain operational during a cyber attack by focusing its resources on devices on the mission network. Due to the recent trend toward network convergence, in which different types of data such as voice and video use the same infrastructure, separate dataflows will experience significant overlap at the mission network level. This establishes a cycle in which the efforts expended by NETOPS technicians on a single device will help ensure that multiple dataflows are secure. However, convergence does not alleviate the need to assess each prioritized dataflow. This analysis sets the stage for an agile response to any threats that may occur.

It is important to note that shared situational awareness is provided for each mission network rather than as a single, all-encompassing infrastructure solution. The goal is to determine the impact of a disturbance on each of the organization's priority missions. Allowing a customer to quickly model a network of interest facilitates mission impact assessment and provides operational focus for the many support organizations during remediation. In addition to hardening each device on a mission network, the NETOPS and cyber defense teams closely monitor these devices to quickly identify any event that might negatively impact a CSL.

Disruption of a CSL can occur if even a single device is disrupted, so the CSL sets the priorities for reporting. Just as this methodology allows precise requirements to be communicated from organization leadership to its technical staff, it also allows an organization's technical staff to easily communicate status and mission impact to the leadership. This consolidates and improves vertical communication within an organization. Additionally, the CSL can be used to establish seamless horizontal integration by providing precise communications requirements between organizations and their Internet and telecommunication service providers.

Since every device on a CSL is critical to overall performance, awareness of any event that could negatively affect a device must be immediate and widespread. Any collaborative scheme that requires all participants to maintain constant communication with one another cannot possibly be agile enough to defend priority resources in the cyber environment. Providing an effective common operational picture (COP) is a dramatic improvement over face-to-face communications in both quality and agility.

Owned versus Used Networks

It is important to understand the distinction between 'owned' and 'used' networks when considering CSLs. An organization will have complete knowledge of all the devices in a network that it owns. However, that knowledge is often very fragmented, residing at different locations and in different formats. Therefore, it is difficult to get a comprehensive picture of the network and its dependencies, especially in a crisis.

The first requirement in developing a framework for cybersecurity is to collect available data and put it into a GIS system. The data need not be complete and error free, though. The database can be built up over time. In fact, the geospatial context can be a very effective quality-control mechanism. However, some data to support initial workflows is a necessary prerequisite. The GIS platform provides the analytical engine that fuses location data and other information with a customer's own IT network data to better anticipate, detect, respond to, and recover from cyber incidents while providing shared situational awareness with cyberspace awareness and associated activities.

The CSL stack organizes the data in each level in the form of directed graphs, which allows users at each layer to model the consequence of various changes to the networks. Since disruptions at lower layers have significant effects at higher layers, the shared situational awareness must account for interrelationships of the various layers. The status of the device serves to couple the layers; each layer considers dependencies that can cause a malfunction within it. When a disruption is identified, models at all higher layers are rerun to determine if a given device change could cause mission failure.

Given the structure of today's telecommunications industry, it is extremely unlikely that a single organization will own the entire network that it uses. So a CSL will likely consist of devices provided by many organizations, making management a challenge. Typically, network providers give their customers very limited data on how the network operates. Once a CSL leaves an organization's network via a gateway device, its route cannot be known unless reported by the provider. This type of reporting by network providers is unusual at the present time.

If data from the network provider is unavailable, estimating techniques are required to complete the CSL model. It is unlikely that the estimates will be completely accurate, but they need not be. The goal is not for the executives to change the Internet to support their CSL; it is to change their behavior in light of Internet conditions that threaten the CSL. This is directly analogous to automobile navigation devices. They help the driver plan the most efficient route between two locations and report variables that affect the chosen route such as traffic conditions, road closures, and weather alerts. Drivers have no ability to affect any of these variables; however, they may decide to alter their route or the starting time or cancel the trip altogether if conditions don't support the drive. These are the same options available to executives when they lose confidence that particular CSLs will support their communication needs under the current environmental circumstances. The CSL-based shared situational awareness simply offers a tool to support risk analysis and management of the resources an organization can control.

Implementing the Cybersecurity Workflow

From the vast number of devices that make up cyberspace, the general solution strategy is to select only those that contribute to delivering a particular dataflow between two identified locations during a particular span of time. Once the CSL is identified, risk analysis is conducted to determine the resiliency of the network to various device disturbances. This allows the executive and technical teams to determine an overall confidence in the ability of the network to support a particular mission and prioritize actions to monitor and respond to possible service interruptions. This shared situational awareness for the mission establishes a context useful for preparing for an operation before it begins; prioritizing, reporting, and responding to various conditions while the operation is under way; and improving organizational response should something go wrong.

The first step is to collect an organization's fragmented data into a single geodatabase. The geodatabase is the common information model; meaning it is the central data repository for storing and managing spatial data.

The cyberspace to geospace nexus is the mapping of devices to locations. For devices owned by an organization, this mapping can be accomplished using existing IT inventory and facilities data. For all other devices, third-party databases can be used to provide approximate geolocations based on Internet Protocol (IP) addresses. Combining cyberspace and geospace data in this way enables model extension by executing external joins to geospatial datasets, using the coordinates of the device location. It also includes cyber datasets using device attributes such as IP and media access controller (MAC) addresses. The primary advantage of the geodatabase is to show how these similarities are distributed over space and time.

The next step is to conduct analysis on how the data will flow between devices to establish the mission network. The GIS platform provides all data fusion and analysis tools needed to allow organizations to derive information from their ever-increasing data stores. ArcGIS Network Analyst is an extension which combines nodes (devices) and edges (the circuits that connect the devices) into a single data structure. This allows a cyber analyst to run various scenarios that describe how the data will flow over the network between the two identified end points (source and destination locations).

Following route discovery, the analyst—still working in ArcGIS for Desktop—will produce a schematic dataset using the ArcGIS Schematics extension. ArcGIS Schematics provides a way to visualize a network in both geospatial and logical formats, allowing a user to visualize the network in the format most appropriate for the task at hand. ArcGIS Schematics integrates these two views so that changes in one are propagated to the other, ensuring that the most accurate, authoritative data is available regardless of which view is preferred by a particular planner or planning team. This allows planners to identify critical components based on the resultant network behavior when various changes are made. A prioritized list of components can then be constructed showing which devices have the greatest impact on the CSL and which must be monitored throughout the operation. This also establishes reporting priorities—leadership must be made aware of any threats to these critical devices.

Once the CSL is constructed, it can be published in a variety of ways across the organization through either a secure server or cloud-based architecture.

The purpose of the CSL concept is to provide a means by which cyber operational overlays can be integrated with other operational overlays (such as the power grid) then placed within the locational context of a basemap. The combination of operational overlays and a basemap provides a static model, as discussed earlier in this paper.

This architecture supports the real-time geospatial analysis of streaming data. Users can configure interfaces and analytic models to ingest streaming data, conduct automated analysis, save the new results, and generate a data stream and/or alerts to mobile users. The CSL can be used to focus the organization's attention on the dynamic data and sensor feeds that will have the greatest impact on a particular cyber mission. Streamed data, such as weather forecasts, flood reports, electrical outages, and even social media reports of social unrest, can be ingested into the platform and geospatially aligned to the CSL. This will determine the data's relevance, and then it will be assessed to determine its impact on the reliability of communications over the CSL. As such, the CSL provides the solution for a multi-INT, multidisciplinary approach to securing an organization's dataflows.

Access to data isn't sufficient to provide value to various workflows, so Esri developed a suite of tools to help organizations make the best use of the data being distributed. Distribution techniques in Operations Dashboard for ArcGIS, Esri Maps for Office, Esri Story Map apps, Briefing Books, and ArcGIS Explorer Desktop can be used to find and visualize geospatial information and produce map-based presentations for leadership. Esri technology is used to create web applications (web apps) by providing application program interfaces (APIs) for web technologies including JavaScript. If a robust client application is needed, developers can use ArcGIS Runtime SDKs to create applications customized to do what users require, such as gather information in the field in a connected or a disconnected environment. All these distribution methods can be accessed by smartphones, tablets, and other handheld devices running on Linux, Android, iOS, or Windows Mobile.

Conclusion

This technical paper describes two approaches to resolve the critical issue of cybersecurity: a geospatial model for perimeter defense and a CSL-based mission-impact assessment. The advantage of the CSL model is that it can organize and manage mission-assurance activities by identifying all devices that support data paths deemed critical by an organization. Much of the ongoing work in cybersecurity is excellent but widely dispersed in location and purpose. The CSL model creates a solution to integrate that work, align it with other security disciplines, and focus both based on the priority dataflows established by the organization. Any framework that can successfully accomplish this feat must have a strong geospatial foundation.

A powerful GIS platform, such as ArcGIS, includes tools, workflows, and applications that can be implemented with an organization's existing cybersecurity data and technologies to improve the following:

- Data management
- Analysis and fusion
- Visualization for situational awareness
- Information sharing

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