

BIOGRAPHICAL INFORMATION

Christopher Tucker
President/CEO
IONIC Enterprise

Specific Responsibilities

Dr. Christopher Tucker is President/CEO of IONIC Enterprise, the world leader in interoperable web mapping, location based services, and online geoservices. Beyond providing overall executive direction for IONIC Enterprise, Tucker also provides architectural consultation and expertise for clients in C4ISR, Earth Observation, Homeland Security, e-Government, Transportation, Location Based Services, and other vertical sectors. Tucker is actively involved in the Open GIS Consortium, and related activities.

Past Experience

Dr. Tucker was a founder and Chief Strategic Officer of In-Q-Tel, the CIA's non-profit venture capital fund, focusing his efforts on developing In-Q-Tel's overall strategy for tackling the Agency's priority IT problems. As such, Tucker was responsible for managing a portfolio of technical projects, issues of organizational design, and relations with the intelligence community, industry and media.

Prior to this, Tucker served as Special Advisor to the Executive Vice Provost of Columbia University and was responsible for a range of issues having to do with strategic institutional development, research portfolio management, federal science and technology policy, and the organization of interdisciplinary research.

Tucker is a proud *ex officio* member of the Board of Directors of the Open GIS Consortium, an international industry consortium of over 210 companies, government agencies and universities dedicated to developing interoperability standards that "geo-enable" the Web and mainstream information technology (IT).

Educational Information

B.S., Columbia College, Political Economy
M.A., Columbia University, Graduate School of Arts and Sciences, Political Science
M.Phil, Columbia University, Graduate School of Arts and Sciences, Political Science
Ph.D., Columbia University, Graduate School of Arts and Sciences, Political Science

Professional Memberships

GITA
Open GIS Consortium

OPENGIS ® INTEROPERABILITY: A REQUIREMENT FOR CRITICAL
INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

Christopher Tucker
IONIC Enterprise
PO Box 2635
Alexandria, VA 22301

ABSTRACT

Critical infrastructure protection inherently requires a spatial data infrastructure that is interoperable, distributed, secure, and enterprise-class. OpenGIS ® interoperability specifications play a central role in the future of homeland security, since they fundamentally enable dynamic, secure access to real-time spatial data from state and local governments, critical infrastructure partners, and a range of federal authorities. This is particularly important since homeland security requires simultaneous access to commercial proprietary data, personal privacy data, official government data, and publicly available data, for the generation of spatially-enabled situational awareness for policy-makers and first-responders. This presentation offers a practical overview of the value of OpenGIS interoperability, and discusses its use in the development of flexible, multi-tiered, scalable homeland security solutions. It will discuss the current state of GIS in the homeland security community (e.g., spatial data is maintained in multiple environments, applications must be built against proprietary APIs, intimate knowledge of the underlying computational environments is required, combinatorial development problems occur) where system stovepipes have become a way of life, data has been replicated continuously, and spatial data quality/integrity has been undermined. And, the presentation will offer tips on migrating legacy systems to an OpenGIS future.

INTRODUCTION

The terrible catastrophe of September 11th immediately highlighted the importance of spatial data and services in disaster *recovery* operations. It did not take long for policy-makers to understand that spatial data and services are critical not only for recovery, but for the entire process of homeland security. Detection, prevention, planning, response and recovery activities are all premised upon the potential for disasters to occur in locations that we have no ability to pre-determine. Disasters almost by definition occur unexpectedly, in places where we are not adequately prepared. As such, most every policy-maker and emergency response leader now believes that spatially-enabled, real-time, comprehensive situational awareness is necessary throughout this process if we are to prevent another September 11th.

Homeland security inherently requires a national spatial data infrastructure that is interoperable, distributed, secure, and enterprise-class. And, a national spatial data infrastructure is nothing if not for dynamic, secure access to spatial data from state and local governments, critical infrastructure partners, and a range of federal authorities.

NYC, SEPTEMBER 11th, AND THE COST OF NO INTEROPERABILITY

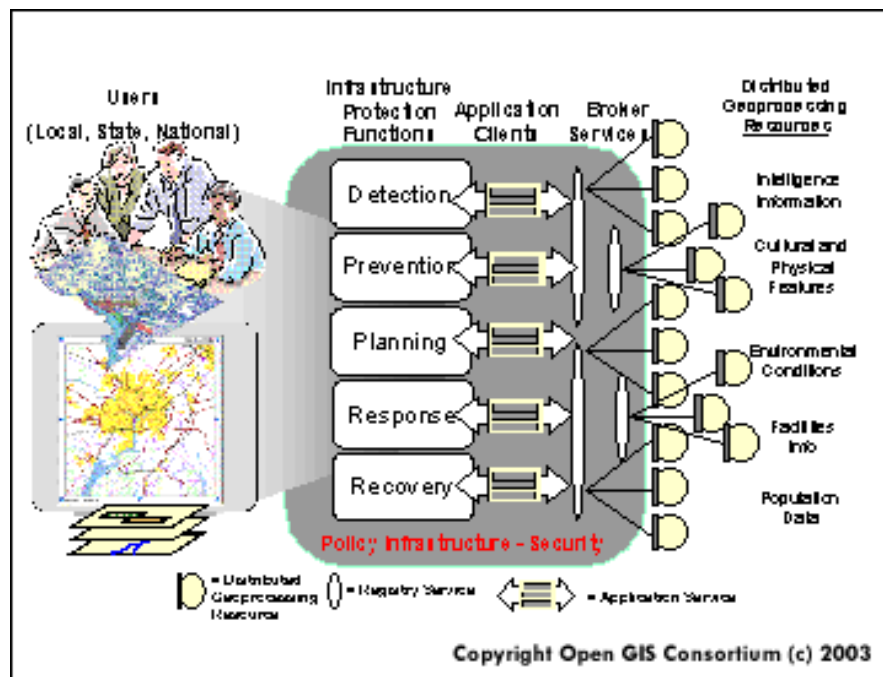
September 11th presented a sudden crisis generating hundreds of requests for immediate support. To face it, the City of New York used the Emergency Management Data Committee (EMDC) and created a crisis center within 24 hours of the disaster. There were 20 GIS workstations, 6 plotters, 50 GIS operators working 24x7, 6 coordinated GIS units including the Office for Emergency Management, the Fire Department of New York (FDNY), the Federal Emergency Management Agency (FEMA) and the Department of Defense (DOD). There were 2600 specific requests to assist operation and decision making by teams in the field: 313 requests from the Police Department, 266 requests from the Emergency Office, 121 requests from the US Army and Lifeguards Units, 106 requests from FEMA, 90 requests from the New York Port Authority, 69 requests from the Coast Guard, 58 requests from the Fire Department, and more.

With the NY/NJ Port Authority, the City of New York, and Con Edison all using different vendor platforms, the exchange of data was a challenge. There was no utilization of OpenGIS web services, and because of this, there was no immediate, comprehensive view of the disaster area during the immediate aftermath. In a single day, the crisis center was set up and running, however data access, exchange and dissemination were a challenge.

THE HOMELAND SECURITY PROCESS AND INTEROPERABILITY

Homeland security threats uniquely forge partnerships and data sharing arrangements among federal, state and local governments and between these public authorities and private critical infrastructure partners such as utilities, telecommunications, financial and transportation firms. Yet, even the willingness to share data does not remove the

technological barriers to dynamically and effectively utilizing distributed spatial data sources for homeland security efforts.



Robust homeland security fundamentally requires interoperability. With different kinds of government and private enterprises depending on different vendor platforms, interoperability is the only way to ensure dynamic access to distributed sources of spatial data. As seen in NYC, any particular emergency scenario can easily engulf dozens of overlapping jurisdictions, enterprises and infrastructures.

Homeland security requires the dynamic integration of spatial data from all of these groups. This integrated view provides enhanced situational awareness and visibility into the events that must be managed. It is important to recognize that this integrated view will be different depending on the role and location of the user, as well on the stage of the homeland security process (e.g., detection, prevention, planning, response and recovery). The notion that a single archive of data will be able to provide sufficient visibility into the evolving complexity of a homeland security event is incredible.

Detection

Some threats and events are obvious, and easy to detect. Others are non-obvious, and require relationship or pattern detection technologies to aid in detection activities. The spatial visualization of real-time event data is one such technology. If an operation center were able to monitor multiple specialized views of real-time event data from a spatial perspective, it would be able to detect non-obvious patterns of emerging threats.

Prevention

The prevention of homeland security threats requires a comprehensive understanding of potential exposures, and a committed mitigation program. Such a threat prevention and exposure mitigation program would require bringing together disparate spatial data sources that provide total visibility. This program would also require real-time visualization of threat and event information that is co-located with known exposures.

Planning

Effective planning for enhanced homeland security requires the analysis of consequences of potential events. Whether it is notional plume analysis, analysis of an hypothetical event's impact on evacuation routes, or the determination of potential captive populations – homeland security authorities require the ability to undertake such scenario thinking based upon actual live feature data that is accessed across a jurisdiction.

Response

In order to effectively respond to a homeland security event, authorities must all be able to access a common operational picture generated from a distributed array of authoritative spatial data sources. This common operational picture must also be portrayed differently based upon a users role and security clearances. And, there must be some means for alerting response resources, providing them situational awareness data that is spatial in nature. Moreover, there must be the flexibility for first responders to ask complex spatial questions from the field, while also providing updates from the field.

Recovery

As we have seen, recovery can be a long process that involves aspects of planning and response, melded with a unique set of logistics challenges. What resources are where? Where *were* things located? What critical systems or infrastructure are still at risk at this location? Many questions must be asked as recovery efforts are undertaken. And, authorities engaged in recovery efforts must demonstrate continued vigilance in its detection, prevention, and planning efforts.

OpenGIS WEB SERVICES AND AUTHORITATIVE DATA STEWARDS

Robust homeland security requires ***authoritative data stewards***, who can best maintain the currency and accuracy of a data source, to serve spatial data into a common environment for use by emergency responders, planners, and more. To achieve this, it is critical that these data stewards publish their data as web services that adhere to OpenGIS interoperability specifications.

Open GIS Consortium (OGC) web services (www.opengis.org), as adopted and implemented by the OGC's 250+ members, provide enterprises an opportunity to expose their legacies through standard interfaces so that many new applications can take advantage of legacies, through standard interfaces. Just as



http: and html/xml comprise the dial-tone of the internet, OpenGIS web services and encodings provide us with the dial-tone of the spatial internet.

Beyond offering a standard interface for accessing data, OpenGIS conformant web services can be **published** so that all of the appropriate users can dynamically **find** these resources and **bind** them into their applications. The power of this “publish, find, bind” model is enormous for homeland security applications, enabling new data sources to be discovered and brought into application on the fly.

Since the highest fidelity (and most timely) spatial data is often maintained at a local level, it is critical that states, localities and enterprises publish their spatial data as OpenGIS web services for secure use by authorities during homeland security exercises. Much of this data is wrapped in issues of personal privacy or commercial confidentiality. The Open GIS Consortium and its many sponsors have worked to ensure that their web services standards enable enterprises to collaborate in such a secure manner. Indeed, the OGC has repeatedly demonstrated that such a distributed infrastructure can be deployed within even the most stringent of security paradigms, such as the Department of Defense (DoD) PKI security regime.

The Open GIS Consortium has enabled the vendor community to collectively achieve interoperability for the GIS customer base, and has helped decision-makers in the U.S. homeland security community realize a vision of collaboration. Steve Cooper, the CIO of the Department of Homeland Security has repeatedly called for solutions that support standards and interoperability, and sees geo-spatial information as one of his top three priorities. The U.S. government’s support of the Critical Infrastructure Protection Initiative is a clear sign of their interest in and commitment to OpenGIS approaches to spatially-enabling homeland security.

REAL-TIME SPATIAL ENABLEMENT WITH OpenGIS WEB SERVICES

GIS has historically been an off-line discipline. But, of course, GIS data has historically been relatively static, and used for cartography, engineering and the like. As a result, many GIS vendors found it difficult to transition to the world of publishing of real-time business data through spatial web services. OpenGIS web services uniquely enable enterprises to publish their underlying spatial data along with their real-time business data. As spatially referenced data objects are committed to, for instance, Oracle Spatial from an operational system, OpenGIS interfaces can enable access to this data through its web mapping products. OpenGIS web services interfaces also can enable on-the-fly access to multiple business ‘objects’ (e.g., CRM, location servers, asset databases, etc.) over enterprise messaging infrastructures that can be dynamically utilized in web mapping applications.

Critical infrastructure partners such as railroads, utilities, pipelines, (air) ports, telecommunications companies, and the like are now beginning to recognize their role as a geo-spatial data provider within the US homeland security context. And, since they are

accustomed to dealing with constantly changing data, these critical infrastructure partners have expressed concern about transferring static extractions of their data that will quickly be out of date. Also, these extractions sever any relationship between the geo-spatial data and the business data (or systems) that are linked to them.

And, critical infrastructure partners only continue to cultivate better real-time views into their own business/infrastructure that can be shared with homeland security officials, first responders, and policy makers. SCADA systems and asset position gateways are two extremely prominent examples of this. SCADA systems offer real-time status of a network that can offer decision-makers and first responders critical information. Position gateways can offer a real-time position of an organization's assets, response resources, or personnel. Both are an example of business systems that offer spatial databases that can easily be exposed as OpenGIS web services, just like any other spatial data source.

A robust homeland security/defense infrastructure clearly requires geo-spatial access to such real-time information, atop all of the other geo-spatial resources available to an organization. By incorporating real-time spatial information, homeland security authorities can go beyond simply geo-graphically orienting themselves as to what has happened. They can now visualize and process what is happening in near-real-time, with comprehensive situational awareness.

DESIGN STRATEGIES FOR SPATIALLY-ENABLED HOMELAND SECURITY

Design strategies differ at different levels in the homeland security "food-chain". It is useful to differentiate between 'base nodes' that can provide spatial data into a larger environment, and 'core nodes' that must be able to access n- distributed base nodes.

Many local governments fall into the category of 'base node'. These organizations manage their spatial data centrally, and could easily upgrade their web-mapping products to take advantage of the OpenGIS interfaces supported by their vendors. Some larger local governments do not manage their spatial data centrally, and need to have some sort of 'core node' within their overall enterprise in order to dynamically bring these distributed services together.

A 'core node' requires the ability to 'cascade' (in the case of WMS resources), or to access multiple distributed WFS resources via a remote API. A core node also requires some method for knowing enough information about the relevant base nodes so that their data can be accessed. The OpenGIS Web Registry Service (WRS) specification enables owners of OpenGIS conformant web services to publish their existence (with ISO19115 & 9 metadata), so that others might find these resources and bind their applications to them. In order for core node applications to have complete and dynamic visibility into a situation, they should be able to access such a WRS. Hosting such a WRS is an ideal design strategy for a core node.

A core node system owner needs to figure out how (s)he will take advantage of all of these OpenGIS conformant sources, and broker them. How will a variety of applications

take advantage of a variety of spatial resources? In order to accomplish this, you will need to find vendors with appropriate middleware products that offer the brokering capabilities, data enhancement facilities, and portrayal services necessary for effectively bridging this divide.

TAKING ADVANTAGE OF THE DATA EXCHANGE INHERENT IN OpenGIS WEB SERVICES

By merely exposing underlying spatial resources as OpenGIS web services, a system architect can, for the first time in history, potentially solve the combinatorial integration problem posed by the mixing and matching of many different spatial applications against many legacy spatial resources. And, this new ability fundamentally launches you into a world where there is:

- No off-line data conversion required
- No redundancy or duplication of geospatial data needed
- No conflict between multiple GIS servers from multiple vendors
- Easily developed cross-department/organization applications
- Native Web access to your spatial resources
- E-business enabled, and secure access to your spatial resources
- A higher level of data integrity, with the same information available for everyone

All while reducing development risk, saving development time, reducing the total cost of system ownership, and providing total visibility into distributed spatial data resources. Through OpenGIS conformance, system architects (and their bosses!) can achieve business goals that have previously been the stuff of strategic plans. No longer is interoperable, distributed geo-processing a vision of the future. It is **the** vision driving the world that we are currently implementing.

Homeland security architects face a daunting challenge when it comes to realizing secure, distributed spatial data exchange. The concept of a single vendor solution is tempting. But this concept is a chimera. Overcoming the challenges inherent in our heterogeneous national spatial data infrastructure can only be achieved by interoperability.