NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-131)TP/645

www.sto.nato.int

STO MEETING PROCEEDINGS **MP-IST-131**

Distributed Data Analytics for Combating Weapons of Mass Destruction

(Analyse distribuée des données dans la lutte contre les armes de destruction massive)

This Report documents the findings of the IST-131 Specialists' Meeting.

Published May 2017

Distribution and Availability on Back Cover

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-131)TP/645

www.sto.nato.int

STO MEETING PROCEEDINGS **MP-IST-131**

Distributed Data Analytics for Combating Weapons of Mass Destruction

(Analyse distribuée des données dans la lutte contre les armes de destruction massive)

This Report documents the findings of the IST-131 Specialists' Meeting.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published May 2017

ISBN 978-92-837-2089-8

Table of Contents

IST-131 Membership List

Dr. Timothy HANRATTY
Army Research Laboratory
2800 Powder Mill Road
Adelphi, MD 20783
UNITED STATES
Email: Timothy.p.hanratty.civ@mail.mil

Mr. Richard MAY (Co-Chair)
Defense Threat Reduction Agency (DTRA)
Advanced Analytics Division
J9ISA Information Sciences and Applications Department
8725 John J. Kingman Road, Stop 6201
Fort Belvoir, VA 22060
UNITED STATES
Email: richard.a.may52.civ@mail.mil

Dr. John PELLENGRINO
Army Research Laboratory
2800 Powder Mill Road
Adelphi, MD 20783
UNITED STATES
Email: John.m.pellegrino.civ@mail.mil

Ms. Lisbeth RASMUSSEN
Danish Defence Acquisition and Logistics Organization
Lautrupbjerg 1-5
DK-2750 Ballerup
DENMARK
Email: lr@mil.dk

Dr. Margaret J. VARGA (Co-Chair)
Seetru Ltd.
Albion Dockside Works
Bristol BS1 6UT
UNITED KINGDOM
and
University of Oxford
Old Road Campus Research Building
Roosevelt Drive
Oxford, OX3 7DQ
UNITED KINGDOM
Email: margaret.varga@oncology.ox.ac.uk

Distributed Data Analytics for Combating Weapons of Mass Destruction

(STO-MP-IST-131)

Executive Summary

Combating Weapons of Mass Destruction (CWMD) is an international military and civilian effort requiring a co-ordinated international and interdisciplinary effort. WMDs are a domestic threat to all NATO Nations, as well as in theatres of operation. The most effective approach to CWMD is to detect and disrupt threats early in the threat cycle. This requires the development of alternate signatures through the use of new data sources and analytical techniques. Open source and expanding commercial information sources represent huge potentials for new approaches to detecting illicit Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) activities. Exemplar information types include:

- Social media;
- Professional media;
- Shipping and transportation;
- Law enforcement; and
- Financial transactions.

However it is often not possible or desirable to co-locate all these data sources. This forces the requirement for new processes and algorithms to analyse data at rest in various locations and return properly prepared results based on a wide range of criteria. This is a complex problem since the quality and completeness of data sources is often unknown. The issue is only compounded when data representations are not compatible. Recent technical advances in cloud architectures, information analytics, and network connectivity require organizations to reconsider how they approach advanced analytics and leverage the cloud technologies now available to them. Adopting cloud-computing strategies represent a new era for national defence agencies' information management, distributed computation, and the foundations required for a next generation of visual analytics. Through increased implementation and acceptance of compatible cloud-based technologies, NATO members will be able to draw on data and analytic services from a broad swath of related domains that share common needs, such as intelligence, cyber defence, maritime, financial, aviation and transportation, etc.

This Specialists' Meeting brought together experts to identify critical operational and developmental needs. The challenge is how to develop the underlying data science and computational constructs that will enable the community to pull data out of today's stove-piped systems and integrate it into a data ecosystem that will support cross-discipline data sharing and analytics.

Analyse distribuée des données dans la lutte contre les armes de destruction massive

(STO-MP-IST-131)

Synthèse

La lutte contre les armes de destruction massive (ADM) est un défi international militaire et civil qui requiert un effort international et interdisciplinaire coordonné. Les ADM constituent une menace intérieure dans tous les pays de l'OTAN, ainsi que sur les théâtres des opérations. L'approche la plus efficace de lutte contre les ADM est de détecter et perturber les menaces au début du cycle de menace. Cela nécessite le développement de signatures alternatives par l'utilisation de nouvelles sources de données et de nouvelles techniques analytiques. Les sources libres et les sources d'informations commerciales en pleine expansion présentent un potentiel énorme pour les nouvelles approches de détection des activités nucléaires, radiologiques, biologiques, chimiques et explosives (NRBCE). Les sources d'information sont par exemple :

- Les médias sociaux ;
- Les médias professionnels ;
- L'expédition et le transport ;
- Forces de l'ordre ; et
- Les transactions financières.

Cependant, il n'est souvent pas possible ou souhaitable de regrouper physiquement toutes ces sources de données. De ce fait, il est nécessaire de disposer de nouveaux processus et algorithmes pour analyser les données stockées dans divers lieux et envoyer des résultats correctement préparés sur la base d'une large palette de critères. Il s'agit d'un problème complexe, car la qualité et l'exhaustivité des sources de données sont souvent inconnues. Lorsque les différentes représentations des données ne sont pas compatibles, la situation se complique. En raison des récents progrès techniques en architecture de « cloud », en analyse de l'information et en connectivité des réseaux, les organisations doivent revoir leur approche de l'analyse poussée et exploiter les technologies de « cloud » auxquelles elles peuvent à présent accéder. L'adoption de stratégies informatiques dans le « cloud » marque le début d'une nouvelle ère pour les agences de défense nationale, à travers la gestion des informations et le calcul distribué, et pose les bases d'une analyse visuelle de nouvelle génération. La mise en œuvre élargie et l'acceptation des technologies de « cloud » compatibles permettront aux membres de l'OTAN de faire appel à des données et services analytiques d'une vaste panoplie de domaines liés qui partagent des besoins communs, tels que le renseignement, la cyberdéfense, la marine, la finance, l'aviation et le transport.

Cette réunion des spécialistes visait à identifier les besoins opérationnels et de développement critiques. Le défi consistait à développer les concepts sous-jacents en matière d'informatique et de science des données qui permettraient à la communauté d'extraire des données de systèmes actuellement compartimentés et de les intégrer dans un écosystème de données supportant le partage et l'analyse interdisciplinaires des données.

DISTRIBUTED DATA ANALYTICS FOR COMBATING WEAPONS OF MASS DESTRUCTION

1.0 ANNOTATED AGENDA

1.1 Day 1: Wednesday, 15 October 2014

1.1.1 Morning – Session 1: Deploying Big Table Architectures for Analytics

Recently there has been a significant push to use HADOOP[1] and big table architectures for enterprise data management. This session consisted of breakout sessions to look at how well these architectures are working for complex analytical and visualization needs and identify next steps in their use.

Presenter: Eric Stickel – President OpsWare, LLC (Limited Liability Company)

Stage Setting Topics and Questions:

- How we can converge on agreed upon interoperability standards?
- Perfect or not, we need to find ways to move from testing to operational use.
- What needs to happen to manage the 'and' between different ontology/context data representations?
- How do we address the policy issues of sharing and can this be better supported through technology?
- Managing cross-domain access control with more robust queries between instances.
- In a NATO context, we could use a paper on how to approach information sharing.
- Are distributed, MapReduce frameworks an appropriate architecture for complex analytics and visualization?
- How can dynamic data that requires constant updating be effectively handled?
- Will early context binding through ontology based indexes scale as needed for analytics and visualization on systems supporting many mission lanes?
- Many systems being developed are using lightweight web interfaces (Ozone Widget Framework). Are these interfaces sufficient for visualization and analytics?
- Technically how do we incorporate specialized hardware?
- Should we promote common standards in creating core and common services?

1.1.2 Afternoon – Session 2: Managing Data – IO and Computation Strategies

Developing strategies for distributed analytics systems still requires the movement of data. Co-ordinating the movement of partial results between analytics nodes introduces unique considerations. There are also novel requirements for computational strategies to support the high-performance computing needs. These breakout sessions addressed current research effort and impact on practical application.

Presenter: Richard May Ph.D. – U.S. Defense Threat Reduction Agency

[1] An Apache Open Source Distributed Framework for Big Data.

Stage Setting Topics and Questions:

- What new schemas are needed for disambiguation and de-confliction of entities, relationships, and events in distributed knowledge repositories?
- To what level is data synchronization needed to maintain knowledge structures across repositories?
- What new methods are needed to run analysis on multiple partial, conceptually overlapping, and inconsistent data sets?
- Are there optimized schemas for addressing balance when data and/or analytics cannot be moved?
- How to optimize image and text knowledge extraction, processing, and metadata management for distributed analytics?

Combined Sessions 1 and 2 Breakout Groups:

- A: Data Sharing Cross-Domain, Cross-Nation;
- B: Specialized Hardware Approaches; and
- C: Context Finding Issues.

1.2 Day 2: Thursday, 16 October 2014

1.2.1 Morning – Session 3: Distributed Data Visual Analytics

Situational awareness for Combatting Weapons of Mass Destruction (CWMD) should involve many different domains. This session consisted of breakout sessions looking at current work in financial, cyber, and maritime domains using distributed data in visual analytic tools, etc.

Presenters:

- Mark Flood Ph.D. – U.S. Department of Treasury
- Valerie Lavigne – Defence Research and Development Canada (DRDC)
- Margaret Varga Ph.D. – Seetru Ltd. / Oxford University, UK

Stage Setting Topics and Questions:

- Unified data representations (definition and meaning).
- Large data strategies (define large vs. big data).
- Screen clutter – graph hair balls as an example.
- Text analysis: Changing of terms and acronym speak.
- In a robust distributed environment new information sources are likely to appear on a regular basis. How can they be made automatically detectable and available to visual analytic tools?
- Distributed analytics and data will likely introduce additional delays in generating results. Can techniques such as progressive disclosure provide interactive feedback?
- How can we support transparency while maintaining confidentiality across distributed users and data?
- Could pooling of aggregate/enhanced data augment the ideas of sharing indexes (soft/hard data)?

Session 3 Breakout Groups:

- D: Unified Data Representations / Large Data Strategies;
- E: Screen Clutter Reduction; and
- F: Text Analysis.

1.2.2 Afternoon – Session 4: Strategies for Challenging Environments

Remote field teams face unreliable communications, restricted bandwidth, and limited processing resources. While mega cities have significant infrastructure, they are potential breeding grounds for discontent and introduce significant challenges for detecting threats. All of these impact the ability to conduct analysis for countering Weapons of Mass Destruction (WMD). This session held breakout sessions looking at how to address these challenges and promote analytics and visualization in these complex environments.

Presenter: Dan Doney Ph.D. – U.S. Defence Intelligence Agency

Stage Setting Topics and Questions:

- Is sense making and decision-making under time constraints becoming even more challenging with knowledge overload?
- When is data too old for reliable analysis and use by field units and how to effectively represent aging information?
- Computing technology is becoming less of an issue in remote locations but connectivity is still a challenge and ways to apply the new capabilities.

1.3 Day 3: Friday, 17 October 2014

1.3.1 Morning – Session 5: Distributed Computing Policy

Addressing the technical challenges of distributed analytics is only part of the work required. There are policy considerations for data access, collaboration, and application of analytics. This breakout session looked at current policy issues impacting international collaboration on distributed analytics.

Presenter: Victoria Lemieux Ph.D. – University of British Columbia, Canada

Stage Setting Topics and Questions:

- How do we deploy mechanisms to securely ensure ownership and distribution of information is correctly enforced on distributed and shared knowledge repositories?
- Privacy rights. Encryption and the needs of authority to access information.

Session 5 Breakout Groups:

- G: Policy; and
- H: Challenging Environments.

2.0 SESSION DETAILS

2.1 Day 1 – Session 1: Deploying Big Table Architectures for Analytics

Eric Stickel presented the work that his company (OpsWare, LLC) and others have been doing in support of U.S. Army activities for data interoperability.

Eric Stickel: Integrated Sensor Architecture (ISA) – Abstract

The challenge is that we traditionally fail at moving from an idea into practice due to a lack of common security and data integrity support for information sharing. We have been developing a system called the Integrated Sensor Architecture (ISA) to support certifications between sensor feeds to support interoperability.

ISA works in a distributed environment where nodes are not assumed to be always available, but rather will come and go off the network based on operational conditions. ISA accounts for this by allowed feeds to dynamically register with the system and feed consumers to search for feeds of interest.

ISA is currently in the final stages of testing in the Amazon Services Cloud using simulated data. We expect to have interim operations in the next few months. At that time we will start to expand on the number of sensors that work in ISA.

2.2 Day 1 – Session 2: IO and Computation Strategies

An introduction to the topic was provided by Richard May followed by a brief discussion to further elaborate on interests and topics to the attendees.

2.3 Day 1 – Session 1 and 2 Combined: Breakout Groups

2.3.1 Breakout Group A: Data Sharing Cross-Domain, Cross-Nation

Group Coordinator: Eric Stickel

From a technical perspective, sharing (that is the transmission of bits) across domains is the same whether they are going between equivalent but separated systems, across security domains, or across national boundaries. The differences come in the policies that govern the what, how, and even why data shall be transmitted.

To this end, advancing the state of sharing for NATO and coalition partners should become a catalyst for other sharing needs. NATO does not need to drive technology itself that is occurring on its own as the Partner Nation's deal with big data and changing realities of information generation and consumption. NATO programs should focus on problems that are unique to Coalition forces. This would be a good way to focus on challenges that do not occur within a single country. While some of these challenges are well known such as language, symbology, and SOP, there are others, such as social context and norms that will impact information sharing and the use of that information.

It was discussed that policy-wise Memorandums of Understanding (MOUs) or Agreement (MOAs) are established to define both the need and scope of a sharing agreement. These arrangements identify the value of a relationship and set the bounds. Many of the MOUs that this group had experience with were broad in nature to support changes in scope and potential increases in collaborations. MOUs are the policy that allows

collaboration to take place. They are not the technical mechanism for information sharing. Network security protocols and the applications that ride on those networks provide the how of data sharing. There are significant challenges that have historically hindered collaboration. This has been especially true for Research and Development (R&D) collaborations which require the sharing of less polished material. The emergence of multi-level security models will help improve dissemination of information between Coalition partners.

A big part of enabling sharing is the enabling of trust. The system needs to maintain sufficient information so that each party knows what the other has done with the data. There are three components to such a system. First is to maintain provenance and ownership tags with data. This changes the relationship between sharing. Outside of the information world people share things every day, but that doesn't mean they give up the item. Children will share toys, but at the end of the day the owner of that toy still leaves with the toy. Typically information sharing is not sharing it is giving it away. Once information is shared it is for all intense and purposes beyond the control of the person that provided it. It requires a higher level of trust to give away your information. If on the other hand, the provider of information was still the owner and had the ability to interrogate the state of the information, then we can lower the level of trust required to share.

Another issue raised is the sharing of knowledge rather than just data. Often Coalition partners would like to share not only the raw data, but the knowledge they have applied to the data. Knowledge management requires more advance structures that are in binary format and could have encryption. Both of these are problems for most security guards. New techniques and technologies are needed to address these limitations to raise the level of knowledge sharing.

Several members of the group expressed the interest in developing a white paper. The focus would be on propositions for pilot projects intended for specific agencies and decision-makers in a NATO context.

2.3.2 Breakout Group B: Specialized Hardware Approaches

Group Coordinator: Matt Kochan

The discussion started with the fundamental question of '**What is Specialized Hardware?**'. We identified several platforms that are examples of different specialized hardware:

- D-Wave computers;
- General-Purpose computing on Graphics Processing Units (GPGPU);
- Automata;
- Quantum;
- Neuromorphic; and
- High-performance computing (contiguous memory) systems.

The links such as Interconnect and Quantum Key Distribution (QKD) are inherent in many of the architectures were discussed; they play the critical role in distributed environments. There will always be the need to move data or derived products between nodes, instances, or clouds.

Next we discussed the importance of storage in specialized environments – Non-HADOOP storage has become a specialized solution. Since most cloud architectures are focused on HADOOP and ACCUMULO[2],

[2] Apache Accumulo is a sorted and distributed key/value store built on top of Apache Hadoop, Zookeeper and Thrift.

the 'traditional' storage mechanisms have now become part of a non-standard architecture solution. That is, for the most part, there are limited ways to store and retrieve extremely large and diverse data sets. So regardless of the specialized hardware used, they will often tie to similar storage mechanism. This represents a strength, since now we can perform esoteric processing, but still access the results from main steam environments.

Why do we need specialized hardware for distributed cloud analytics? Efficiencies needed to produce results for problems that can be solved by traditional platforms, but fail to meet mission needs or objectives. Typically failings are related to performance. Some examples include:

- GPGPU Automata: Deep Neural nets.
- Quantum annealing.

Another problem is the solving of problems that previously were intractable with current computing hardware. Examples:

- Quantum: Factoring Integers, secure key distribution.
- Neuromorphic: Pattern matching.

There are a range of issues when it comes to actually implementing specialized hardware solutions:

- Mobility of data or code: There is a technical aspect of being able to move the data/code or the policy issue of being allowed to move the data/code.
- Specialized requirements: Formatting of data, queries, and algorithms to meet the needs of specialized hardware. For instance, representations of simple concepts (numeric) are not the same for quantum computers.
- Collapsing the architecture through abstraction of the complexities: Bringing memory, storage, and computing to an optimal configuration to provide needed performance.

2.3.3 Breakout Group C: Context Finding Issues

Group Coordinator: Steve Luce

The group's topic was context with respect to determining context from data – unstructured or structured – such that data can be correlated and discovered by context and the role to which ontologies can assist with context recognition without overly imposing constraints of models and processes too soon. The discussion was centered on the topic of ontological late binding, meaning: when can ontological principles be applied to a data to assist in determining context of data without imposing constraints on the data representation too early in the process?

Martin Taylor presented a convincing argument in that the term binding implies a fixed determination of data and context, yet the intent is to be flexible and evolve the context of data, thus, what is really occurring is the application of ontological principles when needed to assist with context with respect to the user's problem and/or hypothesis.

While Valarie Lavigne's briefing on the new multi-intelligent system was after this discussion, her system uses an 'uber' ontology, yet while its use is early on in the ingestion phase, its application is incrementally applied throughout the system. Little detail was provided, but the process may be worthy of further exploration.

Another Note: Martin Taylor's model of context is worthy of exploring to determine if it can be combined with a grammar-based data representation to assist in defining context in data.

Flexibility of data representations permits context to evolve with new data rather than imposing models and rules on data at the time data is introduced or ingested in to a system.

Grammar representations for data were discussed briefly as a mechanism for flexible data representation; the discussion was, however, curtailed as it required considerable time and should be a topic of another full discussion.

Contextual relevancy:

- Relevancy of context is important, yet it is subjective to an individual.
- Context of the event observed needs to be matched against the context of the interest/query.
- Relevancy simply defined as why perform an analytic, what is expected to be achieved and what action to be taken.
- Sensory data is continuous and constantly alters the context of the meaning of data – adjusts current understanding.
- Sensory, working episodic and semantic memory.
- Input context and output context are different and should be kept separate.
- Some technologies such as FrameNet, OWL, and rdf are helpful, but deemed not sufficient for contextual representation.
- Feedback mechanisms are helpful for determining life cycle of context and context relevancy … little feedback more decay.
- Prunable semantics automation as an aid to contextual de-confliction.
- Hypernodes [1] matching at different levels of similarity, network of similarities – worthy of exploration for tracking multiple contexts and data's participation in multiple contexts.

2.4 Day 2 – Session 3: Distributed Visual Analytics

Mark Flood Ph.D.: Cryptography and the Economics of Supervisory Information: Balancing Transparency and Confidentiality – Abstract

Financial regulation, like many official activities, faces important trade-offs between transparency and confidentiality of information. For example, prudential supervision can expose confidential financial information to examiners, who have a duty to protect it. At the same time, different agencies – often in different jurisdictions – can act more effectively when they share information to work with a more complete view of the situation. This tension often creates a confidentiality/transparency dichotomy that tends to push supervisory information policies to one extreme or the other. We argue that careful use of new techniques from the fields of secure computation and statistical data privacy can help relieve this dilemma by enabling sharing of key details while protecting the security of others. We provide a broad overview of these new technologies, and describe three specific usage scenarios where such beneficial solutions might be implemented.

Valerie Lavigne: Distributed Analytics for Maritime Domain Awareness and Social Network Analysis – Abstract

Defence Research and Development Canada (DRDC) supports defence and security operations at home and abroad with knowledge and technology. Over the last years, DRDC has performed applied research to explore the potential of visual analytics science and technology in a number of domains. We developed generic visualization tools that enable maritime situation and vessel of interest analysis, as well as social network

analysis in a counterinsurgency context. We plan to integrate these tools in a Sensemaking Support System prototype for enabling better joint intelligence collection and analysis capability.

Margaret Varga Ph.D.: Cyber Situation Awareness – Abstract

"*A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11*", Leon E. Panetta, U.S. Secretary of Defense, October 2012.

We are increasingly dependent on the ever-expanding internet with its increasing complexities and inter-dependencies. While on the one hand it provides immensely powerful infrastructure underpinning society, on the other hand its vulnerabilities to cyber-attacks pose immense risks to society and national security. Cyber attackers can cause widespread network destruction remotely, anonymously and at low cost. The attacks can be conducted through Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS), flooding, worms, viruses, hacking, etc.

In Spring 2007 the DDoS attack on Estonia targeted government websites as well as websites of banks, universities, and Estonian newspapers. The Estonian government decided to stop all international web traffic, resulting in cutting off the entire country from the rest of the world. After three weeks the attacks stopped abruptly.

In 2008, NATO set up the NATO Co-operative Cyber Defence Centre of Excellence in Tallinn. NATO 2020 states – Responding to the rising danger of cyber-attacks, NATO must:

> *"accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence."*

Cyber situation awareness is vital in support of making informed decisions for maintaining a safe and secure environment. In order to be effective security analysts must have:

- A constant and clear understanding of the status, health and performance of the networks;
- Be able to detect and identify any patterns or trends;
- Be able to detect and identify any changes or anomalies, and recognise their significance in a timely manner; and
- Be able to identify and reveal relationships, dependencies/inter-dependencies and vulnerabilities implicit in the data.

Cyber situation awareness is a continual round-the-clock operation, it includes: awareness of availability, confidentiality, operations and integrity, etc. It requires awareness of the network infrastructure and the security aspects of both the physical and cyber domains. There are also new sources of data such as social media to explore and exploit. In short, there is wide-ranging distributed data that can provide different insights and perspectives on the cyber situation.

Effective cyber situation awareness must not only be reactive but pro-active – supporting situation prediction.

In order effectively to realise the potential of distributed data, they must be made accessible for exploration, exploitation, analysis and visualization. There must be tools and techniques to support this – there is thus an extremely strong need to develop and apply visual analytics approaches that are appropriate for exploiting these distributed data.

2.4.1 Breakout Group D: Unified Data Representations / Large Data Strategies

Group Coordinator: Marty Jeffers

Unified Data Models (uber ontologies):

- Is it realistic to have a single global common data model? Probably not, but having access to all the data is important. We think it better to have a model that is more of a process to understand our requirements. The discussion then turned to the issue of provenance.

Provenance controls initial context; context evolves as the data is shared or manipulated:

- We asked if we can trace provenance through a piece of data's lifecycle; through appending attributes or other tactics; working is being done in this area that may or may not apply to our challenge; Provenance Standards is a starting point; build upon the origin of the data and its transforms; we are not sure we understand all the complexities of provenance so we should investigate this topic further; so what strategies can we use to handle the large and big data we expect in the future.

Process to develop the ontology grounded by physics constants or facts:

- We then went back to the topic of a process versus a model for an ontology; like physics, are there constants or facts in our ontology like basic physics; we think (assumption) there is with Time (temporal) and Space (location) being constants with any group we would want to share data; so maybe this is our starting point that "grounds" us and helps build a foundational process to build the grammar of our ontology.
- Grammar drives the structure of the ontologies to represent the data in some manner that the data can be used (grammar and provenance are aspects of the data that is shared).
- We didn't think this has been developed, so we need a process to converge and understand versus a single model for all data; our outcome is the need to define the process to determine how we structure, integrate, and visualize the ontology through the grammar we use to define it; a common process tied back to provenance traceability and how we can retain our internal meaning of the data or information while facilitating the ability of others we share with to have their own viewpoint and meaning for a piece of data.
- Outcome: We should investigate ways to develop this process for our internal ontologies and propagate and evolve it to include how we share with our external partners.

2.4.2 Breakout Group E: Screen Clutter Reduction

Group Coordinator: Paulette Aye

This group was interested in the current display techniques for big data sets that are clustered through a variety of techniques. We wanted to explore the display and user interaction and not the clustering techniques themselves. So we started with the initial question:

"Are current User Interface (UI) techniques sufficient for big data sets?"

The exact definition of 'big data' was not a concern to us as we felt the ability to display and interact with data was more of a constraining factor than the absolute mass (quantity, complexity, velocity) of the data.

Two common display approaches involve variants of using hypernodes or filtering. Hypernodes are used to display a cluster of nodes that have common elements allowing them to be represented as a single hypernode.

Filtering removes data from the display based on a common element or elements. It can be considered as a cluster removal approach. This brought us to the discussion that when designing the UIs, hypernodes can emphasis patterns of similarity, while filtering (or displaying that which is not filtered out) emphasis dis-similar elements.

Sampling was then discussed as a way to reduce the loss of fidelity that is common with most cluster display techniques as the data sets get larger. Used effectively, sampling can remove the need for clustering by reducing quantities sufficiently. Clustering algorithms are sometimes not as reliable as sampling. Clustering algorithms need to be tailorable to specific problems rather than abstracted to a general state. Understanding and documenting the mathematical rigor needed for tailored clustering was identified as a study or potentially research area. It does need to be recognized that there are many known weaknesses of sampling such as in network traffic or some sensor systems where sampling is not effective.

Cognitive design can help to ease the learning curve for clustering displays. Another customization is to exploit the use of metadata provided in the environment. Metadata can be one of the most powerful resources to make sure a design has cognitive relevance to the user.

It was mentioned that clustering is a way to reduce clutter from the display, but we were not clear as to what qualified as clutter. Two simple aspects were identified in the time we had. Clutter is anything that gets in the way of understanding the information. Clutter contributes to distraction.

2.4.3 Breakout Group F: Text Analysis

The group was concerned with psycho-linguistics, diplomatic and bilateral co-operative models of reading. The discussion was around issues on symbology, subterfuge, language innovation, gender/culture, power structures, and different modes of communication.

Text analysis is challenging with new words and acronyms constantly being created. Although, manual coding can, to some extent, address a “bag of words” approach, this does not scale for the ever-changing words in the social media. Entity extraction in texts remains a challenge, in particular, for large and multiple distributed datasets. The group concluded that there is a need for condensing text analysis results into a rich analytically salient visual representation for the analyst so as to support situational awareness and decision-making.

2.5 Day 2 – Session 4: Strategies for Challenging Environments

Dan Doney Ph.D.: Views on Cloud Development for Dynamic Coalition Partnerships

Defense Intelligence Agency (DIA) leadership has committed unequivocally to innovation as a top priority for the agency. Our relevance rests in large measure on the Agency’s ability to improve efficiency, effectiveness, and security through innovation in an era of rapidly declining resources and increased demand for products and services. Strategic focus and execution are required to address systemic barriers undermining agency agility, limiting creativity, and impeding the flow of resources to the best ideas.

To execute on the commitment to innovation, DIA leadership has established the Innovation Office (INO). INO is responsible for the establishment of an innovation-friendly environment across the Defense Intelligence Enterprise. The environment is designed to match the best ideas, existing or novel, big or small, from inside or outside the organization, and create mechanisms that enable discovery of what we didn’t know we needed. The INO is actively engaged in a transformational culture shift which welcomes change, unleashes the creativity

of DIA's workforce and empowers problem solvers to quickly turn ideas into solutions. Establishing an infrastructure of "systematic opportunism" supports the generation, mobility, and growth of ideas and will unlock new possibilities enabling us to tackle current and future challenges efficiently and effectively.

2.6 Day 3 – Session 5: Distributed Computing Policy

Victoria Lemieux Ph.D.: InterPARES, Metadata: Authenticity and Provenance in the Cloud – Abstract

The iTrust Project seeks to discover to what degree metadata about records in the cloud contribute to the assessment of their authenticity. In previous InterPARES (International Research on Permanent Authentic Records in Electronic Systems) research projects, authenticity was shown to be guaranteed by the identity of the record(s) and their integrity, but also the integrity of the system(s) holding them. When those systems are cloud systems, we need to ask whether this model of metadata and the design requirements for preserving authentic digital records changes. The overall goal of InterPARES Trust is to understand these new records environments and what we can expect from them with regard to metadata and system integrity.

We also are interested not only in records in the traditional sense, but also data and datasets, often repurposed from various sources, that are increasingly in use in predictive analytics and decision-making. The world of data often talks not so much about authenticity as about provenance – a concept foundational to archival science, but reinterpreted in the era of big data. We need to know who is responsible – and this is increasingly a distributed responsibility

2.6.1 Issues Related to Metadata in the Cloud

So far we have made the tacit assumption that metadata is added by the creator of the record, knowingly or not, but in a cloud environment new challenges arise. In order to manage client data, a cloud service-provider takes a certain level of control over that material. When records or data are entrusted to cloud systems, creator-generated metadata are also stored, and Cloud Solution Providers (CSPs) assume control of the material. Within this new environment, these user records will acquire additional metadata from the CSP that will be indicative of a number of important elements, including, but not limited to, storage locations, access controls, security or protection measures, failed or successful manipulations or breaches, etc. CSPs may also outsource some components of their services to other third parties, who may also generate service metadata that provide assertions about the maintenance and handling of the material, and about their own actions taken in the course of handling the material. While these metadata are linked to the users' records, much of it remains proprietary to the provider and not the user.

Consequently, proprietary CSP metadata present a sort of event horizon, beyond which the ability to establish an unbroken chain of custody is lost to the owner of the records. CSPs remain reluctant to share information about the cloud environment itself, the movements of a client's data within the system, and when the provider (or its contracted third parties) might have access to the data. Additionally, the network of third-party subcontracts employed by a provider may make it impossible for them to know such information. Nevertheless, these metadata remain invaluable to the user in assessing and ensuring the accuracy, reliability, and integrity of the material over the whole service lifecycle [2], [3]. Is there a way in which a balance might be struck between a provider's desire to protect the confidentiality of their business processes and trade secrets, and a client's need to ensure trustworthy records in the cloud? Much of the reluctance to engage cloud services might be mitigated by transparent and standardized metadata that is collected, managed, and then shared with users by CSPs Castro-Leon et al. [2].

2.6.2 Establishing the Chain of Custody and Preservation

The Chain of Custody, needed to establish the authenticity of records in cloud environments, has been defined as: "*1. Records · The succession of offices or persons who have held materials from the moment they were created; 2. Law · The succession of officers or individuals who have held real evidence from the moment it is obtained until presented in court.*" … and … "In both senses, the ability to demonstrate an unbroken chain of custody is an important test of the authenticity of records or evidence." [4].

The Chain of Preservation is a complementary construct that extends the notion of the chain of custody into future time. It is defined as "*A system of controls that extends over the entire lifecycle of records and ensures their identity and integrity in any action that affects the way the records are represented in storage or presented for use.*" [5]. There must be an unbroken process extending over the life of the records that, at the very least, enables an assessment of whether the records remain uncorrupted and ideally protects them against loss or corruption.

The minimum requirements for the Chain of Preservation are set out in the InterPARES 1 Baseline and Baseline Requirements.

To establish a model for the chain of preservation in cloud environments, iTrust is working with the Object Management Group (OMG) on a Preservation Services Initiative. The OMG is an international, open membership, not for- profit technology standards consortium. Founded in 1989, OMG standards are driven by vendors, end-users, academic institutions and government agencies.

OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries. In June 2014, iTrust proposed to the OMG the development of an OMG standard on digital preservation based on the functional requirements being defined in PaaST (Preservation as a Service for Trust). The proposal was accepted and is going forward under the OMG Government Domain Task Force. The preservation standard will be aligned with the existing OMG Records Management Services Specification.

2.6.3 Breakout Group G: Policy

Group Coordinator: Victoria Lemieux

We noted that trust is key but very context sensitive. "What are the mechanisms by which I can check that the trust has not been violated?" We need to explore this. Systems need to have built in TRUST metadata. Just like security, it has to be a first-order member of the data world. It has to be immutable and reliable and 'interrogatable'. People don't mind if they trust and can verify that the government is going to do the right thing with their data.

We observed that human weakness an issue – this is the reason we have security; people feel that they are the exception to the rule. This is both internal and external to the system. Policy is commonly used to inforce accepted convention. In the world of data, those policies are often distinct from the data itself – the policy sits on a shelf and the data sits in a computer; and other than training a user, we do not connect the two.

We spoke about the tension between privacy and security, e.g., current discussion about encryption on the phone to protect the data privacy – but this would make security investigations more difficult. This is not a new debate and no easy answers have been identified recently. In fact the tension between privacy and security has become more heated as more communications are electronic. In the age of FaceBook, Instagram, Twitter, Flickr and many others, the importance of more formal email and phone calls are becoming diluted.

We noted the need for structured conversation with private/public policy debate. For example, the need to protect information about data gathering and analytic capabilities for investigative purposes. It is paramount to ensure the investigation process can stand up in a court of law. It is also vital that the community understand the process involved.

We noted that we need to interrogate the level of granularity that is really necessary for a particular task. This can be described as the difference between tactical and strategic needs. A tactical task might need to know individuals involved to conduct a targeting task, wherein strategic assessment only cares about changes in broad trends that could be indicators of broad-based changes.

There is a growing technology suite of masking techniques to protect the individuals identified in data; however, it is possible to reverse-engineer these techniques.

We noted that data granularity is hard to manage. Being very specific about the type of data and who can have control and authority for a significant number of granular rules down to word token and every attribute value pair that's matched to an individual is burdening. As policy people we tend to approach this task through manual effort. In the big data world where data resides everywhere and anywhere, this is not practical.

What are the factors that matter in modelling access?

- Temporal changes (related to the notion of change of status in users/purpose over time).
- Who uses it?
- Who has responsibility?
- What is the context and purpose?

A rather esoteric debate then came up around the reasonableness of expectations on privacy in the present environment. What are the trade-offs between privacy and the lack thereof. What are the things that we want to keep private? What are the risks to them not being private? It is probably safe to say everyone has things they would wish to keep private, but when does that expectation clash with our actions. For instance, posting to Facebook where only 'friends' can see them.

We noted that people/organizations don't always accurately assess risk. What is the perceived risk? Studies have often shown that people can be very bad at assessing risk. Yet we commonly rely on human assessment of risk. Can data have an inherent risk element?

Attributes around the particular situation/context, e.g., strategic security of information versus tactical security – is it better to reveal information about a sniper in the field to let him know you've seen them? If that stops them from killing again then was it worth the risk of not capturing him. Morality is sometimes the core of the situation, but not the data.

We still have to deal with the data correlation problem and what can be learned from combining data. What is the risk, value, classification, from a government perspective, of combined data? The assessment of derivative classification is a growing problem.

What is an analytic and how does it differ from data? If I have a result of an algorithm, I can expose the analytic result without having re-run the analytic. Do we need to protect the result of the analytic?

2.6.4 Breakout Group H: Challenging Environments

Group Coordinator: Richard May

There is a growing technology base for using powerful hand-held devices as a wide range of sensors. In some cases it is utilizing or enhancing the sensors already on the device. For instance, photogrammetry can be done with a built-in camera, Global Positioning System (GPS), and 6 degree-of-freedom sensors. Other sensors such as chemical, biological, and audio are more readily added through the common access ports or Bluetooth technology now standard on all smart devices. This dramatically changes the use of 'human sensors' as well as the new need for advanced processing capability and ad-hoc networks.

It was recognized that we need to document activities through pictures, notes, and breadcrumb markers, but there are a significant number of cases where this has to be done without leaving a footprint. That means rapid uploading and deletion from the device through secure and reliable communications. At a minimum, on-device encryption and 'device slagging' is required. All this only adds to the problems associated with supporting disadvantaged environments.

Often disadvantaged environments are associated with third-world countries. However, after a natural disaster we are sometimes the disadvantaged environment. Commercial cell networks have proven to be fragile and those parts that do remain active quickly become overwhelmed. Societal norms that are taken for fact and provide a base to function on are swept aside by much more basic needs including the need to survive. Developing for maintaining situational awareness though information and communications has to take these realities into account.

In cases of disease outbreaks or potentially chemical disasters, samples are collected in the field. Analysis in the field is often challenging, so these samples are sent off-site for analysis. From a data sciences perspective, this causes several problems. Often provenance is lost, making it extremely difficult to place samples in context. Being able to provide in-situ analysis requires processing and network leaf (at the end of the network) sustainability. By automating as much of this as possible, we can remove the need for humans to spend time writing down information and more time assessing vital information and making informed decisions.

We have already discussed and alluded to many different challenges, but it is important to remember those that underlie everything. Things like visual displays. Direct sunlight makes it hard to read screens, as will bouncing around in a vehicle driving over dirt roads. Hazmat gear makes touch screen or even stylus use difficult, if not impossible. Both power and connectivity remain a challenge, although new technology is helping to address these.

It was discussed earlier that sensors are now becoming a common part of smart devices or can readily be added. However, there are hard-science limitations to many of these sensor precision and reliability. Not all information is good information if the noise is too great or reliability insufficient.

When addressing connectivity, we generally are looking to using a hub and spoke model as this better accommodates the 'no footprint' model. Given the likely connectivity issues, a mesh model between different nodes might provide better data reliability across the network and at the specific end nodes. It also opens up the possibility for developing local clouds even if outside connectivity is severed. With advances in solid-state drives and other systems, significant process can be pushed out to the end nodes. Using cloud services approaches there, isolated cloudlets can conduct significant analysis and share it in real time with nodes on the cloudlet. Once connectivity is re-established, a synchronization process is done.

In the not-distant-future there are likely to be many more autonomous units (flying, crawling, swimming, and stationary). How can we consider the use of that information in decision-making? These sensors will have a wide variance in accuracy, velocity, and on-board calculations, yet somehow we need to feed the field teams easily understood information and context. Safety is a time-critical variable for CWMD. Current weather input can be the deciding factor of knowing if you are inside or outside the calculated area of concern. If a field team is being informed by field sensors, then weather information becomes less relevant, but only if the sensor feeds are timely. Model development that takes into account all these factors could provide a more robust measure of the current situation.

This led to the fundamental question. Does data decay become a fundamental element of information? But decay has multiple dimensions. For example, the decay rate of a person being in a building could be very small, but if it is known that he/she rarely leaves a neighbourhood, then that decay rate is long. Understanding which external factors have effect on decay is important. For instance, the decay value of a road is very long, but if it is prone to floods, then in times of rain the decay becomes short – or is it that the certainty of the decay that changes?

Prioritization was the final topic discussed. We have potentially conflicting values of need-to-know and completing tasks in the new high-information environments. The old view of compartmentalization requires significant time and has built-in assumptions as to the amount of information. How that data is prioritized for transition and display determines what is displayed relative to the task at hand. Issues of need-to-know (security, distribution, authorization, trust) have to be backed into the data from ingest and maintained throughout the life cycle.

3.0 REFERENCES

[1] Bjørke, J.T., Nilsen, S. and Varga, M.J., "Visualization of network structure by the application of hypernodes", International J. of Approximate Reasoning, 51, pp. 275-293, 2010.

[2] Castro-Leon, E., Shekhar, M., and Harmon, R.R., "On the Concept of Metadata Exchange in Cloud Services, Part 1", Service Technology Magazine, 71, March/April, 2013.

[3] Smit, M., Shtern, M., Simmons, B and Litoiu, M., "Partitioning applications for hybrid and federated clouds", Proceeding of CASCON '12 Proceedings of the 2012 Conference of the Center for Advanced Studies on Collaborative Research, pp. 27-41, 2012.

[4] Pearce-Moses, R., "A glossary of archival and records terminology", Chicago: Society of American Archivists, 2005.

[5] InterPARES 2 Project glossary, International Research on Permanent Authentic Records in Electronic Systems, The InterPARES 2 Project Glossary, 2 February 2014, http://www.interpares,org/ip2/ips_terminology_db.cfm.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-MP-IST-131 AC/323(IST-131)TP/645	ISBN 978-92-837-2089-8	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Distributed Data Analytics for Combating Weapons of Mass Destruction

7. Presented at/Sponsored by

This Report documents the findings of the IST-131 Specialists' Meeting.

8. Author(s)/Editor(s)	9. Date
Multiple	May 2017
10. Author's/Editor's Address	**11. Pages**
Multiple	28

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Archival
Cloud computing
Distributed
Security
Social media
Visual analytics
Weapons of mass destruction

14. Abstract

Combatting Weapons of Mass Destruction (CWMD) is an international military and civilian issue requiring a coordinated international interdisciplinary effort. WMDs are a domestic threat to all NATO Nations as well as in theaters of operation. The most effective approach to CWMD is to detect and disrupt threats early in the threat cycle. This requires the development of alternate signatures through the use of new data sources and analytical techniques. Open source represents one of the greatest potentials for new approaches to detecting illicit Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) activities. Exemplar information types include social media, professional media, shipping and transportation, law enforcement, and financial transactions. However, it is often not possible or desirable to co-locate all these data sources. This forces the requirement for new processes and algorithms to analyze data at rest in various locations and return properly prepared results based on a wide range of criteria. This is a complex problem since the quality and completeness of data sources is often unknown. The issue is only compounded when data schemas are not compatible. There are many unresolved research questions in relation to distributed analytics.

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

DIFFUSION DES PUBLICATIONS

STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST
Recherche et développement pour la défense Canada
101 Colonel By Drive, 6 CBS
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Centro Gestione Conoscenza
Secretariat General of Defence
National Armaments Directorate
Via XX Settembre 123/A
00187 Roma

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM
Defence Research and Development Canada
101 Colonel By Drive, 6 CBS
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Centro Gestione Conoscenza
Secretariat General of Defence
National Armaments Directorate
Via XX Settembre 123/A
00187 Roma

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2089-8