Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Visual Analytics in Public Safety

Example Capabilities for Example Government Agencies

Curtis Garton

William Wright

Oculus INFO INC.

Prepared By:
Oculus Onfo Inc.
2 Berkley St., suite 600
Toronto, ON
M5A 4J5

Scientific Authority: Dr. Andrew Vallerand, Director S&T Public Security, 613-944-8187

Defence R&D Canada – CSS

Contract Report
DRDC CSS CR 2011-25
October 2011

Canada

Visual Analytics in Public Safety

Example Capabilities for Example Government Agencies

Curtis Garton

William Wright

Oculus INFO INC.

Prepared By:
Oculus Onfo Inc.
2 Berkley St., suite 600
Toronto, ON
M5A 4J5

Scientific Authority: Dr. Andrew Vallerand, Director S&T Public Security, 613-944-8187

Defence R&D Canada – CSS

Contract Report
DRDC CSS CR 2011-25
October 2011

Principal Author

Original signed by Curtis Garton

Curtis Garton

Oculus INFO INC.

Approved by

Original signed by Dr. Andrew Vallerand

Dr. Andrew Vallerand

DRDC CSS Director S&T Public Security

Approved for release by

Original signed by Dr. Mark Williamson

Dr. Mark Williamson

DRDC CSS DG - DRP Chair

Abstract

This is a short report discussing how Visual Analytics at large can improve capabilities at Canadian Departments and Agencies, such as Candian Security Intelligence Services (CSIS), Royal Canadian Mounted Police (RCMP), Public Safety Canada (PSC) and the Canada Border Services Agency (CBSA). The report begins with a brief summary of Visual Analytics. Several indicative visual analytic tools are then presented. These "case study" tools illustrate visual analytic technologies that are at a high Technology Readiness Level (TRL). There follows a description of potential visual analytics opportunities for several representative federal organizations. The report concludes with several recommendations on how the federal government may facilitate the adaptation and exploitation of Visual Analytic tools.

Résumé

Ceci est un bref rapport dans lequel nous démontrons comment l'analytique visuel peut améliorer les capacités des ministères et organismes gouvernementaux canadiens comme le SCRC, la GRC, Sécurité publique Canada et l'ASFC. D'abord, nous donnons une description brève de l'analytique visuel. Nous présentons ensuite divers outils illustrant bien ce qu'est l'analytique visuel et qui en sont à un stade de développement technologique avancé. Nous explorons ensuite diverses solutions potentielles pour divers organismes fédéraux types. Le rapport se termine par des recommandations quant aux façons dont le gouvernement fédéral pourrait s'y prendre pour faciliter l'adaptation et l'exploitation d'un outil d'analytique visuel.

This page intentionally left blank.

Executive summary

Visual Analytics in Public Safety: Example Capabilities for Example Government Agencies

Curtis Garton; William Wright; DRDC CSS CR 2011-25; Defence R&D Canada – CSS; October 2011.

This is a short report discussing how Visual Analytics can improve capabilities at Canadian Departments and Agencies, such as Candian Security Intelligence Services, Royal Canadian Mounted Police, Public Safety Canada and the Canada Border Services Agency. The report begins with a brief summary of Visual Analytics. In the last few years a new field called visual analytics has emerged, combining and extending information visualization and computational analytics. Visual analytics support analytical reasoning facilitated by interactive visual interfaces and integration with computational analytics. Indeed, a wide variety of technologies are brought together in visual analytics applications. Several indicative visual analytic tools are then presented. This paper describes six leading visual analytic products. These are examples of innovative capabilities that are representative of the nature of visual analytic functions and benefits. This is by no means an exhaustive list. These "case study" tools illustrate visual analytic technologies that are at a high Technology Readiness Level (TRL). There follows a description of potential visual analytics opportunities for several representative federal organizations. The report concludes with several recommendations on how the federal government may facilitate the adaptation and exploitation of Visual Analytic tool

Sommaire

Visual Analytics in Public Safety: Example Capabilities for Example Government Agencies

Curtis Garton; William Wright; DRDC CSS CR 2011-25; R & D pour la défense Canada – CSS; juillet 2011.

Ceci est un bref rapport dans lequel nous démontrons comment l'analytique visuel peut améliorer les capacités des ministères et organismes gouvernementaux canadiens comme le Service canadien du renseignement de sécurité, la Gendarmerie royale du Canada, Sécurité publique Canada et l'Agence des services frontaliers du Canada. D'abord, nous donnons une description brève de l'analytique visuel. Au cours des dernières années, nous avons été témoins de l'émergence d'un nouveau domaine de spécialité appelé « analytique visuel », lequel combine et approfondit les domaines de la visualisation de données et de l'analytique computationnel. L'analytique visuel contribue au raisonnement analytique grâce à des interfaces visuelles interactives et en se combinant à l'analytique computationnel. En effet, les applications d'analytique visuel font appel à une grande variété de technologies. Nous présentons ensuite six outils innovateurs représentant bien les fonctions et les avantages qu'offre l'analytique visuel. Il ne s'agit pas d'une liste exhaustive, mais de certains outils qui en sont à un stade de développement technologique avancé. Nous explorons ensuite diverses solutions potentielles pour divers organismes fédéraux types. Le rapport se termine par des recommandations quant aux façons dont le gouvernement fédéral pourrait s'y prendre pour faciliter l'adaptation et l'exploitation d'un outil d'analytique visuel.

Table of contents

List of figures

List of tables

This page intentionally left blank.

1 Introduction

This is a short report discussing how Visual Analytics at large can improve capabilities at Canadian law enforcement agencies, such as CSIS, RCMP, Public Safety Canada and the CBSA. The report begins with a brief summary of Visual Analytics. Several indicative visual analytic tools are then presented. These "case study" tools illustrate visual analytic technologies that are at a high *Technology Readiness Level* (TRL) [17]. There follows a description of potential visual analytics opportunities for several representative federal organizations. The report concludes with several recommendations on how the federal government may facilitate the adaptation and exploitation of Visual Analytic tools.

2 About Visual Analytics

In the last few years a new field called visual analytics has emerged, combining and extending information visualization and computational analytics. Visual analytics support analytical reasoning facilitated by interactive visual interfaces and integration with computational analytics. As shown in Figure 1, a wide variety of technologies are brought together in visual analytics applications.

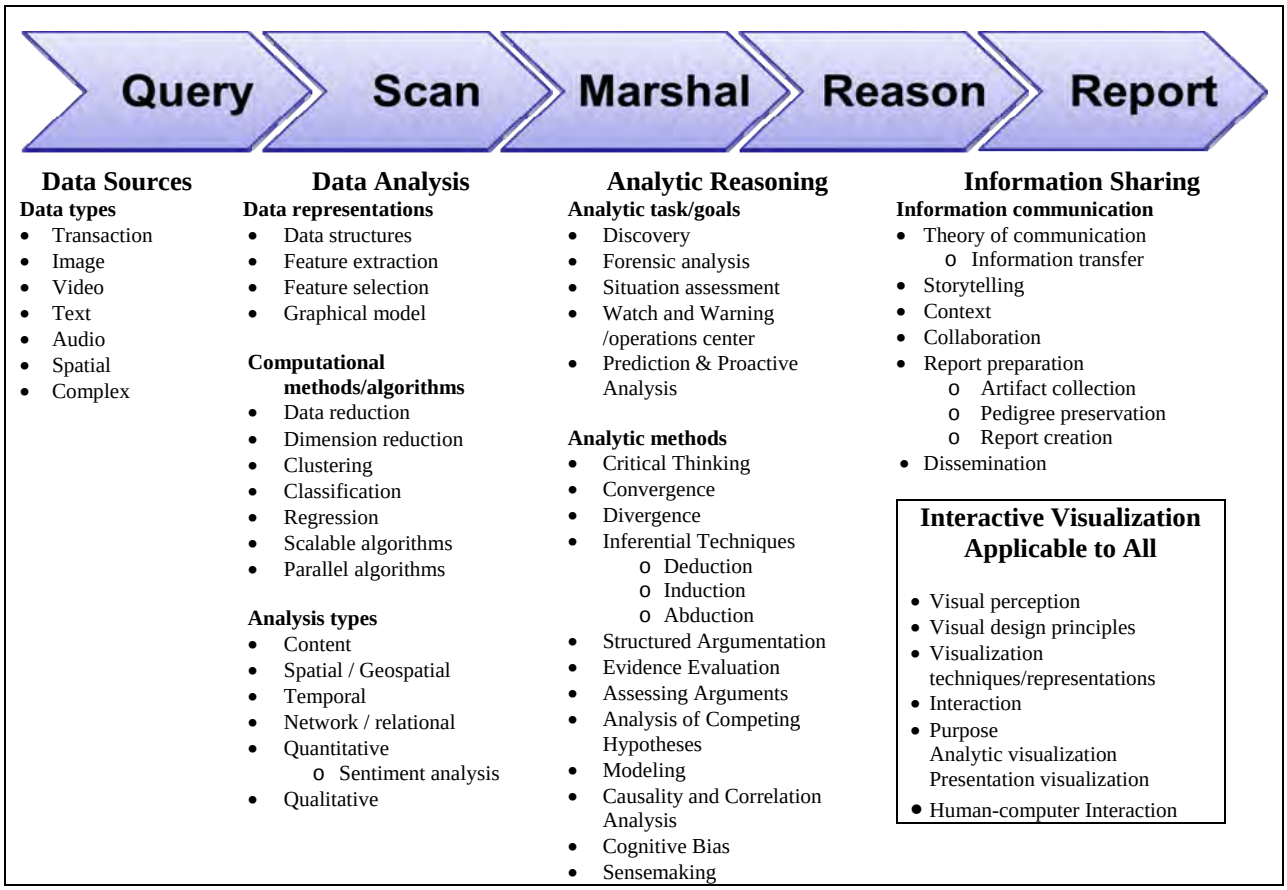


Figure 1 Visual Analytics Capabilities in the Analytic Workflow [Cook, 2010

Visual analytics is a multidisciplinary field with many contributing capabilities. People, data and analytics work together in a visual system of systems to harness the respective strengths of each component. People use visual analytics tools and techniques to synthesize information and derive insight from massive, dynamic, ambiguous, and often conflicting data; to detect the expected and discover the unexpected; to provide timely, defensible, and understandable assessments; and communicate assessments effectively for action [Thomas, 2005]. Visualization and visual analytics produce superior information and knowledge products to support human decision-making. William Wright at Oculus is a leading researcher and practitioner in visual analytics and was a contributing author to Jim Thomas' research agenda for visual analytics.

3 Example Visual Analytic Capabilities

The following describes six leading visual analytic products. These are examples of innovative capabilities that are representative of the nature of visual analytic functions and benefits. This is by no means an exhaustive list. Please note the first two examples are from Oculus, the same organization as the authors of this short report.

3.1 Geo-Temporal Analysis - GeoTime

GeoTime ® is a visual analytics tool used for communication analysis and financial transaction analysis, as well as for tracking high value individuals, criminal organizations, smuggling vehicles and boats. It is also used for geo-temporal trend analysis. GeoTime improves the perception of entity movements, events, relationships, and interactions over time within a geospatial context. For space-time analysis of events and behaviors, it has been shown to double analytic performance. As illustrated in Figure 2, events and tracks are represented within an X,Y,T coordinate space, in which the X,Y plane shows geographic or diagrammatic space and the vertical T axis represents time. Events animate in time vertically through the 3-D space as the window of time being viewed changes.

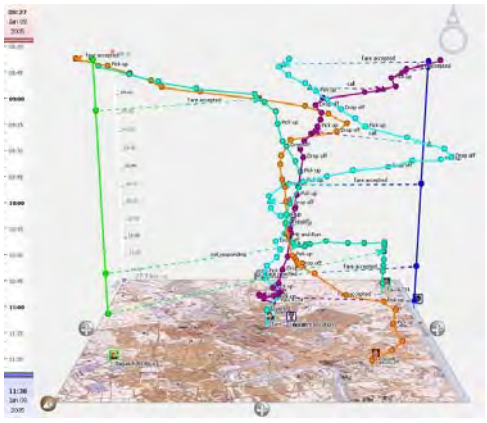


Figure 2 GeoTime visualization for analysis of events, communications and transactions in time and space Time is in the vertical dimension. Behaviors in time-space are visible

.

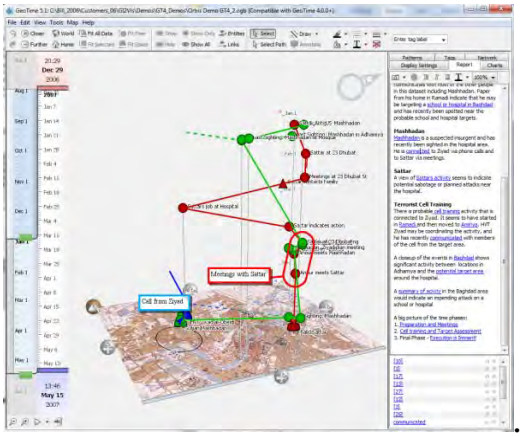


Figure 3 Time space visualization of two HVI entities in Baghdad. A meeting is highlighted. The "stories" panel on the right captures analysts' thinking, hypotheses and evidence using "analytic state".

The GeoTime display makes behavior visible. Activity, speed, coordinated movements, transactions among entities, regular and irregular patterns are all quickly discernable. For analysts, GeoTime's combined temporal-spatial three-dimensional space amplifies the concurrent cognition of entity relationships and behaviors [Kapler, 2004] [6] [14]. Analysts can see the who and what, in the where and when. GeoTime is an interactive analysis tool with link chaining to

assess connectivity, indirect and direct link analysis, automatic pattern detection, zoom by interest controls, a variety of filtering (e.g. by entity, by charted properties) and an ability to save and recall previous analytic "states".

With the GeoTime *"Stories"* capabilities [Eccles, 2007], rather than working with raw or atomic data, the analyst is able to work and think in terms of higher order behaviors, events and threats leading to improved comprehension, discovery, hypothesis generation and communication. A common problem for analysts is that they must wade through large volumes of low-level data and painstakingly extract behaviors and patterns in order to understand a situation. To address this, the stories system provides functions for automatic detection of patterns in movement activity, including discovery of possible meetings, speed of movement, percentage of time spent at unique locations, and identifying gaps in observations. The results of these functions are then fed into the annotation system that uses a graphic vocabulary. Extensive user-generated, in-scene annotations are also provided to support the analyst's narrative. This allows the analyst to work at a higher level of abstraction, thereby stimulating faster recognition and monitoring of larger behaviors or threats. The story window, as shown in Figure 3, is the focus of story-authoring functionality in GeoTime. It enables the analyst to review pattern search results, author and present stories about events in time and space, capture moments of insight, and collaborate with other analysts.

For complex "when, what and where" questions, in which people need an overall understanding of the spatiotemporal situation, a recent between-subjects experiment with 30 participants showed that 3D space time displays had on average *twice as fast* response times with no difference in error rates compared to the 2D baseline [Kristensson, 2009]. The participants reported that the 3D space time display was intuitive, engaging and easy to understand. It is concluded that this "dramatic reduction in response times" is evidence there is significant benefit provided for observing and comprehending nontrivial spatio-temporal patterns.

GeoTime is TRL 9 (actual system 'flight proven' through successful mission operations). GeoTime is a unique, patented COTS product. Many U.S. federal agencies use GeoTime. Some state and local organizations are now taking advantage of GeoTime and that user base is also growing.

3.2 Open Source Analytics - nSpace2

nSpace is comprised of two visual analytics systems: TRIST (The Rapid Information Scanning Tool) and the Sandbox. It combines the multi-dimensional linked views found in TRIST with the visible, cognitive mechanisms of the Sandbox (Figure 4.). nSpace TRIST ® provides query planning, rapid scanning over thousands of search results in one display, and includes multiple linked dimensions for result characterization and correlation. Change difference visualization allows the efficient comparison of different sources and the monitoring of issues from day-to-day. Analysts work with TRIST to triage their massive data and to extract information into the Sandbox evidence marshaling environment [Jonker, 2005]. The nSpace Sandbox ® is a flexible and expressive thinking environment that supports both ad-hoc and formal analytical sense-

making [Wright, 2006]. Key capabilities for the Sandbox include “put-this-there” cognition, animated automatic layout of evidence with analytical templates, gestures for the fluid expression of thought, assertions with supporting/refuting evidence gates, analytic methodologies such as analysis of competing hypotheses (ACH) and scalability mechanisms to support larger analysis tasks.

The critical factor is that nSpace is an integration platform that also marshals tools and data sources for analysts. Using open web services interfaces and protocols, nSpace integrates computational resources such as reasoning services, agent-based modeling and advanced computational linguistic functions including entity extraction, supervised and unsupervised clustering, and automatic ontology construction. nSpace spans multiple data sources using a variety of Service Oriented Architecture (SOA) integration mechanisms such as OpenSearch (RSS / Atom), REST and SOAP Web Services and native JDBC connectivity. Configuration settings allow multiple computational resources in different organizational contexts to be combined in a unified analysis environment. *This combination of easy-to-use, advanced visualization, computational services and integration is what marks the best of Visual Analytics solutions [Proulx, 2007] [Chien, 2008].*

Manage Projects | Triage Multiple Sources | Analytical Sense-making and Reporting

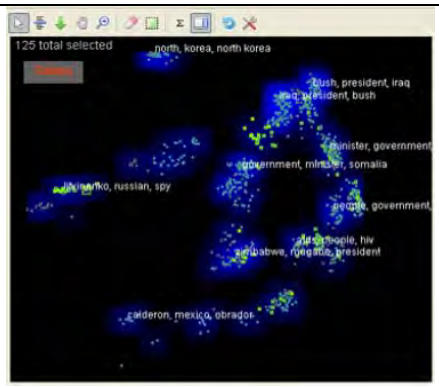
Figure 4 nSpace2 provides triage and sense-making. It is web-based with a SOA.

nSpace 2 is TRL 8 (actual system completed and 'flight qualified' through test and demonstration). It is in two pilot projects in the U.S. with federal agencies, and a third pilot project is expected shortly.

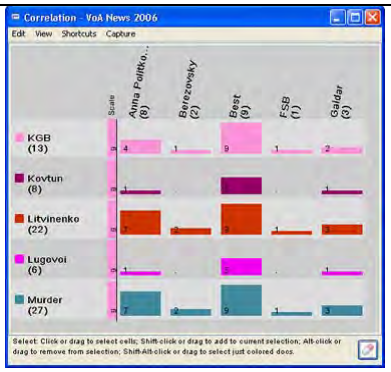
3.3 Text Analytics - IN-SPIRE

As described on the IN-SPIRE website [8], this tool quickly and automatically conveys the essence of large sets of unformatted text documents, such as technical reports, web data, newswire feeds and intelligence message traffic. It can handle near real-time data by adding new documents as they arrive. It also processes foreign language data and provides robust support for translation. By clustering similar documents together, this visual analytics tool unveils common

themes and reveals hidden relationships within the document set. IN-SPIRE allows analysts to spend more time exploring the information they find most relevant and less time sifting through the masses of irrelevant documents.



Galaxy View



Correlation View

Figure 5 IN-SPIRE Visualizations

.

Computational linguistics clustering methods analyze large numbers of text files and determine key topics or themes in each. IN-SPIRE's includes a number of visualizations, examples of which are shown in Figure 5. The two main visualizations display representations of the documents in which those with similar or related topics appear closer together. The Galaxy visualization uses the metaphor of the stars in the night sky with each star representing an individual document. The ThemeView visualization uses a 3-dimensional terrain map display to provide a high-level overview of the data. Other tools, such as the Correlation Viewer, help to explore trends over time and relationships between concepts.

IN-SPIRE is TRL 9 (actual system 'flight proven' through successful mission operations). It is in use in several federal and state agencies in the U.S.

3.4 Video Analytics – Indigo Vision

Video content analysis is a new technology with applications for Federal Police, Border Security and Port Security for instance. The technology has moved beyond recognizing license plate numbers, but there are challenges with being able to reliable extract and analyze behaviors. For video analytics, there is both a monitoring and a forensics use case. Each requires extraction of events and entities, tracking of entities, and alerts or content search based on extracted objects/events/entities/behaviors.

Indigo Vision is a UK company that provides video security systems including associated video analytics that appears to be mostly oriented for real-time monitoring applications. As described on the Indigo Vision website, patterns in video feeds can be recognized to provide alerts on such things as congestion detection (e.g. queues in public spaces), motion detection (e.g. through

unauthorized exits), abandoned object detection, virtual tripwires, shaped-based detection (e.g. trucks and buses), theft detection (e.g. missing objects) and camera faults (e.g. camera deliberately covered by a bag) as shown in Figure 6. Northrop Grumman's AlertVideo is another product. It tracks people, vehicles and other objects for law enforcement. Tracking inmates and guards in correctional facilities, AlertVideo also can alert when more than one inmate (settable number) enters a cell, or if a guard has not exited a cell within a designated time period when an inmate has been detected entering a cell. During surveillance operations, AlertVideo easily monitors the area and alerts the watch to designated movement such as vehicles or people entering or exiting an area, abandoned objects or drops, stopped or loitering activities, and many more.

Detection Shape

Detection Theft

Detection Camera Fault

Figure 6 Indigo-Vision Video Analytics.

Video analytics for forensics applications combines speech recognition, image understanding (e.g. scene characterization, scene segmentation, similarity matching, face detection, object tracking) and video OCR (for recognizing text in the scene). Large amounts of video are processed to produce meta-data tagged searchable archives. Because of the difficulties and errors involved, an analyst user interface is required as part of the processing of the video.

Some current research issues in video analytics include:

- Improved pattern recognition of complex behaviors
- Joining WAMI (wide area motion imagery) entity “track-lets” into longer tracks
- User interfaces for video analysis that optimize cognition
- Tools for exploring video collections
- Applications that categorize videos based on content
- Annotation schema for video analysis
- Automated and/or social methods of annotating videos for improved retrieval
- Image, speech, sound track, and text processing that supports analysis of large video collections
- Methodologies for determining originator, message, and audience impacts of video

Indigo Vision appears to be TRL 9 (actual system 'flight proven' through successful mission operations). IndigoVision apparently has extensive reference sites including seven rail networks,

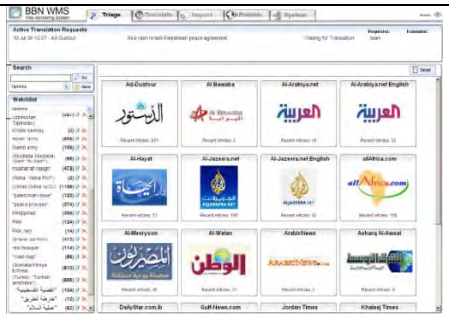
two of the world's top five banks, 28 airports, 27 casinos and two Olympic Games. However, the authors have no direct experience with this product.

3.5 Broadcast and Web Monitoring - BBN

Broadcast monitoring is another application of video analytics. The BBN monitoring systems are an example. As described on the BBN website, the BBN Broadcast Monitoring System creates a continuous, searchable, one-year archive of international television broadcasts. The real-time audio stream is automatically transcribed and translated into English with technology from Language Weaver. Both the transcript and translation are searchable and synchronized to the video, providing powerful capabilities for effective retrieval and precise playback of the video based on its speech content. However, image processing is not used to identify video content features.

The BBN Web Monitoring System is a similar capability but applied to websites and blogs. It is an end-to-end capability for collecting, organizing, and translating open source content from the World Wide Web. The system integrates and manages the workflow of the media analysis process from beginning to end— from data collection and processing, to automated triage and retrieval, to machine-assisted translation and support for human translation, to publication and dissemination. The system's automatic analysis of Web site content supports effective content-based retrieval and triage for human analysts who must deal with overwhelming volumes of continuously accumulating media.

Broadcast Monitoring



Web Monitoring

Figure 7 BBN Monitoring Tools

Current broadcast and web monitoring systems employ web harvesting, data management and computational linguistics technologies. There is an opportunity to enrich these capabilities with additional visualization functions such as those used in nSpace2.

BBN Monitoring apparently is TRL 9 (actual system 'flight proven' through successful mission operations). It is in use in several U.S. COCOMs and with at least one U.S. agency.

3.6 Social Network Analysis – ORA from CMU (Carnegie Mellon University)

As described in the ORA user manual, ORA is an analysis tool designed to help evaluate one or more networks. It can be used to assess the nature of, features of, change in, and determinants of complex networks. ORA computes a wide variety of network metrics or measures. A large variety of networks can be assessed including, but not limited to, social networks, activity networks, task networks, knowledge networks, supply chains, and communication networks. Using ORA questions such as the following can be addressed: what is critical, are there groups of interest, are there patterns of interest, how might interventions impact the network, who is critical, are there emerging groups, how is the network changing.

ORA can assess any type of network. Anything that can be represented as a set of nodes and relations can be assessed. Typical networks are: social networks (who interacts with whom), financial networks (who lends money to whom); Gantt charts (what task needs to be done before what), supply chains (what resources are needed to build what other resources), semantic networks (what ideas are linked to what ideas), proximity networks (what states border on what states), etc. ORA can assess any data that can be represented as nodes and relations regardless of what the nodes are or what the relations are.

ORA can be used to assess change in networks over time. Over time the shape or topology of a network might change; e.g. startup companies move from a collaborative to a hierarchical structure, terrorists change what weapons they use to attack sites, scholars cite different papers, and so on. Consequently over time, who or what is critical in a network might change. ORA can assess change in networks, and forecast possible ways in which the network might change in the future.

ORA apparently is TRL 9 (actual system 'flight proven' through successful mission operations). It is in use in several U.S. COCOMs and with at least one U.S. agency. The authors have no direct experience with ORA.

4 Example Opportunities for Visual Analytics to Assist Federal Agencies

We have identified a number of opportunities within several federal agencies for the use and exploitation of visual analytics tools and technologies. They span public safety, defence, intelligence, as well as policy and decision makers. These tools and technologies provide insight, situational awareness and increased efficiency in the analysis, reporting and comprehension of complex data sets. This list of five example opportunities is not an exhaustive list by any means but is meant as a starting point to further the understanding and adoption of visual analytic tools and technologies by the Federal Government. A more comprehensive follow-on study could extend and elaborate these few examples.

The following list describes current challenges faced within a specific agency and an initiative that could benefit from the adoption and use of visual analytic tools and technologies. A brief description of the current challenges is provided, followed by a list of recommended tools and techniques. Some of the opportunities listed also contain workflow scenario descriptions that describe the process in which these tools would be used.

4.1 MSOC: Great Lakes Maritime Domain Awareness

A number of federal agencies are responsible for maritime security on the Great Lakes, including the RCMP, DFO, CBSA, CCG, DND and Transport Canada. The monitoring and response to maritime events presents challenges in both the collection and analysis of vessel movement over time due to the large volumes of real time geo-temporal data being captured. Computational analysis being used today provides base statistics and rules-based detection of anomalies. To augment this capability, visual analytics pattern recognition is recommended to quickly and accurately identify patterns of interest within vessel movements over time.

Current situation:

- Radar surveillance systems currently deployed around the Great Lakes for the tracking of vessels
- Large volumes of tracking data is generated on a daily basis, tracking hundreds of vessels
- Limited visualization of tracking data
- Basic GIS system for mapping, with simple 2D mapping showing static vessel positions

Opportunities to deploy visual analysis techniques and technology:

- Geo-temporal visualization provides analysts with a view that displays the complete time range of a dataset, showing vessel movement within a geographical space
- Geo-temporal visualization to also display live data feeds
- Rapid automatic detection of movement patterns, vessel meetings, etc.
- Increase in analysis efficiency
- Support predictive analysis of future movement patterns

4.2 RCMP: Crime Analysis

The RCMP currently employs a number of systems to collect and manage information related to case activity. A list of data systems includes, but is not limited to: the Police Records Information Management Environment for British Columbia (PRIME-BC), the Police Reporting and Occurrence System (PROS) and the Violent Crime Linkage Analysis System (ViCLAS). These systems provide access to case and occurrence files across the RCMP force and are used daily by crime analysts working on active investigations. Basic query and retrieval tools are available but lack visualization and analysis capabilities. This limits both the discovery and linking of relevant information held within these systems.

Current situation:

- Records and case management systems that lack tools for visual query, filtering and scanning of relevant information
- Laborious manual assessment, summary and reporting procedures
- Computational analysis capabilities that rely on rigid variables defined by user input
- Limited interaction, visualization and presentation capabilities

Opportunities to deploy visual analysis techniques and technology:

- Visual search and filtering for rapid identification of relevant documents
- Graphical environment for visual evidence marshaling
- Interactive linking and grouping of documents
- Shared workspaces for collaborative workflows
- Multimedia analytics to fuse text/imagery/video/audio

4.3 Correctional Services of Canada: Review and Analysis of Parole Tracking Data

The Correctional Services of Canada is responsible for offenders who have been released on parole but are deemed a potential risk for reoffending. These parolees are monitored using a variety of high and low tech means, including, but not limited to GPS trackers, electronic breathalyzers or passive monitoring equipment. Monitoring and tracking information on parolees is collected and analyzed for potential breaches of their probation's conditions of release. These systems employ computational functions to identify breaches. Once alerted to a potential breach, an analyst must manually confirm by reviewing the recorded data.

Current situation:

- Large number of parolees monitored via GPS and other tracking technologies
- Massive amount of tracking data being collected and stored
- Basic alerts setup with rules based conditions that require manual validation
- Limited visualization and analysis capabilities
- Basic reporting functions

Opportunities to deploy visual analysis techniques and technology:

- System that combines both computational and visual analysis of parole's movement over time
- Monitoring of paroles locations over time with real-time updates
- Identify high risk parolees through repeated movement behaviors that violate conditions of their parole
- Provide a common operational picture of a district/territory
- Visual link and network analysis of individuals meeting or communicating
- Geo-temporal analysis of parolee movements for fast identification to quickly identify changes or alternations in their movement patterns

4.4 Canadian Security Intelligence Service (CSIS): Counterterrorism

Canada's intelligence service is tasked with monitoring and alerting of potential threats against to Canada's National Security. It provides services for the collecting, analyzing, reporting and disseminating of intelligence products. This requires analysts within CSIS to search and analyze large volumes of both private and public information sources. These sources include a variety of data types include structured and unstructured text, as well as multimedia elements. Once located, these pieces of information are then linked and organized in order to produce structured intelligence products.

Current situation:

- Need for rapid scanning and organization of information from multiple sources
- Focused on discovering links between key individuals, groups and events
- Reliance on broad spectrum of data sources, including internal resources and public information sources
- Large volume of reports generated with associated credibility and impact evaluation

Opportunities to deploy visual analysis techniques and technology:

- Triage raw information visually
    - Query across multiple data sources
    - Visual information scanning, characterization, correlation
    - Source monitoring for change/update detection
    - Trend and frequency analysis
- Visual evidence marshaling and sense making
    - Visual cognition
    - Link and network analysis
    - Hypothesis generation
    - Assertions with evidence
    - Structured analysis, e.g. Analysis of Competing Hypotheses
- Mixed initiative (human and machine reasoning combined in a visual analytic environment)
    - Cognitive and workflow modeling
    - Automated pattern detection
    - Natural language processing, e.g. automated entity, event, topic extraction
    - Multimedia analytics to fuse text/imagery/video/audio

4.5 Canadian Cyber Incident Response Centre (CCIRC): Cyber Security and Monitoring

With the continued rise in the number of cyber incidents and attacks, the role of Public Safety Canada's CCIRC center has become increasingly important in the identification, monitoring and reporting of cyber activity that could pose a threat to Canada's national security.

Opportunities to deploy visual analysis techniques and technology:

- Real-time monitoring and analysis of network activity events

- Aggregate view of events, incidents and alerts being generated across multiple agencies
- Visualization across all data sources
- Overview of current incidents and activity
- Deep dive visualization of incident activity and events

Scenario description utilizing visual analysis techniques and technology:

- A spike in inbound traffic targeting a Canadian Forces network is detected and shown on a large display, showing multiple servers on a network with their geographic location, linked to the nodes responsible for generating the inbound traffic
- The traffic pattern is quickly identified via visual recognition as a DDOS attack from a variety of hosts across the globe
- Low traffic volume hosts are filtered out of the visualization and large nodes are highlighted for identification
- Visual analysis of the large traffic nodes reveals that they are located all within the same geographical location
- Alerts are sent to the Canadian Forces network administrators
- Visual captures of the traffic patterns, locations and volumes are recorded and added to the incident report

5 Facilitating the Adoption of New Technology

Visual analytics is a new field of technology with demonstrated success among innovative organizations. The challenge is to continue this success with early adopters and with the mainstream of users. Innovators and early adopters are drawn to technology and experimentation, while mainstream users tend to be more pragmatically focused on solving problems. Best practices indicate that the rate and success of technology diffusion is largely dependent upon focusing on the needs of the user. Key points from the literature are summarized here.

In adapting new technologies, organizations exhibit several characteristics and stages of using the new capabilities. These should be understood in order to facilitate the successful introduction of a new technology to an organization and its subsequent nourishment there so that its use can grow to achieve its potential, and that the benefits are fully realized by the organization.

Technology adopters progress through five stages in the adoption/diffusion process [Rogers, 1995]:

1. Knowledge – awareness of the innovation
2. Persuasion – attitude toward the value of the innovation
3. Decision – choice of adoption or rejection
4. Implementation – putting the innovation to use
5. Confirmation – evaluating the results of the decision

Innovations are judged by adopters based on the following percieved attributes:

- Relative Advantage – improvement over the previous technology
- Compatibility – fit with environment adopted into
- Complexity – amount of difficulty to learn and use
- Trial-ability – ease of experimentation during the adoption process
- Observability – observable results visible to others

Technology adopters fall into several groups. These adopter groups or categories range from most to least innovative and are distributed in a bell-shaped curve as shown in Figure 1.

- Innovators – risk takers interested in technology
- Early Adopters – interested in technology to solve problems
- Early Majority – pragmatic problem solvers
- Late Majority – sceptical of new technology
- Laggards – critical of new technology

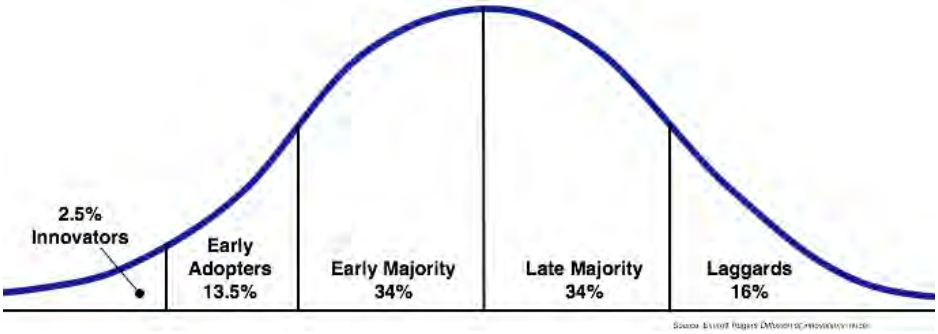


Figure 8 Technology Adopters [Rogers, 1995].

The transition from early adopters to early majority is key, but poses particular risk because of significant differences between the two as shown in Table 1. What works for one group does not work for the other. Each has different needs and needs to hear different messages.

Early Adopters	Early Majority
• Technology focused • Proponents of revolutionary change • Visionary users • Project oriented • Willing to take risks • Willing to experiment • Individually self-sufficient • Tend to communicate horizontally (focused across disciplines)	• Not technically focused • Proponents of evolutionary change • Pragmatic users • Process oriented • Averse to taking risks • Look for proven applications • May require support • Tend to communicate vertically (focused within a discipline)

Table 1 One Set of Messages is Required to Begin. Then Different Messages are Required to Transition to the Early Majority.

After an organization has started the ball rolling with an early adopter user group, different early majority adoption strategies need to be used. The keys to success are based on perception and needs and include the following methods.

- Include them in planning and policy making
- Relate technology to their specific work processes
- Address their real problems
- Provide training and support
- Ease of use of technology is more important
- Early success in use of technology needs to be shared
- Institutional advocacy is helpful

A user-centered implementation methodology is recommended. This includes structured interviews to determine requirements and needs, as well as collaborative and iterative refinement of the technology to meet the organization's needs. Pilot evaluation is recommended. This includes metrics-based user evaluation as well as usability and utility assessments. Diffusion to late majority and laggards will follow, encouraged through communication with early majority users.

6 Conclusion and Recommendations

This short report highlights 1) relevant and important visual analytic tools and technology, 2) opportunities within federal agencies to exploit visual analytic capabilities and 3) an overview of the pathway to adoption. It is our opinion that the science and technology of visual analytics helps facilitate the mission of the above mentioned agencies and can play a key role in driving discovery and comprehension of complex data used today. Innovative visual analytics tools at high technology readiness levels are available. In conclusion, we have the following recommendations for the DRDC Center for Security Science that would help to increase the awareness and rate of adoption of visual analytic capabilities within the Canadian public safety and first responder communities:

6.1 Provide sponsorship of pilot deployment of visual analytic tools within public safety and first responder agencies

- Engage industry and relevant agencies via government sponsorship
- Designed to help incubate the usage of innovative tools within agencies
- Successful deployments to be used as reference sites to encourage proliferation of usage and best practices of visual analytic tools

6.2 Formation of a Canadian Visual Analytics Technology Group (CVATG)

- Established to further the research, development and support of visual analytics tools and technology
- With representatives from industry, research and practitioner communities
- Sponsor an annual meeting to exchange information on successes and new developments

6.3 Creation and publication of visual analytics recommendations and best practices

- List of visual analytics tools and technologies relevant to the public safety and first responder communities
- Best practices and recommended implementations derived from panel of expert users, venders and researchers
- Updated and distributed on an annual basis

References

[1] BBN Web http://www.bbn.com/products_and_services/web_monitoring_system/

[2] **BBN Broadcast**
http://www.bbn.com/products_and_services/bbn_broadcast_monitoring_system/

[3] Carley, Kathleen & Reminga, Jeffrey & Storrick, Jon & Columbus, Dave, **ORA User's Guide 2010**, Carnegie Mellon University, School of Computer Science, Institute for Software Research, Technical Report, CMU-ISR-10-120.

[4] Chien, L., W. Wright, et al, Grand Challenge Award 2008: Support for Diverse Analytic Techniques - nSpace2 and GeoTime Visual Analytics, IEEE VAST Conference, 2008.

[5] Eccles, R., T. Kapler, R. Harper, and W. Wright, **Stories in GeoTime**, Winner Best Paper, IEEE Visual Analytics Science and Technology, 2007.

[6] **GeoTime**. http://www.oculusinfo.com/SoftwareProducts/GeoTime.html

[7] IndigoVision. http://www.indigovision.com/products_analytics.php

[8] **IN-SPIRE** http://in-spire.pnl.gov/index.stm

[9] Jonker, D., W. Wright, D. Schroh, P. Proulx, **Information Triage with TRIST**, Conf Intell Analysis, 2005.

[10] Kapler, T. and Wright W., **GeoTime Information Visualization**, IEEE InfoViz, 2004.

[11] Cook, K, Richard Fujimoto, Guy Lebanon, Haesun Park, and John Stasko, **A Taxonomy for Visual Analytics**, Mar, 2010. http://smlv.cc.gatech.edu/2010/03/17/a-taxonomy-for-visual-analytics/

[12] Kristensson, P., et al, **An Evaluation of Space Time Cube Representation of Spatiotemporal Patterns**, IEEE Transactions on Visualization and Computer Graphics, Vol 15, No 4, July 2009.

[13] Moore, G.A., Crossing the Chasm: Marketing and Selling Technology Products to Mainstream Customers, New York: Harper Business, 1991.

[14] Patent: System and Method for Visualizing Connected Temporal and Spatial Information, Patent number: 7180516, Filed Mar 29, 2004.

[15] Proulx, P., W. Wright et al, **nSpace and GeoTime - VAST 2006 Case Study**, IEEE Computer Graphics and Applications, Special Issue on Visual Analytics, Sept, 2007.

[16] Rogers, E.M., **Diffusion of Innovations** (4th ed.). New York: The Free Press, 1995.

[17] **Technology Readiness Levels**.
http://en.wikipedia.org/wiki/Technology_readiness_level

[18] Thomas, J. and K. Cook (Ed.), Illuminating the Path: The R&D Agenda for Visual Analytics, IEEE Press, 2005.

[19] Wright, W., D. Schroh, P. Proulx, **The Sandbox for Analysis – Concepts and Methods**, ACM CHI, 2006.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Oculus Onfo Inc.
2 Berkley St., suite 600
Toronto, ON
M5A 4J5

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE

Visual Analytics in Public Safety: Example Capabilities for Example Government Agencies

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Garton, Curtis; Wright , William

5. DATE OF PUBLICATION	6a. NO. OF PAGES	6b. NO. OF REFS
October 2011	34	19

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Centre for Security Science
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
	DRDC CSS CR 2011-25

11. DOCUMENT AVAILABILITY

Unlimited

12. DOCUMENT ANNOUNCEMENT

Unlimited

13. ABSTRACT

This is a short report discussing how Visual Analytics at large can improve capabilities at Canadian Departments and Agencies, such as Candian Security Intelligence Services (CSIS), Royal Canadian Mounted Police (RCMP), Public Safety Canada (PSC) and the Canada Border Services Agency (CBSA). The report begins with a brief summary of Visual Analytics. Several indicative visual analytic tools are then presented. These "case study" tools illustrate visual analytic technologies that are at a high Technology Readiness Level (TRL). There follows a description of potential visual analytics opportunities for several representative federal organizations. The report concludes with several recommendations on how the federal government may facilitate the adaptation and exploitation of Visual Analytic tools.

Ceci est un bref rapport dans lequel nous démontrons comment l'analytique visuel peut améliorer les capacités des ministères et organismes gouvernementaux canadiens comme le SCRC, la GRC, Sécurité publique Canada et l'ASFC. D'abord, nous donnons une description brève de l'analytique visuel. Nous présentons ensuite divers outils illustrant bien ce qu'est l'analytique visuel et qui en sont à un stade de développement technologique avancé. Nous explorons ensuite diverses solutions potentielles pour divers organismes fédéraux types. Le rapport se termine par des recommandations quant aux façons dont le gouvernement fédéral pourrait s'y prendre pour faciliter l'adaptation et l'exploitation d'un outil d'analytique visuel.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS

Visual Analytics; Public Security; Public Safety: Homeland Security; Decision Making; Large Complex Datasets