
NORTH ATLANTIC TREATY
ORGANIZATION



AC/323(SCI-279)TP/931

SCIENCE AND TECHNOLOGY
ORGANIZATION



www.sto.nato.int

STO TECHNICAL REPORT

TR-SCI-279

Technical Considerations for Enabling a NATO-Centric Space Domain Common Operating Picture (COP)

(Considérations techniques favorisant une situation opérationnelle commune (COP) du domaine spatial centrée sur l'OTAN)

Final report of RTG SCI-279.



Published December 2020





STO TECHNICAL REPORT

TR-SCI-279

Technical Considerations for Enabling a NATO-Centric Space Domain Common Operating Picture (COP)

(Considérations techniques favorisant une situation opérationnelle
commune (COP) du domaine spatial centrée sur l'OTAN)

Final report of RTG SCI-279.

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 December 2020

Copyright © STO/NATO 2020
All Rights Reserved

ISBN 978-92-837-2256-4

Single copies of this publication or of a part of it may be made for individual use only by those organisations or individuals in NATO Nations defined by the limitation notice printed on the front cover. The approval of the STO Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Table of Contents

	Page
List of Figures	iv
List of Acronyms	v
Acknowledgements	vi
SCI-279 Membership List	vii
Executive Summary and Synthèse	ES-1
Technical Considerations for Enabling NATO-Centric Space Domain Common Operating Picture (COP)	1
1.0 Introduction	1
2.0 Space Domain Awareness	2
2.1 General Context	2
3.0 The Three Pillars of SDA	4
3.1 Space Object and Tracking	4
3.2 Space Environment Effects and Impacts	11
3.3 Radio Frequency Interference	14
3.3.1 Sources of Radio Frequency Interference	15
3.3.2 Mitigation Measures	16
3.3.3 Maintaining an Operational Picture of the RF Environment	17
3.3.4 The Traffic Plan	17
3.3.5 Monitoring the RF Environment	17
4.0 Challenges of Creating a Common Operational Picture	19
4.1 Space Domain Awareness and Big Data Science and Analytics	20
4.2 Architectural Concepts for a Common Operational Picture	23
4.3 Information Security and Assurance	25
4.4 Role of Standards	26
4.5 Challenges of Displaying the Space Domain	27
5.0 Conclusions	28
5.1 Summary Observations and Recommendations	30
6.0 References	31
Appendix 1: Approach and Assumptions	33
Appendix 2: Scenario Descriptions	35
Scenario 1: “Loss of Satellite Communication”	35
Scenario 2: “Overflight Warning”	35
Scenario 3: “GPS Accuracy”	36
Scenario 4: “Contingency Awareness and Response to Adversarial Action”	36

List of Figures

Figure		Page
Figure 1	Correlated vs. Uncorrelated Detections from the Space Surveillance Telescope (SST)	6
Figure 2	Orbit Determination Process	7
Figure 3	Biometric Identification Process	9
Figure 4	Artist's Rendition of Topex ASO	10
Figure 5	First Pass of Photometric Signature of Topex Represented in a Mollweide Projection	10
Figure 6	Second Pass of Photometric Signature of Topex Represented in a Mollweide Projection	11
Figure 7	Earth's Magnetic Field Affected by the Solar Wind	12
Figure 8	Earth's Atmosphere	13
Figure 9	From Information to Decisions: Image from Oracle Online Presentation	20
Figure 10	Schema Implemented Currently in ASTRIAGraph	21
Figure 11	RDF-Based Big Data Framework	22
Figure 12	Examples of Big Data Analytics	23
Figure 13	Data Fusion	24
Figure 14	Local Maritime Operating Picture	24
Figure 15	Global Maritime Operating Picture	25

List of Acronyms

COP	Common Operating Picture; also, Common Operational Picture
GEO	Geostationary Earth Orbit
GPS	Global Positioning System
ISA	Information Security and Assurance
LBP	Linear-based Production
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
OD	Orbital Determination
QKD	Quantum Key Distribution
RF	Radio Frequency
RFI	Radio Frequency Interference
SCI	(NATO STO) Systems Concepts and Integration (Panel)
SDA	Space Domain Awareness
SSA	Space Situational Awareness
STO	(NATO) Science and Technology Organization
TLE	Two-Line Element (Set)

Acknowledgements

Special thanks go to the NATO STO/CSO Staff, in particular to the SCI Executives, to the SCI Panel Assistant, Ms. Carlotta Rossi, and to the SCI Panel POC, Dr. Donald A. Lewis for the support and advice during the lifetime of the Task Group and the preparation of this final Technical Report.

All the members of the NATO STO SCI-279 TG are also gratefully acknowledged for their contribution to the objectives of this study.

SCI-279 Membership List

CO-CHAIRS

Dr Moriba JAH*
The University of Texas at Austin
UNITED STATES
Email: moriba@utexas.edu

Dr Tiziana CASINELLI*
EUTELSAT SAOperations
ITALY
EMail: tizicasi@gmail.com

MEMBERS

Dr Kyle T. ALFRIEND
Texas A&M University
UNITED STATES
Email: alfriend@tamu.edu

Dr Pascal FAUCHER
French Space Agency
FRANCE
Email: pascal.faucher@cnes.fr

Mr Lars Christer ANDERSSON
Swedish Defence Agency (FOI)
SWEDEN
Email: christer.andersson@foi.se

Dr Hauke FIEDLER*
Deutsches Zentrum für Luft- und Raumfahrt
e.V. (DLR)
GERMANY
Email: Hauke.Fiedler@dlr.de

Mr Andrew ASH
Dstl
UNITED KINGDOM
Email: aash@dstl.gov.uk

Mr Nicolas FROUVELLE
CS Communications & Systemes/Systèmes
d'Information
FRANCE
Email: frouvelle.nicolas@c-s.fr

LtCol Kevin BOLLINO
European Office of Aerospace Research
and Development (EOARD)
UNITED STATES
Email: kevin.bollino@us.af.mil

Dr Neil James GORDON
DSTO, Dept. of Defence
AUSTRALIA
Email: neil.gordon@dsto.defence.gov.au

Mr Richard Henry BUENNEKE
Bureau of Arms Control, Verification
and Compliance
UNITED STATES
Email: BuennekeRH@state.gov

Mr Henry (Hank) GRABOWSKI
Applied Defense Solutions
UNITED STATES
Email: hank@applieddefense.com

Dr Ronald Patrick DONNELLY
Dstl
UNITED KINGDOM
Email: rpdonnelly@dstl.gov.uk

Mr Thomas GRAUPMANN
Germany Ministry of Defence
GERMANY
Email: thomasgraupmann@bundeswehr.org

Dr Daniel Casquilho FARIA*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: daniel.faria@foi.se

Dr Clinton HEINZE
Defence Science and Technology London
AUSTRALIA
Email: clinton.heinze@defence.gov.au

* Contributing Author

Mr Christopher KEBSCHULL
TU Braunschweig
GERMANY
Email: c.kebschull@tu-braunschweig.de

Dr Thomas KELECY
Boeing
UNITED STATES
Email: thomas.m.kelecy@boeing.com

Dr Reinhard KIEHLING
Deutsches Zentrum für Luft-und Raumfahrt
e.V. (DLR)
GERMANY
Email: Reinhard.Kiehling2@dlr.de

Mr Thomas John KUBANCIK
Applied Defense Solutions
UNITED STATES
Email: tkubancik@comcast.net

Dr Michael LINDEN-VÖRNLE*
Technical University of Denmark
DENMARK
Email: mykal@space.dtu.dk

Prof. Marco MARTORELLA*
University of Pisa
ITALY
Email: m.martorella@iet.unipi.it

Lt Col Steffen NEUMANN
Germany Ministry of Defence
GERMANY
Email: steffenneumann@bundeswehr.org

Mr Tomas Matti-Pekka NYLUND
Swedish Defence Research Agency (FOI)
SWEDEN
Email: matti.nylund@foi.se

Dr Xavier PASCO
Fondation pour la Recherche Stratégique
FRANCE
Email: x.pasco@frstrategie.org

LTC Lothar PICHLER*
German Space Situational Awareness Centre
GERMANY
Email: LotharPichler@bundeswehr.org

Mr Mark RAWLINS*
Global Government Services EMEA
UNITED KINGDOM
Email: mrawlins@eutelsat.com

Major Melissa REYES*
Defence Research & Development (DRDC)
CANADA
Email: MELISSA.REYES@forces.gc.ca

Dr David ROBERTS
Defence Science and Technology Organisation
AUSTRALIA
Email: David.Roberts22@defence.gov.au

COL Franck SCHROTTENLOHER
Département Emploi des Forces
FRANCE
Email: franck.schrottenloher@intradef.gouv.fr

Ms. Caroline SCHWEITZER
Fraunhofer IOSB
GERMANY
Email: caroline.schweitzer@iosb.fraunhofer.de

Mr Robert (Lauchie) SCOTT
Defence Research & Development (DRDC)
CANADA
Email: Robert.Scott@drdc-rddc.gc.ca

LtCol Dr Giovanni SEMBENINI
CMRE
ITALY
Email: Giovanni.sembenini@cmre.nato.int

Ms Carolyn SHEAFF*
AFRL/RIED
UNITED STATES
Email: carolyn.sheaff@us.af.mil

Mr Thomas USLEANDER
Fraunhofer Institute
GERMANY
Email: marion.hutzel@iosb.fraunhofer.de

Mr Juan-Luis VALERO*
European Union Satellite Centre
SPAIN
Email: juanluis.valero@satcen.europa.eu

* Contributing Author

Ms (Ir.) Linda VAN DER HAM*
TNO Defence Safety and Security
NETHERLANDS
Email: linda.vanderham@tno.nl

Mr Wouter VAN DER WIEL
TNO
NETHERLANDS
Email: wouter.vanderwiel@tno.nl

Ms Xuemin WANG
Defence Research & Development (DRDC)
CANADA
Email: Xuemin.Wang@drdc-rddc.gc.ca

Dr Carsten WIEDEMANN
Technical University Braunschweig
GERMANY
Email: c.wiedemann@tu-braunschweig.de

Prof Marek ZIEBART*
University College London
UNITED KINGDOM
Email: m.ziebart@ucl.ac.uk

PANEL/GROUP MENTOR

Dr Donald LEWIS
The Aerospace Corporation, Strategic Awareness and Policy Directorate
UNITED STATES
Email: donald.a.lewis@aero.org

* Contributing Author



Technical Considerations for Enabling a NATO-Centric Space Domain Common Operating Picture (COP) (STO-TR-SCI-279)

Executive Summary

The SCI-279 Task Group explored the technical considerations of a NATO Common Operating Picture for space and recommended actions for strengthening NATO space domain awareness capability. Focus was placed on three space domain areas:

- 1) Space Surveillance and Tracking;
- 2) The Space Environment; and
- 3) Radio Frequency Interference.

The following are the six summary observations and recommendations cutting across those three focus areas that resulted.

Observation: The common space domain awareness requirements of the NATO Alliance to achieve maximum exploitation and preservation of its space capabilities are not well understood, nor have they been formally discussed or documented.

Recommendation: Conduct strategic analyses of the NATO requirements for space domain awareness involving its military planners, operators, space service (e.g., SATCOM, PNT, ISR) providers as well as providers of space domain awareness data, products and services.

Observation: Currently there are no NATO standards for describing space objects or events, or for processing and dissemination of data and information related to the space domain.

Recommendation: Develop an initial set of foundational standards for characterizing and applying space domain related data, products and processes critical to enabling and preserving NATO space activities.

Observation: Currently no commonly agreed upon processes or models for fusion of space domain data from disparate sources exist that can be applied to anticipated future NATO needs.

Recommendation: Articulate the requirements for initial space data fusion capabilities and the initial investments and focus that should be pursued consistent with anticipated NATO requirements for space domain awareness.

Observation: Throughout NATO member nations there is uneven technical and operational experience with space domain data collection, processing, dissemination and application that hinders both maximum exploitation and preservation of NATO space capabilities.

Recommendation: Expand the sharing of tradecraft, data and experiences throughout the NATO space capability providers, S&T community, and NATO military trainers, planners and operators.

Observation: Within NATO there has been no shared experience with the collection, fusion and dissemination of space domain data or information to provide a basis for understanding the opportunities and challenges of achieving a NATO common space domain operating picture.

Recommendation: Seek opportunities for experiments and field trials involving shared collection, processing and dissemination of space domain data and products to facilitate a common understanding within the Alliance of the opportunities and challenges ahead.

Observation: The integration of space domain awareness into NATO military planning and operational decision making is limited principally due to a minimal degree of operational art involving space.

Recommendation: Undertake, via NATO S&T elements, modelling and simulation analyses of the military utility of various decision-making options involving space domain awareness as well as exploration of technical solutions enabling timely and effective integration of space domain awareness into NATO military planning and operations.

Considérations techniques favorisant une situation opérationnelle commune (COP) du domaine spatial centrée sur l'OTAN

(STO-TR-SCI-279)

Synthèse

Le groupe de travail SCI-279 a étudié les considérations techniques d'une situation opérationnelle commune de l'OTAN pour l'espace et a recommandé des mesures de renforcement de la capacité de connaissance du domaine spatial de l'OTAN. L'accent a été mis sur trois aspects du domaine spatial :

- 1) La surveillance et le suivi de l'espace ;
- 2) L'environnement spatial ; et
- 3) L'interférence sur les fréquences radioélectriques.

Nous résumons ci-dessous les six observations et recommandations résultant du RTG dans ces trois domaines.

Observation : les besoins de connaissance commune du domaine spatial de l'Alliance pour obtenir une exploitation maximale et une préservation de ses capacités spatiales ne sont pas bien compris et n'ont pas été officiellement discutés ni documentés.

Recommandation : mener des analyses stratégiques des besoins de l'OTAN en matière de connaissance du domaine spatial, impliquant ses planificateurs, opérateurs et prestataires de service spatial (par exemple, SATCOM, PNT, ISR), ainsi que les fournisseurs de données, de produits et de services de connaissance du domaine spatial.

Observation : il n'existe pas, à l'heure actuelle, de normes OTAN permettant de décrire les objets ou événements spatiaux ou de traiter et diffuser les données et informations liées au domaine spatial.

Recommandation : élaborer un ensemble initial de normes fondamentales visant à caractériser et appliquer les données, produits et processus cruciaux liés au domaine spatial, pour favoriser et préserver les activités spatiales de l'OTAN.

Observation : actuellement, il n'existe pas de processus ou de modèle consensuels, relatifs à la fusion de données du domaine spatial provenant de sources disparates, qui puissent être appliqués aux futurs besoins anticipés de l'OTAN.

Recommandation : articuler les exigences en matière de capacités initiales de fusion des données spatiales et les investissements initiaux et se concentrer sur ce qu'il faudrait rechercher en cohérence avec les besoins anticipés de l'OTAN pour la connaissance du domaine spatial.

Observation : l'expérience technique et opérationnelle des différents pays de l'OTAN est inégale du point de vue de la collecte, du traitement, de la diffusion et de l'application des données du domaine spatial, ce qui entrave à la fois l'exploitation maximale et la préservation des capacités spatiales de l'OTAN.

Recommandation : étendre le partage du savoir-faire, des données et des expériences parmi les prestataires de capacité spatiale de l'OTAN, la communauté de S&T et les formateurs, planificateurs et opérateurs militaires de l'OTAN.

Observation : au sein de l'OTAN, il n'y a aucune expérience partagée de collecte, fusion et diffusion des données ou informations du domaine spatial susceptible de fournir une base de compréhension des défis et opportunités relatifs à l'obtention d'une situation opérationnelle commune du domaine spatial.

Recommandation : rechercher les occasions d'expérience et d'essai de terrain impliquant la collecte, le traitement et la diffusion de données et produits du domaine spatial, afin de faciliter une compréhension commune des défis et opportunités à venir au sein de l'Alliance.

Observation : l'intégration de la connaissance du domaine spatial dans la prise de décisions militaires opérationnelles et de planification est principalement limitée par le faible niveau technique opérationnel impliquant l'espace.

Recommandation : entreprendre, par l'intermédiaire d'éléments de S&T de l'OTAN, des analyses de modélisation et simulation de l'utilité militaire des diverses options de prise de décision impliquant la connaissance du domaine spatial, ainsi que l'exploration de solutions techniques permettant d'intégrer la connaissance du domaine spatial dans les opérations et la planification militaires de l'OTAN.

TECHNICAL CONSIDERATIONS FOR ENABLING A NATO-CENTRIC SPACE DOMAIN COMMON OPERATING PICTURE (COP)

1.0 INTRODUCTION

This report documents the work of the NATO Science and Technology Organization (STO) SCI-279 Task Group (SCI-279 TG) that addressed the technical considerations for enabling a NATO-Centric Space Domain Common Operating Picture (COP). The impetus for this effort is the growing dependence by NATO and its member nations on space capabilities to achieve its mission responsibilities as well as the growing role that space, as an operational domain is playing in matters concerning global security. NATO has recognized this important reality and increased the Alliance's collective attention on ensuring NATO operations maximize their leverage of space while ensuring the space capabilities provided by its member nations are preserved to the maximum extent possible. A critical element of ensuring the availability and efficacy of these space capabilities is the availability of a common operational perspective or picture of the space domain throughout the Alliance and its partners.

The presumption is that NATO forces will be more efficient, protected and successful in their future missions if a common operational picture can be achieved across all operational domains in which NATO must operate; air, land, sea, cyber AND space. Without a common Alliance perspective of the space domain, serious operational weaknesses may result when space services and capabilities are degraded or denied to NATO forces by either natural or man-made causes. With the rapid assimilation of information technology globally and associated applications to the modern battle space, it becomes imperative that NATO maximizes its total battle-space awareness to include the space domain.

A foundational role of the NATO STO collaborative technical activities is providing critical perspectives across the Alliance on the contributions (and threats) that emerging technologies will have on future NATO mission operations. Over the last several years STO has critically examined enabling technology developments and applications related to the ever-growing importance of space to the Alliance. One of the cornerstones of the Alliance has been pervasive interoperability in its materiel and non-materiel resources, assets and operations. It is apparent from those activities that, for NATO to sustain its strength through interoperability, then interoperability in the space domain must be considered as well. One of the intents of the NATO STO focus on space has been to identify intersections among plausible future NATO operational environments and emergent science and technology developments that can be leveraged to ensure NATO's success. This is the basis upon which STO has undertaken an examination of the enabling considerations necessary for a NATO-centric space domain Common Operating Picture (COP).

Space capabilities and services have been essential supporting utilities underpinning much of the command and control infrastructure throughout NATO for many years. However, the threats to those capabilities and services, along with the consequences of their loss or degradation, have only recently become a NATO concern given the proliferation of plausible threats and the growing dependence upon space throughout the Alliance. NATO has no space assets of its own – all space capabilities and services are of individual national origin. The protection of space systems (satellites and controlling ground infrastructure) that provide the capabilities and services to NATO is a singularly sovereign responsibility. In fact, not only the operation of those systems, but the collection/acquisition and dissemination of information on and about the space domain is also inherently sovereign in nature. Since space has become more important as a war fighting domain, this increasingly poses a dilemma for achieving the NATO objective of maximizing the interoperability and integration of force capabilities.

Historically, two of the more pervasive challenges of integrating multi-nationally sourced data and information that contributes to space domain awareness are: a) overcoming the national sensitivities of data sharing; and b) the accurate technical fusion of such data. Those challenges extend to the effective achievement of space domain awareness within NATO. For the purposes of this effort, a deliberate decision was made to NOT address the current and future policy remedies that will be necessary to deal with the sovereign sensitivity issues that must be overcome to achieve a comprehensive NATO common set of data and information on the space domain. However, it is posited that the following three types of data and information may be more likely to be shared than other more sensitive information (e.g., space-related intelligence):

- 1) Space object tracking;
- 2) Space environment; and
- 3) Radio frequency interference (as experienced by space communication links).

Thus, these three areas of space domain awareness are used within the SCI-279 Task Group effort as the exemplary pillars for characterizing an initial NATO-centric space common operating picture for space.

Since there is currently neither the capability for a NATO-centric space common operating picture, nor an established NATO requirement for one, the question of whom within NATO would be the future customers/consumers of such insight arises. For the purposes of this effort, the following two primary customer/consumer groups were postulated in a future NATO mission environment. The first are the NATO operational command elements which, having joint forces command responsibilities, are presumed to likely have some future need for insight into the space domain in order to effectively consider the Alliance space capabilities as well as to develop a proper appreciation of possible threats to them. A comprehensive and current space domain awareness is required in all phases of military planning through to mission execution and assessment. Providing the most comprehensive space domain awareness picture available to NATO commanders and operators is the objective in this case. The second are the national command elements of individual member nations providing national forces and resources to the NATO operational environment. In this case, providing a common Space Domain Awareness (SDA) picture across all participants in a NATO operation enables maximum common insight for individual command and control decisions by the nations involved.

2.0 SPACE DOMAIN AWARENESS

This section provides background on the anticipated future NATO Alliance need to have access to a common space domain awareness picture to enable successful execution of its missions. In addition, background is provided on the technical, materiel and non-materiel challenges that lie ahead for which solutions will be needed.

2.1 General Context

The underlying premise of the NATO Alliance is a system of collective defence wherein its members have agreed upon mutual defence in the event of an attack by any external party. The practical evolution of the Alliance's ability to effectively and efficiently enable collective defence has been to adopt standards and profiles that strive for seamless integration of defence systems and capabilities. NATO standards enable and encourage maximum interoperability as well as common basis for command and control. Of particular interest to the SCI-279 Task Group is the projected need for standards with respect to future NATO operations involving the space domain.

The NATO Alliance does not own space assets and is not anticipated to do so for the foreseeable future. The Alliance relies upon the space capabilities and services provided to it from member nations. Although all of

NATO uses space capabilities and services, presently only ten (10) members provide those services through their sovereign space assets. Additional services may be available to NATO from non-aligned nations and commercial entities. Consequently, there are several important implications of how NATO acquires its space capabilities.

NATO members that provide space capabilities and services to NATO operations are currently solely responsible for the protection and defence of their sovereign space assets. Some of those assets are intended, designed, and operated as national security systems. Others were intended and designed as civil or dual-use systems and thus not necessarily expected to be resilient within military operational environments. Thus, the national capacity and capability to defensively operate and protect those systems varies throughout the Alliance. This includes the ability to establish a comprehensive space domain picture. For example, the ability to track space objects potentially posing a risk to operational satellites is limited to only a few of the Alliance member states. However, all Alliance members owning, operating or using space systems have a need to understand the operational risk potential to those systems upon which they critically depend.

Use of and reliance upon space capabilities and services within NATO comes with an implicit responsibility to understand the general nature of the threats and vulnerabilities to those services as well as maintaining the capacity to operate effectively under degraded or denied services through whatever means available. Execution of that responsibility requires maximal knowledge of space domain and related operational environmental conditions. The ability to have forewarning of impending threats (predictive analytics) to space capabilities in use, even those provided by space assets owned by others, is essential in many projected military conflict scenarios. For the Alliance as a whole, the ability to have a shared awareness of the space environment and impending threats is essential to efficient and coordinated protection of critical NATO resources and effective response.

Historically, NATO operations have been minimally challenged or impacted by degradation, loss or denial of space capabilities. This is largely due to the lack of sophistication and technical capabilities of those adversaries NATO has actually faced in combat. However, the present-day situation has changed and, with the current capabilities and potential of future adversaries to have equivalent technical prowess and operational capabilities in the space domain, more emphasis must be placed on improving the preservation of NATO space capabilities. Furthermore, with the increase in the proliferation and assimilation of radically improved information technology intersecting the commercial, civil, and military elements of the space domain, more vulnerabilities are likely to be created.

The NATO Defence Planning Process (NDPP) Long-Term Aspect (LTA) on Space Capability Preservation was established to promote the identification and development of materiel and non-materiel solutions to *“preserve space capability / situational awareness for assets used by NATO through a combination of defensive measures of space and ground-based assets.”* The NATO STO was given the lead for the development and execution of a program of work to realize the objectives of this LTA. NATO STO issued a *“Framework for Addressing NATO Space Capability Preservation”* (AC/323-D(2013)0002) in which the eventual requirement for a NATO common space domain operating picture was postulated. This Task Group is an element of the NATO STO program of work consistent with that framework.

As NATO and national-level defence systems and military operations become more dependent upon comprehensive awareness of all relevant facets of the mission and battle space, the concept of common operating pictures has evolved to encompass not only tactically relevant awareness but also of the larger prevailing strategic context as well. Thus, the traditionally and narrowly defined tactical concept of space situational awareness is evolving toward becoming more inclusive of all facets of the space domain relevant to military and security missions. The term Space Domain Awareness (SDA), (analogous to maritime domain awareness, cyber domain awareness, and air domain awareness) captures the required broader operational context relevant to conducting effective space operations as well as preserving space capabilities from loss or degradation. The term Space Domain Awareness is used in that context in this Task Group.

The space domain can be defined as all conditions, areas, activities and things terrestrially relating to space, adjacent to, within, or bordering outer space, including all space-related activities, infrastructure, people, cargo, and space capable craft that can operate to, in, through and from space. Space domain awareness, in the NATO context, can similarly be defined as the effective understanding of anything associated with the space domain that could impact the security, safety, economy or environment of space systems or activities within the NATO Alliance. The definition acknowledges the supportive activities and threats related to land, maritime, air and cyber regimes relevant to space operations. It requires the combination of space situational awareness foundations of detecting, tracking and environmental monitoring, along with space intelligence foundations of characterizing normal behavior and sensitivity, to detecting change to know when something has or is predicted to occur. A purpose of SDA is to provide decision-making processes with a timely and actionable body of evidence of behavior(s) (predicted, imminent, and/or forensic) attributable to specific space domain threats and hazards.

Comprehensive operational awareness of the space domain is essential to the achievement of the NATO Long-Term Aspect requirement for NATO Space Capability Preservation [1] (as identified by the SCI-238 Specialists' Meeting, March 2013) [2]. To ensure that NATO forces, space planners and operators can maximize their deployment and protection of the space capabilities brought to the Alliance through its member nations, a shared Common Operating Picture (COP) of the space domain will be essential. Due to the multi-dimensional technical scope of the involved data and product streams along with associated variations in data protocols, sensor attributes and other technical variables, it will be necessary to evolve a common integrated environment within the NATO space planning and operational domains to ensure the timely exploitation of those data and products. Although there are no limits on what constitutes space domain awareness data, it is essential to initially address, at a minimum, space weather and environmental reporting, space object tracking and characterization/classification, as well as radio frequency interference characterizations and attributions against satellite control links and communication services.

3.0 THE THREE PILLARS OF SDA

Three areas of space domain awareness were considered by the SCI-279 Task Group effort for characterizing an initial NATO-centric space common operating picture. These three pillars are space object tracking and characterization/classification, space weather and environmental reporting, and radio frequency interference characterizations and attributions against satellite control links and communication services. There are other important contributing elements of space domain awareness important to NATO operations such as insights derived from terrestrial and space-based ISR into space operations support including offensive weapon deployment and use. However, due to sovereign sensitivities concerning sources and methods associated such space domain awareness elements they were not addressed in this activity. Even so, substantial value will accrue to NATO if an extensible approach to a NATO common space operating picture can be established with these three fundamental space domain awareness pillars.

3.1 Space Object and Tracking

To achieve a Common Operating Picture (COP) in space, the NATO Alliance must be able to, at a minimum, know where Anthropogenic Space Object (ASOs) have been in the recent past, as a nowcast, and will be soon (i.e., a forecast). In other words, the NATO Alliance must effectively have "Custody" of all trackable ASOs. Ideally, NATO should know this along with parameters that can successfully classify and uniquely identify each detectable space object. A minimum of six parameters are required to describe an orbit (e.g., three for position and three for velocity). However, this six-parameter state is insufficient to uniquely identify any given ASO, and only provides its geometric (kinematic) relationship with the Earth and any point of reference of interest. The general process of understanding the geometric relationships of ASOs with respect to each other and assets on Earth is called Space Surveillance and Tracking (SST).

As defined by the United States Strategic Command (USSTRATCOM) [3], space surveillance involves (but is not limited to) detecting, tracking, cataloging and identifying man-made objects orbiting Earth, which include active/inactive satellites, spent rocket bodies, debris, and fragments. Generally, U.S. space surveillance enables the following:

- Analysis of new space launches and evaluation of orbital insertion;
- Detection of new man-made objects in space;
- Determining the present position of space objects and their anticipated orbital paths;
- Production and maintenance of current man-made space object orbital data in a catalog;
- Inform manned space activities when objects or space environmental conditions may interfere with manned platforms;
- Prediction of when and where a decaying space object will re-enter the Earth's atmosphere;
- Prevent a returning space object, which to radar looks like a missile, from triggering a false alarm in missile-attack warning sensors of the U.S. and other countries;
- Determine which country owns a re-entering space object; and
- Predict surface impacts of re-entering objects and notify the Federal Emergency Management Agency and Public Safety Canada if an object may make landfall in North America or Hawaii.

To maintain knowledge on the population of Earth-orbiting ASOs, tracking observations are required. These inputs tend to come from physics-based sensors (e.g., radars and telescopes). Once these are collected, there must be algorithms which attempt to assign sensor ASO detections (tracking observations) to unique ASOs and do so with quantifiable measures of uncertainty.

Ideally, the tracking data are collected in a way driven by the need to maintain the most accurate trajectory knowledge possible on any given ASO. Current state-of-practice for the USSTRATCOM ASO catalog maintenance does not do this. Instead, the U.S. Satellite Surveillance Network (SSN) is tasked to provide a minimum set of observations per ASO per a set of user-defined importance criteria. The challenge is that this assumes all observations to be equally informative regarding the ASOs trajectory. If a user is provided with one million observations of an ASO in a Geosynchronous (GEO) orbit and all million observations are taken over the span of one minute, the first few observations will have the majority (~99%) of the information regarding the ASO's location and the remainder of the million observations will provide virtually no additional insight or knowledge. However, if the user is provided with one observation of an ASO at GEO every two hours, the 12 observations over a day will provide more detailed knowledge of the ASO's orbit than the one million over one minute. Technically, this is quantified in what is called the Fisher Information, which is computed by evaluating the sensor observation with respect to the kinematic relationship of the detected ASO and said sensor. In other words, the collection of tracking information on space objects, should in some measure be driven by maximizing the Fisher Information of the possible data with respect to any given ASO.

It is important to note that USSTRATCOM has developed and implemented the SST process and the SSN since the launch of Sputnik to achieve the above functions. As such it has been evolutionarily improved and does not represent the state-of-the-possible in terms of space surveillance capability. If one were to develop a new SST system, it would probably not look (or operate) like the current USSTRATCOM SSN. Part of the SSN system is a set of common analysis libraries and formats designed for ASO catalog maintenance and available to users of the SSN space catalog system. While these are important standards that could be the common basis for a NATO SDA system, additional data formats and analysis standards are required to integrate the broader base of space tracking and surveillance information and data available to the NATO Alliance that could be applied to the SDA mission. With modern open source libraries, like Orekit, and open format specifications like CCSDS there is a foundation from which one could build NATO standards that do

not require a “clean sheet” development effort or a government release process from one of the nation’s existing national assets.

Finding: Various members across the NATO Alliance have their own definitions of “space objects,” which events are operationally relevant, and each member state may have its own space tracking systems developed independently of other states. NATO lacks a *Lingua Franca* (i.e., Common Battle Management Language) required for a meaningful Common Space Domain Operating Picture.

Finding: NATO has no common definition or standard for uncertainty and ambiguity associated with the characterization of orbital objects in space.

Without loss of generality, tracking an individual in a population implies an ability to “tag” (read “uniquely identify”) the individual and monitor this individual through time/space/frequency with quantifiable ambiguity or uncertainty, evaluating the interaction of the individual with others and its environment. However, if an individual object cannot be physically tagged (or labelled) in a uniquely identifiable way, this poses serious limitations and challenges to comprehensive knowledge of man-made objects in the space domain. An example of this can be seen in Figure 1, in which the plotted points represent sensor tracking observations from the U.S. Space Surveillance Telescope. The plotted data represent actual sensor detections over a single night. This telescope can detect space objects in MEO, GEO, and HEO. There are two sets of plotted data, distinguishable by color. The black dots represent space objects believed to be previously known; in other words, the detections were assigned to unique objects. The blue dots are detections that are not correlated to known objects; in this case, detections for which we have no associated orbits nor for which we can say anything about their origin.

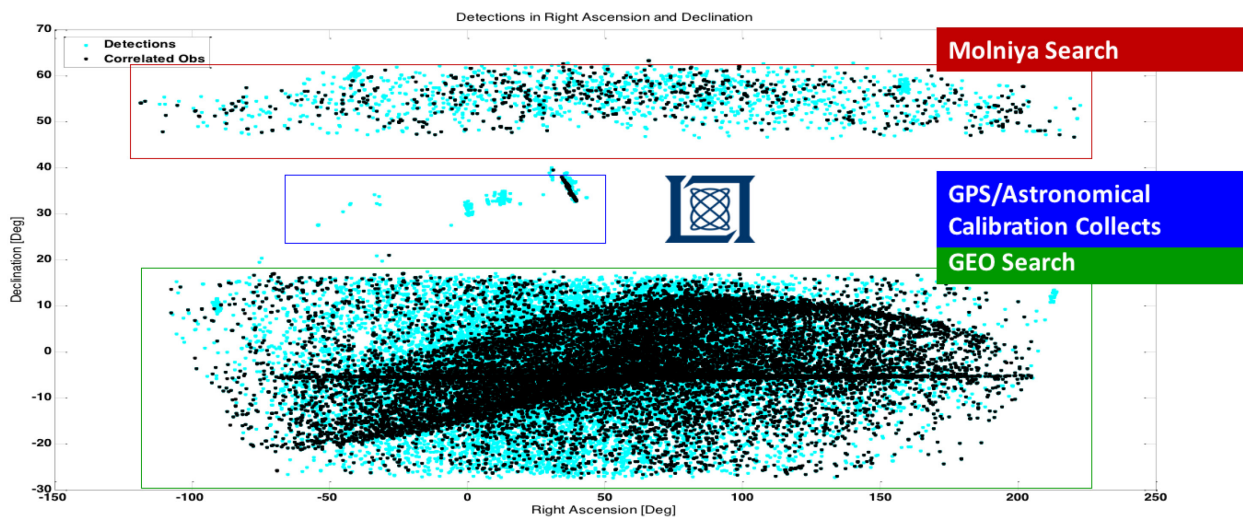


Figure 1: Correlated vs. Uncorrelated Detections from the Space Surveillance Telescope (SST).

Successful tracking of a space object means that one can identify this object (i.e., correlate sensor detections or inputs as having originated by unique space objects) with quantifiable and acceptable ambiguity and reconstruct and predict its behavior (usually referring to its location or motion). When this is constrained to the object’s trajectory or flight path, this process is more commonly known as orbit determination and prediction as shown schematically in Figure 2.

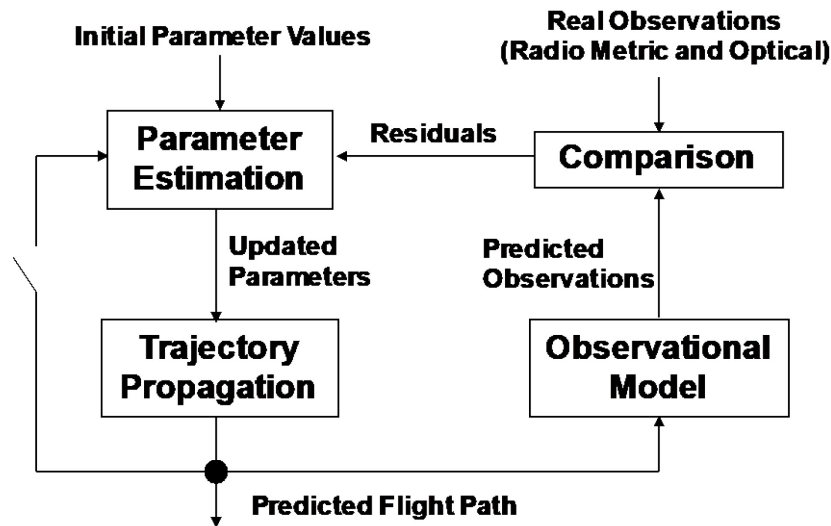


Figure 2: Orbit Determination Process.

Orbit Determination (OD) is the process of adjusting trajectory models to best match the observed tracking data, and quantify the error associated with the trajectory estimated. The collected tracking data are the actual or *Observed* measurements. The trajectory models produce predicted or *Computed* measurements. Then, what are termed *Data Residuals = Observed – Computed* measurements. The OD method typically aims to minimize the residuals by adjusting the trajectory models. These residuals are minimized in a weighted least-squares sense. The OD process accounts for measurement accuracies and accuracies with which parameters were known before taking measurements (a priori uncertainty). The OD produces:

- a) An updated trajectory estimate; and
- b) An estimate of error associated with current trajectory prediction.

The various forces influencing the motion of the space object must be understood [4].

OD, especially for uncooperative¹ space objects, requires scientific detective work. Successful OD requires the application of the scientific method as an ongoing process. The OD process is subjective in that the result is not unique given the large number of assumptions regarding the models used for characterizing the space environment, astrodynamics, and the sensors and observation system used to collect tracking and surveillance data. Moreover, results may differ depending on what states and parameters are estimated and the assumptions regarding their uncertainty.

Determining a space object’s orbit is typically easier than predicting what it will be in the future. In order to best predict an orbit, the OD process must not only reconstruct the trajectory of the space objects but also infer or refine key model parameters, both dynamic and non-dynamic. The only way to confidently understand a space object’s behavior and its interaction with the space environment is through the ability to accurately predict its behavior as corroborated by future observations. Gravitational perturbations to space object trajectories are well understood and quantified. They are the dominant source of perturbing forces and don’t depend on the physical characteristics of the space object itself, but rather only upon its location with respect to planetary masses (e.g., the Earth). However, there are other perturbations that are non-gravitational and these depend on the physical characteristics of the space object (i.e., size, mass, shape, material properties, orientation, etc.). In general, there is no a priori information on these physical characteristics and thus an effort must be made to infer these to improve trajectory predictions.

¹ Space objects whose motion and behavior are not under the control of the interested entity.

Non-gravitational forces and torques acting upon space objects all depend on space object characteristics (i.e., size, shape, material properties, orientation, mass) and modelling all space objects as spheres limits and prevents more accurate modelling and prediction of space object motion and behavior, which negatively affects space object detection, tracking, and identification. This is an important consideration when developing a common space picture. Although tracking implies both the ability to detect and uniquely identify a space object from location alone, is not sufficient to maintain custody of all anthropogenic space objects. Characterization of such object is also necessary.

Trajectory prediction involves accurately modelling and estimating all past forces and events associated with an object, as well as predicting all forces and future events. This includes the current *Estimated* trajectory error, as well as all future, or non-estimated errors that can also contribute. More specifically, there is a need to consider [5] the error contribution due to any uncertainty in model parameters that cannot be estimated in the OD solution. For maneuvering space objects, future powered events (via activation of onboard thrusters) are uncertain (even if predicted) and must be included as potential uncertainties that cannot be estimated (i.e., there is a random error in every thrusting event). Many times, the orientation, size, and material properties of the space object are unknown and their uncertainty should be considered upon the influence and uncertainty in the predicted trajectory as well.

It should be noted that a significant limitation to current state-of-practice in trajectory estimation methods for space surveillance exists because they are predicated on likely simplified assumptions including those used to quantify errors and uncertainties. For example, linearized assumptions and simplified astrodynamics modelling techniques that poorly account for stochastic effects and significant non-linear motion of space objects.

OD cannot be absolutely validated because the collected data do not have *observability*² into all components of state. There are several indicators of solution quality: Regarding quality of fit, are the Data Residuals mean zero with no systematic trends? Regarding estimated parameters, are estimates realistic, within a priori uncertainties? The solution quality can be trended by comparing various solution strategies that are:

- a) Data span dependent;
- b) Data type dependent;
- c) Sensor dependent; and
- d) Model assumptions dependent.

To arrive at a common space operating picture based upon disparate sources of information, a standard method to successfully gather, store, organize, manage, and exploit data must be defined, developed, and implemented. An example of a general data fusion model is the Joint Directors of Laboratories (JDL) model [6]. This has been extended to a Space Domain Information Fusion (SDIF) model [4].

Regarding current state-of-practice in fusing sensor data, a very limited insight on any given ASO is achieved because the ASO is only described by its orbital parameters and ballistic factor. For all intents and purposes, all ASOs are modelled as uniform spheres. This is insufficient to uniquely identify and describe any given ASO. Moreover, to maximally exploit all sources of information, any given ASO must be described with a set of parameters that are sensitive to the information collected. In other words, one cannot infer the orientation of an ASO if it is described and modelled as a sphere. Therefore, the set of parameters or Essential Elements of Information (EEIs) used to describe an ASO must be sufficient in quantity and sufficiently rich and diverse to allow for maximum information fusion and exploitation as well as space object identification.

² Observability refers to the information content in data with respect to a parameter we wish to infer.

It should be noted that the most common sources of error regarding the exploitation and exchange of sensor data tend to be found in unknown biases, error distribution, timing, coordinate/reference frame inconsistencies, and the formatting and representation of the data in terms of real significant digits.

The sources of information regarding space objects and events aren't limited to physical (hard) inputs but also include human (soft) inputs. These two sources are not mutually exploited for space, in an optimal manner. The field of Hard/Soft information fusion is still young. NATO has studied the development of a Common Battle Management Language that would facilitate this fusion and this should be leveraged and adapted for a Common Space Domain Operating Picture. The main value of the soft inputs is to provide context to the physical behavior being measured or observed with physical sensors and the ability to provide a richer description and interpretation of the sensor data being collected and exploited.

The ASTRIA program at The University of Texas at Austin [7] has begun to develop space object identification methods based upon biometric techniques and processes (called Biometric-Inspired Space Object Recognition – BISOR), and develop such things like ASO Fingerprints. ASTRIA proposes to have a three-step process that leads to space object identification: enrollment, verification, and identification as seen in Figure 3.

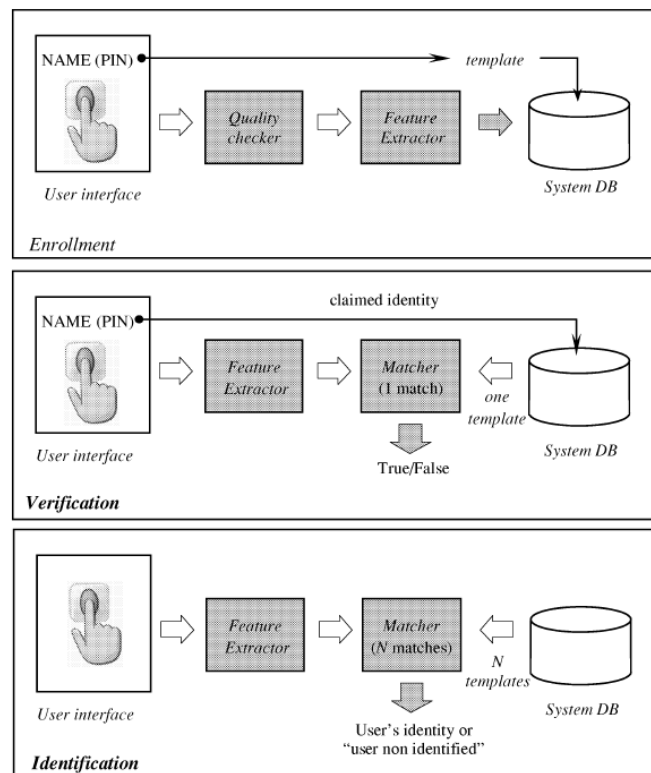


Figure 3: Biometric Identification Process [8].

As an example of an ASO Fingerprint, high-rate photometric data were recently collected on a few overhead passes of the Topex spacecraft (Figure 4). The goal is to find a common manifold upon which to map observed phenomena. One such manifold would be to map the observed phenomena to the ASO body frame. In order to visualize this, an ASO-centred celestial sphere is created and the observed RSPO brightness is associated to the ASO frame and then projected onto this unit sphere enclosing the ASO model. Once this is done, the sphere is made into a 2-dimensional so-called Mollweide Projection. The images in Figure 5 and Figure 6 demonstrate the results, and the reader will see that there are features common to both independent overhead passes.



Figure 4: Artist's Rendition of Topex ASO.

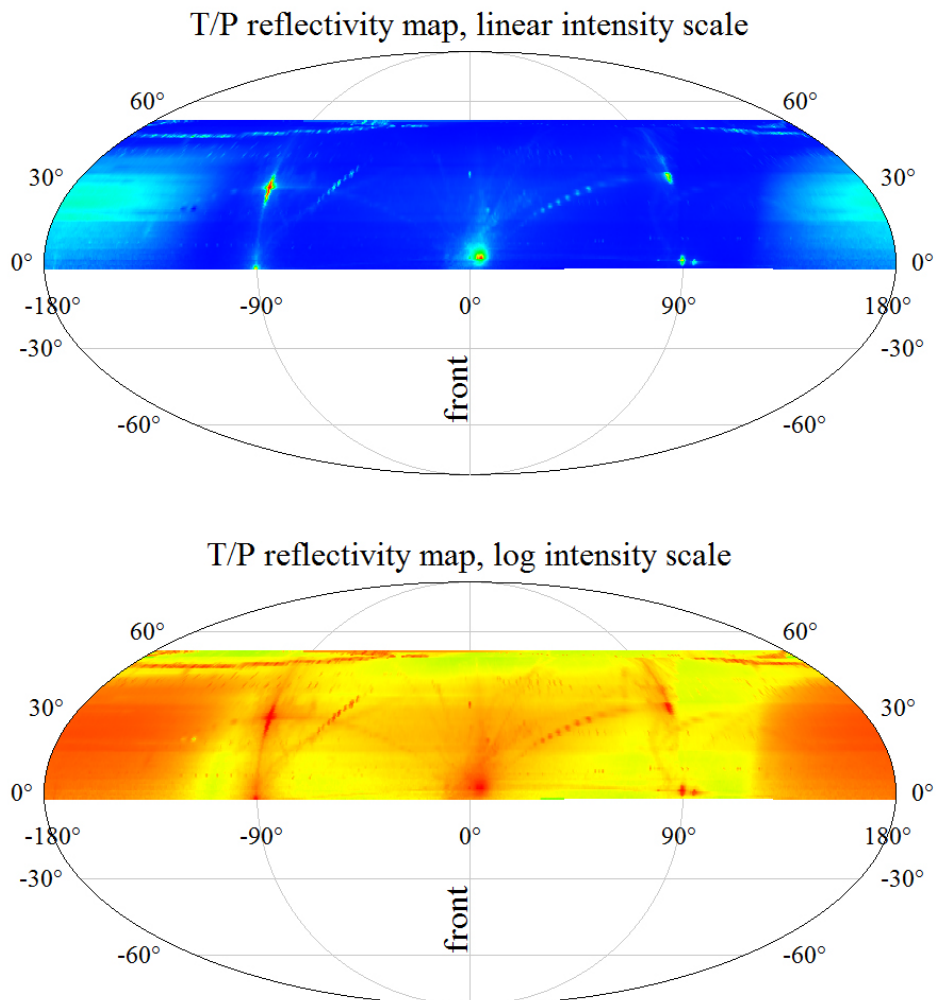


Figure 5: First Pass of Photometric Signature of Topex Represented in a Mollweide Projection.

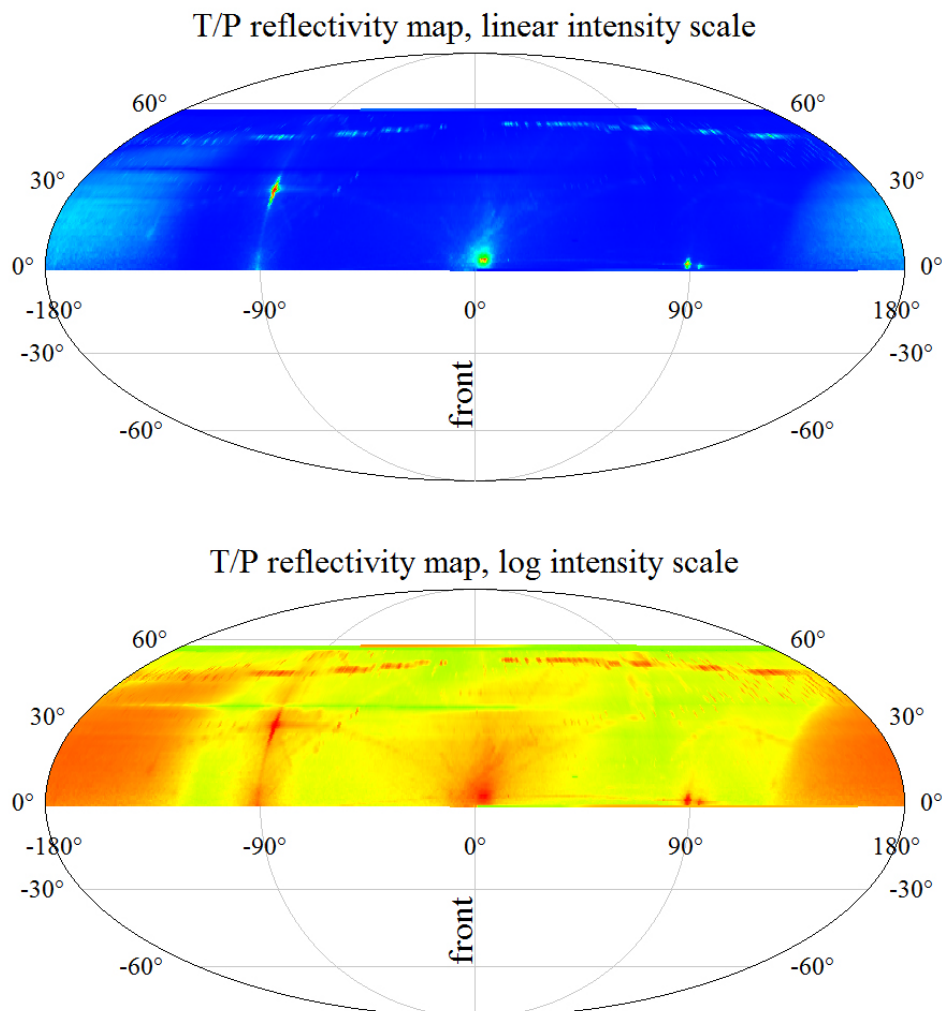


Figure 6: Second Pass of Photometric Signature of Topex Represented in a Mollweide Projection.

These are examples and there is still yet much to do in terms of the science and engineering of BISON.

The next steps required to make meaningful progress toward a Common NATO Space Domain Awareness Picture is to conduct field trials and experiments where actual data can be collected by NATO Alliance members and made into a common “data lake” where all participants can have access to the data, and infer as much as possible from the data set, then comparing results amongst each other. This will be a driver for NATO Alliance standards in SDA because these will need to be communicated effectively in order for the data exploitation comparison to make sense and be consistent amongst the participants. Statistical inconsistencies will indicate problem areas that need further analyses. Semantic inconsistency should lead to a common SDA vernacular and definitions.

3.2 Space Environment Effects and Impacts

Space is a dynamic environment that in many ways is radically different, often extreme and thus more challenging than what is experienced in the classic domains: land, sea and air. In order to achieve a space Common Operating Picture (COP), the Alliance must, at a minimum, have continuous access to sufficient relevant data on the space environment as well as sufficient analytical capability to model for the purposes of nowcasting and forecasting potential environmental impacts on space services and capabilities critical for

NATO operations (i.e., loss, disruption or degradation). The analytical capabilities should also support forensic analysis for attribution of cause as well as improving general understanding (i.e., expanding the science) of space environment effects on critical space services and capabilities.

Even though NATO does not currently own or operate space-based systems, its operations and activities are widely dependent on space services and capabilities such as communications, positioning and surveillance. The importance of understanding the space environment is to provide NATO planners and decision makers sufficient awareness of the possible effects on space services and capabilities to enable timely mitigation of such effects.

The main actors on the space environment stage are the Sun, the Earth's gravitational field, magnetic field, its atmosphere and radiation belts and galactic cosmic rays. The Sun affects its surroundings in two different ways: via emission of radiation and via charged particles. Besides visible light, the Sun also emits radiation with higher energy (ultraviolet light and x-rays) and lower energy (infrared or heat radiation and radio waves). Charged particles, mainly protons and electrons, are continuously emitted from the Sun creating solar wind that propagates throughout the Solar System carrying along the Sun's magnetic field.

Earth is surrounded by a magnetic field that is generated by the movement of molten material in the outer core of our planet. The Earth's magnetic field is affected by the solar wind, resulting in the magnetosphere's (the region of space affected by Earth's magnetic field) elongated shape (see Figure 7).

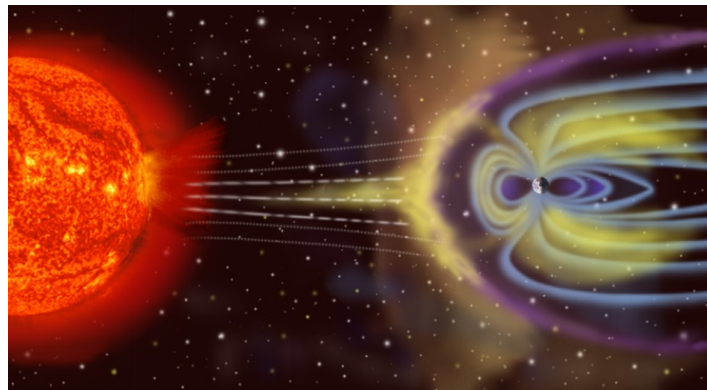


Figure 7: Earth's Magnetic Field Affected by the Solar Wind.

Within the Earth's magnetic field are regions where charged particles (again mostly protons and electrons) are trapped creating radiation belts (or Van Allen belts). The Earth's atmosphere consists of a number of layers as indicated in Figure 8. The layer closest to space is the thermosphere, which therefore can have a direct impact on spacecraft, whereas the lower atmospheric layers also can have an impact on the use of satellite services on the ground. Further elements of the natural space environment are energetic charged particles originating from outside our Solar System (Galactic Cosmic Rays), and dust particles and micrometeorites.

The main driver for most effects in the Earth's space environment is the activity of the Sun, especially changes in activity, which occur over timescales from minutes to years. Variations over shorter timescales (minutes, hours and days) are either due to changes in the density and speed of the solar wind or due to violent eruptions known as solar flares. Changes in the solar wind are caused by disturbances in the Sun's magnetic field known as coronal holes that can persist for days or weeks. The increased density and speed of the solar wind particles affect the Earth's magnetic field inducing a geomagnetic storm. Solar flares are very violent events caused by release of huge amounts of energy stored in tangled regions of the Sun's magnetic field much like energy in a tangled rubber band can be released by the band snapping.

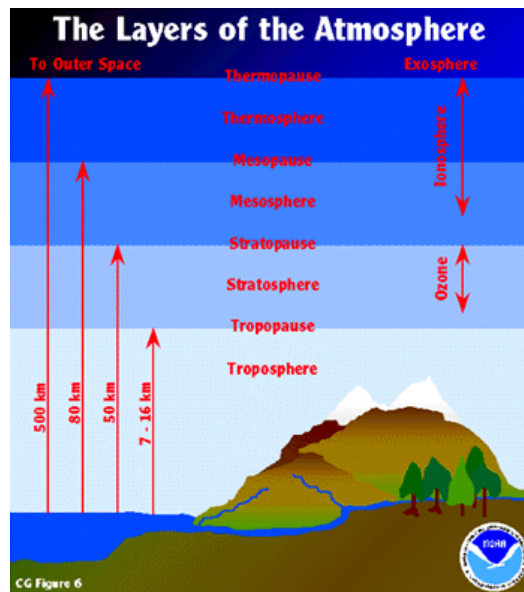


Figure 8: Earth's Atmosphere.

A solar flare causes several effects:

- Increase in high-energy radiation (ultraviolet light and x-rays);
- Release of a shower of high-energy particles (protons) travelling almost at the speed of light, termed relativistic protons; and
- Release of a huge cloud of charged particles (protons and electrons) travelling at a speed considerably faster than the average solar wind, termed a Coronal Mass Ejection (CME).

Further impacts on space systems are solar radiation drag, atmospheric drag due to increased solar radiation, direct and indirect particle events, surface charging and problems with orientation, communication and tracking of satellites. In relation to space surveillance and tracking, a decision maker needs an ability to discern between an active maneuver or drift due to natural effects (gravity, drift, drag). At the Earth's surface, events in the space environment may cause radar interference, degradation of HF communications and power blackouts.

The essential data needed to characterize the space environment are thus measurements of the radiation environment (both electromagnetic and particles) as well as measurement of the Earth's magnetic field. For the electromagnetic radiation, the focus is the high-energy radiation (ultraviolet light and x-rays) emitted by the Sun. Since this radiation is effectively blocked by the Earth's atmosphere, these data can only be obtained using spacecraft. Several operational spacecrafts are continuously observing the Sun e.g., the NASA/ESA satellite Solar and Heliospheric Observatory (SOHO) and NASA's Space Dynamics Observatory (SDO). These satellites will be the first to observe solar flares and changes in solar wind. Furthermore, they provide data to predict solar flares by observing the active regions on the Sun (e.g., sun spots) optically.

Finding: Data from solar observation satellites about high-energy solar radiation can be used to predict space environmental effects.

Earth observation satellites such as ESA's SWARM mission obtain data about the Earth's magnetic field and changing magnetospheric conditions resulting from variations in the solar wind and solar flares. Another satellite commonly used as information source for space weather services is the Geostationary Operational Environmental Satellite (GOES-12/13). Ground-based sensors, in combination with space-based sensors, are

mainly used to observe atmospheric conditions, like the Total Electron Content (TEC), which is an important input for scintillation modelling relevant for propagation of GNSS signals. The models and statistical tools needed to analyze space environment data and predict operational impact are discussed in Appendix 2.

Finding: Data from Earth observation satellites about changes in magnetospheric conditions can be used to predict space environmental effects.

Finally, operational impact can be measured directly, by using the equipment itself as a sensor. For example, GPS error or SATCOM signal degradation, can be used to verify or as input for forecasts. Also, since orbit determination becomes more and more precise, space weather effects like solar radiation are derived from satellite drag and scintillation from GPS like SCINDA or DLR's high-rate GNSS measurement network. These in situ measurements are required for establishing baseline performance.

Finding: Operational impact of space environmental effects can be measured directly by the impacted hardware.

Finding: Measurement data of space environmental impact at hardware can be used to establish baseline performance and verify forecasts.

To pave the way for a Common NATO Space Domain Awareness Picture, a natural next step would be to evaluate the relevance of space environment data and analysis tools available now and soon to establish a data baseline. Many data products are publicly available or may be made available through proper agreements with NATO Alliance members or partners. It is however important to ensure reliability of data delivery as well as data completeness and compatibility. Given a space environment data baseline, the next step would be to test data fusion to disclose any adverse effects resulting from such a process. Here obviously, data standards, sampling rates and completeness of data are issues to be investigated. If data are not fused properly the reliability of the prediction may be affected. Following such an effort, the next steps would be a set of field trials and experiments, perhaps to coincide with major NATO exercises to explore how space domain awareness can support NATO operations.

3.3 Radio Frequency Interference

Radio Frequency Interferences (RFI) are the most likely source of disruption to telecommunications to NATO operations. RFI equally impacts both ground and space-based communication links. RFI disruptions can affect two critical NATO space capabilities: satellite-based telecommunications and Global Navigation Satellite Systems (GNSS).

RFI can be categorized as unintentional (including environmental) or intentional (generally referred to as "jamming"). Their impacts can range from disrupting the service level via a degradation of capability such as accuracy, availability, and timeliness to include a total denial of service. This can lead to local, regional, or total loss of capability of the NATO functionality and satellite service availability. Space RFI effects fall into four broad categories:

- Interference involving signals sent from a satellite to one or more terrestrial receivers (i.e., downlinks);
- Interference involving signals sent from terrestrial transmitters to a satellite (i.e., uplinks);
- Interference with signals transmitted from one satellite to another (i.e., crosslinks); and
- Interference involving signals sent from terrestrial transmitters to one or more terrestrial receivers (i.e., ground links).

There are several RFI mitigation techniques available, if NATO can forecast the threat or identify the source of the interference. At present, most space RFI involves downlinks and uplinks of Satellite Communication

(SATCOM) networks as well as interference with the downlinks signals transmitted by Global Navigation Satellite Systems (GNSS). Knowing the location and nature of potential sources of RFI enables NATO military planners and operators to adjust their activities accordingly.

3.3.1 Sources of Radio Frequency Interference

3.3.1.1 Unintentional Human Error

Most interference affecting satellite communications occurs due to unintentional human error. There are four types of human errors that can occur:

- 1) Operator error;
- 2) Poor equipment installation;
- 3) Poor system engineering; and
- 4) Poor equipment maintenance.

Operator errors normally occur at the start of a transmission, and this is the reason for the generally established procedure referred to as the Pre-Transmission Line Up (PTLU). The PTLU establishes that the transmission occurs according to the technical specifications for that transmission, generally referred to as the transmission plan. This entails checking that the transmission is being made to the correct satellite, with the correct frequency and polarization; the PTLU continues on to verify that the transmit power to the satellite and that the signal bandwidth are both correct. The PTLU is also the occasion that the satellite operator takes to ensure that the ground station is registered and that registration information includes around-the-clock point of contact information for operations crews. If the PTLU procedure is not executed for any reason, interference to other satellite services can occur.

Poor equipment installation can sometimes be detected at the moment of the PTLU; however, it can include poor cabling, which can introduce interfering terrestrial RF sources into the transmit chain which may be subsequently uplinked to the satellite alongside the legitimate signal. Simple things such as the antenna being inadequately anchored or fixed can result in interfering with another satellite links.

Poor engineering can involve several situations resulting in RFI. For example, limited budgets can encourage cheaper equipment to be deployed. Deployment of poor reflectors or antennas which then radiate higher than acceptable levels of signal to adjacent orbital positions or the under-dimensioning of amplifiers that result in intermodulation noise being transmitted to the satellite.

Poor equipment maintenance includes such things as failure to perform periodic maintenance (e.g., cleaning filters) that can lead to equipment degradation or failure resulting in unwanted RF transmissions.

3.3.1.2 Adjacent Satellite Interference

Adjacent satellite interference is generally accidental and results from poor inter-system coordination or user error in antenna pointing. Interference caused by adjacent satellites is becoming more prevalent as the geostationary arc becomes more crowded. Mitigation requires good planning and correctly specifying and deploying user terminals; for example, orienting the terminals to point to the correct satellite and ensuring that the terminals use sufficiently narrow, high-performance beams.

Adjacent Satellite Interference (ASI) is caused under two situations, on the uplink when signals intended for one satellite also arrive at an adjacent one, or on the downlink when signals from a satellite are 'seen' by terminals receiving service from an adjacent satellite. There are two factors affecting Adjacent Satellite Interference, firstly, the orbital separation between two satellites using the same frequencies in the same geographical area, and secondly, the size of the antennas used for either transmitting or receiving the

services. The cases of ASI are increasing due to changes in both these domains, the satellites are getting closer together, there are more of them, and user demands towards smaller antennas. Added to these, which is particularly relevant in the military domain, is the use of antennas on mobile platforms and high demands for bandwidth from multiple satellites, often close together, in specific geographical zones, often referred to in the community as theatres. A lot of work is being put into coordinating, even between competing satellite operators, to minimize the occurrence and the effects of these types of interference.

- **Terrestrial Interference:** This describes the type of interference where terrestrial sources are either picked up by the satellite or where they impact on the reception of satellite signals by the terminals. Terrestrial RFI to SATCOM networks can be caused by a variety of means, including existing terrestrial microwave systems, new microwave systems that have commenced service following deployment of the satellite, and civil or military radar systems used on land, sea, and air platforms. Inter-system frequency coordination procedures, pursuant to the International Radio Regulations, are designed to address this issue. WIMAX causes impact to C band systems causing the satellite signals to be overcome the much higher levels of local WiMax terminals. A form of deliberate interference has been anecdotally noted and is caused by the deliberate transmission of high-power signals at specific satellite receive frequencies to block their reception, this is currently believed to be common in particular hostile countries.
- **Equipment Failure:** Equipment failure can cause uncontrolled and unwanted radio emissions. Poorly designed terminals, instead of shutting down in their failure mode, can continue to transmit signals, causing interference. Equipment failure can be managed through better design, planning, systems management, operator training, and maintenance.
- **Purposeful Interference:** Purposeful Interference (PI) can include actions to intentionally jam, block or interference with satellite services. These can include GNSS “jammers” which can degrade or disrupt Positioning, Navigation And Timing (PNT) services used by civilian and military users [9]. Such systems can be used by governments around key facilities to degrade the accuracy of unmanned aerial systems and precision guided munitions [10]. PNT jammers also can be used by individuals to frustrate commercial tracking applications, which can result in inadvertent interference to navigation and computer networks [11].

PI of SATCOM uplinks be geopolitically motivated and exceptionally rare; however, its effects can be significant. In the cases of PI observed over the past decade, an important step to mitigate the issue includes rapidly locating the source of the jamming signal(s) so that appropriate measures can be initiated at the government-to-government level to resolve the situation, such as the use of International Telecommunication Union procedures or bilateral approaches. Jammers can employ several strategies, including mobility, to thwart mitigation.

Finding: A NATO common operational picture of RFI incidents must consider a wide range of potential sources and factors, including human error, equipment failures and purposeful interference.

3.3.2 Mitigation Measures

Overall, there are several mitigation options, depending on the type of RFI to address:

- User training and certification;
- Equipment maintenance to eliminate a possible source of interference source;
- Use of filters, grounding and shielding equipment;
- Ad hoc frequency use;
- Geolocate the source and report; and
- Use of type approved antenna systems.

Traditional communications satellite systems employ large footprints that may cover wide regions or even continents. Low-power or infrequent jammers may seek to distort the user's data to reduce effectiveness or trust in the system; this can be difficult to differentiate from unintentional interference. At higher powers, a more overt jammer can saturate key satellite components so that the desired signal is essentially eliminated altogether.

3.3.3 Maintaining an Operational Picture of the RF Environment

To understand the RF and RFI environment, knowledge of what are the normal and abnormal elements of that environment is required.

There are two elements required to build knowledge of the actual or normal situation in the RF environment. The first is to understand what the expected situation is, in real terms this means for the operator of a communications satellite to have a traffic plan of the RF spectrum. The second is the means to monitor and verify that this traffic plan and satellite infrastructure upon which it depends is available for supporting this plan.

With this knowledge, it is necessary to understand what contributing factors may affect the two points above; this can extend from simple factors such as poor local weather conditions through to complete satellite failure or a deliberate jamming or denial of service attack.

3.3.4 The Traffic Plan

Commercial satellite operators maintain a tight control on the way that the communication payload resources on their satellites are operated and managed. The RF bandwidth and power are allocated to users of the satellite based on commercial agreements, the most common way of allocation is for a fixed frequency measured in Hertz a fixed bandwidth, also in Hertz and a power level, normally measured as the Estimated Isotropic Radiated Power (EIRP) measured in dB Watts.

These traffic plans are normally managed by specific software packages, either in house or commercially available that allow these plans to be constructed.

Other additional elements which are required to construct the plans include information on the transmit systems, antenna sizes, amplifier powers and locations in order to construct link budgets, but also to respect regulatory, coordination and regional limits and conditions.

The traffic plan must provide the operator of that communications satellite RF payload with a complete picture of what is normal and abnormal. Any abnormality or excursion from that nominal situation will need to trigger a process that will restore the nominal situation.

The operator of a communications satellite will provide the user with a transmission plan that defines the technical parameters of the transmissions that the user will be transmitting or receiving from the satellite.

3.3.5 Monitoring the RF Environment

To be able to have knowledge on whether you are in a normal or abnormal situation in the RF domain, a means of measuring and monitoring this environment is required.

Most communications satellites operate in a range of microwave frequencies from 2 to 30 GHz. They operate within limited geographic regions based either on the visibility of the satellite from a given point on the Earth's surface or by the use of antennas directing the RF signals to geographic regions on the Earth's surface. Satellites may have multiple frequency bands and geographic coverage regions. In order to maintain

a complete knowledge of the RF operational situation on a communications satellite, sufficient monitoring facilities, potentially on multiple geographically dispersed sites, will be needed to alimnt this knowledge.

In today's environment, it is becoming increasingly necessary to have knowledge of the RF environment beyond that which a single entity controls. Geostationary satellites share common frequency bands and operate in orbital slots in the geostationary arc that are sometimes at less than 2 degrees of spacing.

To maintain the knowledge of the situation most entities operating communication satellites use commercially available monitoring and control systems that control monitoring devices connected to antennas to measure the RF spectrum and compare the measured information with the nominal situation provided by the traffic plan. These systems make continuous measurements to quickly detect excursions from the traffic plan so that processes aimed at restoring the nominal situation are activated.

The monitoring of the RF environment is also a means of ensuring that the communication satellite is operating according to its nominal status, anomalous events may occur on the spacecraft which affect the services that it provides, the monitoring provides a means of quickly assessing to impact of this type of event.

Beyond the monitoring systems that allow for a knowledge of the environment, additional means or tools that allow for a more detailed picture to be built up, these are most often used as means of analyzing anomalous situations. These include the following tools:

- 1) **Satellite Telemetry** – Used to assess the operation of the satellite and its subsystems, but can also be a useful tool to provide supplementary information on the operation of elements supporting the delivery of the RF services; these include input power levels or drive to amplifiers, for example.
- 2) **Signal Characterization** – For determining modulation and coding types and potentially extending to identification information that is contained within the signals, in DVB headers, for example.
- 3) **Geolocation Systems** – Used to generate the location of a source of transmission of a signal. These can be systems hosted on board the satellite, or are ground-based systems.

To achieve the fullest possible operating picture, the more data in the pool the better, whether this is within the context of a commercial satellite operator or a military mission. There is a growing motivation, more specifically linked to working in a limited physical electromagnetic environment, to share, collaborate and coordinate to maintain the operational domain. Non-governmental entities, such as the Space Data Association (SDA), are working towards having systems that can do this securely and efficiently, allowing competing entities to have access to enough information from others to allow them to resolve their interference issues, for example.

Finding: RFI affecting space services can be mitigated by operator planning and monitoring tools; collaborations among multiple operators can support improved RFI detection, geolocation and characterization.

Finding: Collaborations between NATO Allies, governmental agencies and private sector activities can help to advance a common operating picture to facilitate resolution of RFI incidents.

Within the context of NATO, efforts to develop a Common Space Picture could include direct participation by Allied governments in non-governmental entities to exchange information involving RFI incidents involving civil government and commercial SATCOM systems. These exchanges could be complemented by a parallel government-to-government collaboration constructed around similar principles to share classified data regarding RFI issues and threats relating to military satellite communications networks.

Collaboration between commercial, civil and military systems for RFI detection, geolocation and characterization could be facilitated by the pooling of data and analyses to allow for comparisons of

conclusions. The effectiveness of such pooling is directly related to the amount of data shared on SATCOM as well as radars and other potential RFI sources. A certain amount of RFI prediction is possible on newer commercial systems, but this is limited to evaluating the configurations in the system and highlighting specific hot spots where inter-system interference is likely to occur. As a result, user discipline and a firm set of guidelines for pooling data would need to be developed and followed.

Multi-system collaboration on RFI detection, geolocation and characterization would also need to consider issues associated with ensuring consistency between multiple data sets, especially in the case where RFI incidents arise involving governmental and private sector spacecraft. A second concern relates issue of data security, specifically the issue of releasing high-fidelity RFI geolocation and characterization data associated with certain USG and Allied government payloads to third parties. These issues will require careful consideration as part of the development of any pooling arrangements and other Alliance collaborations.

4.0 CHALLENGES OF CREATING A COMMON OPERATIONAL PICTURE

This section addresses the net technical challenge of establishing a NATO common space domain awareness operating picture that fully leverages the information provided to it from its member nations to support both the NATO command structure as well as providing the same picture throughout the Alliance. To accomplish this, it must clearly involve significant institutional and policy accommodations throughout NATO. Some of the more important bridges between the projected technical requirements and those non-materiel accommodations will be highlighted, but it is beyond the scope and expertise of this Task Group to address much more. This section is organized along the following thread of thought; first a discussion of what it means technically to implement and sustain a common operating picture followed by a discussion of the architectural concepts that might be usefully applied to this challenge. Since common operational pictures are essentially organized pools of information and data that are sensitive and presumably yield a military advantage, the issue of information security is then discussed. NATO during peacetime is largely about ensuring common, interoperable capabilities, both materiel and non-materiel which is largely managed through the issuance of standards as well as NATO-wide training exercises. In a similar manner, the need for standards to achieve effective space domain awareness throughout NATO is addressed. Finally, the NATO efforts to address a similar challenge associated with sharing a common, fused ISR picture is discussed in the context of the Joint Capabilities Group for Intelligence, Surveillance and Reconnaissance.

Creating a Common Operational Picture (COP) is challenged by conflicting objectives and constraints. This can be expected in the development of a NATO common space domain awareness operating picture. The definition of common operational pictures varies but can be characterized by the following Wikipedia definition:

A Common Operational Picture (COP) is a single identical display of relevant (operational) information (e.g., position of own troops and enemy troops, position and status of important infrastructure such as bridges, roads) shared by more than one Command.

A Common Operating Picture (COP) offers a standard view, thereby providing information that enables the command decision makers and any supporting operational commanders to make effective, consistent, and timely decisions. Compiling data from multiple sources and disseminating the collaborative information ensures that all responding entities have the same understanding and awareness of the complete situation and circumstances when conducting operations.

For simplification, this Task Group report only addresses a Space COP to be used by NATO decision makers. One could also consider a User-Defined Operational Picture (UDOP) in which the user selects what

information should be included or excluded from the data picture. As such, a specific user would only be visualizing information for specific needs, as opposed to the COP being used for situational awareness of the big picture and making decisions from that information.

The implementation of a true Space COP has proven to be a difficult venture for those countries who are forging the path to information sharing in the space domain.

The Canadian Department of National Defence (DND) recently approved a Space Common Operating Picture (COP) task in one of its Defence Research and Development Canada's (DRDC's) Space Operations Projects. The intent of the task is to improve Space Situational Awareness through the demonstration and delivery of concepts and techniques and as such, enabling decision makers and operators with the ability to visualize information from the space domain, and use the information to assess risks and determine possible courses of action. During initial research into what technologies and capabilities currently exist for a Space COP, it was evident that the focus in industry still lies only on the real-time information available, such as information on orbital objects and conjunction predictions. Real-time information could also include ground systems, threat vectors, terrestrial clients, space weather and events [12], information which has not yet been integrated in industry's COP applications.

As mentioned in Section 3, the three main pillars of SDA (in this document) are Space Surveillance and Tracking, Space Environment and Impacts, and Radio Frequency Interference. With the amount of information that could be used in a Space COP, even considering only the three SDA pillars mentioned, that amount of information could possibly inundate decision makers, making it difficult to decide upon the appropriate actions to be taken and ultimately, making the information ineffective. As such, it was also evident that the more important factors for a Space COP are information fusion of Big Data and how those Big Data would be fused in an effective architecture and visualized, interoperability, data models, and decision making tools [13]. Decision-making tools could help analyze real-time data and consider using machine learning to detect anomalies in behavior and alert the decision makers to events as they occur.

4.1 Space Domain Awareness and Big Data Science and Analytics

What follows are general concepts taken from the Big Data Science, an Analytics community that is recommended to NATO to use as a foundation for Space Domain Awareness and creating a Common Operating Picture.

In general, one is interested in information acquisition, organization/management, analysis/exploitation, and decision making (Figure 9).

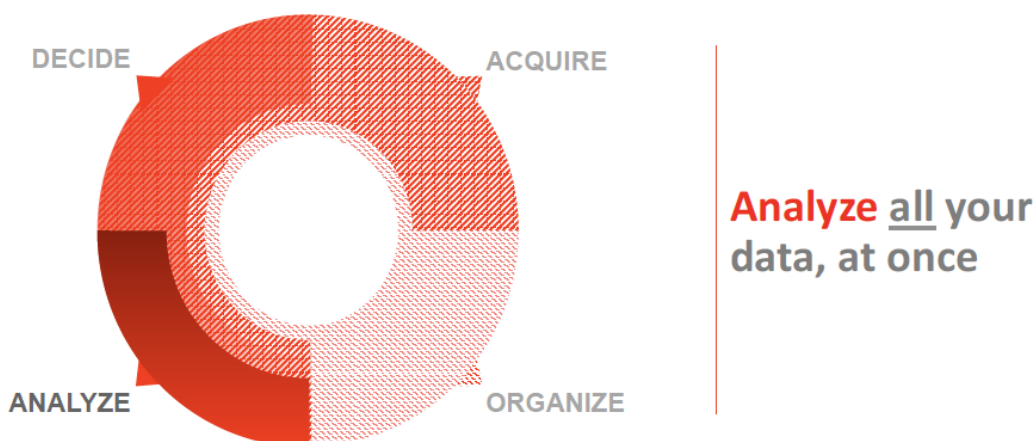


Figure 9: From Information to Decisions: Image from Oracle Online Presentation [14].

A key tenet of Big Data is to analyze all sources of information simultaneously, so as to get the maximum mutual information on desired space domain awareness criteria and enable going from Data to Discovery. A “best practice” in organizing information is to do so in an ontology-based knowledge graph, leveraging a so-called schema. The basic structure of this schema is a semantic connection with nodes being entities and the edges (or lines) being “directional” relationships. An example of one such schema implemented currently in ASTRIAGraph is shown in Figure 10.

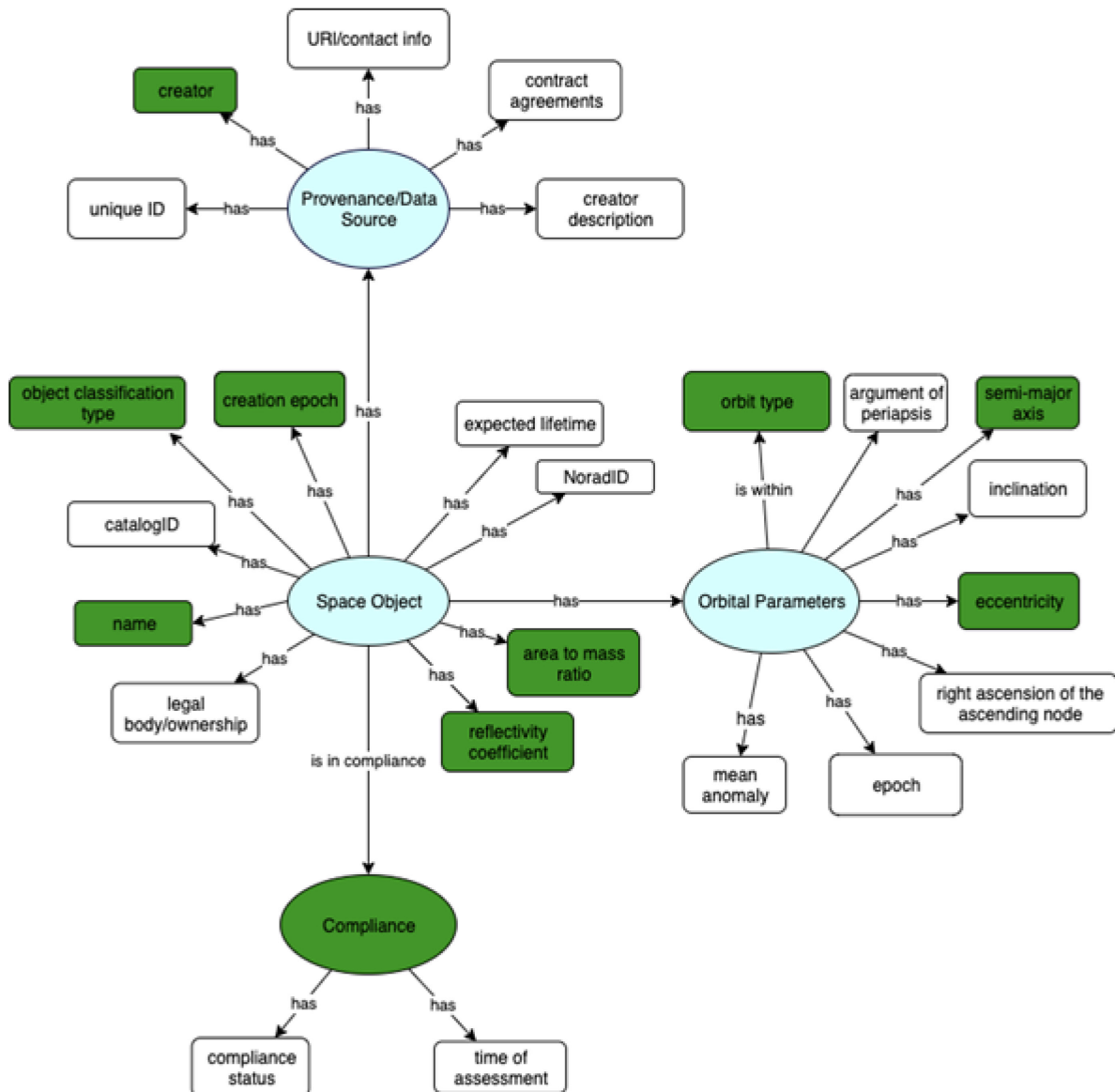


Figure 10: Schema Implemented Currently in ASTRIAGraph [15].

The power in organizing information in this semantically connected fashion is that it enables linking disparate sources of information, creating vast trees of descriptions of many different elements and encouraging “discovery” from data linking. This schema has been successfully implemented to enable the assessment of which ASO owners/operators are compliant and non-compliant with GEO disposal guidelines (ref: <http://astria.tacc.utexas.edu/compliance>). Multiple sources of information are ingested, modeled, curated, and exploited to make this assessment.

The schemas are used in a graph and are a middle layer in a holistic SDA framework. The information one would use gets acquired via a variety of methods and sources into so-called “instances,” as seen in Figure 11. These can be structured (as what comes from sensors) or unstructured (as what could get reported by humans online, via tweets, etc.). The desire is to have automated processes that are always acquiring information and storing them as instances. The information acquired would have a so-called “landing zone” with metadata generated to provide a timestamp on this process. The information is stored as is and absolutely no changes or alterations are made to any instance data. The data are in their “raw” or acquired form.

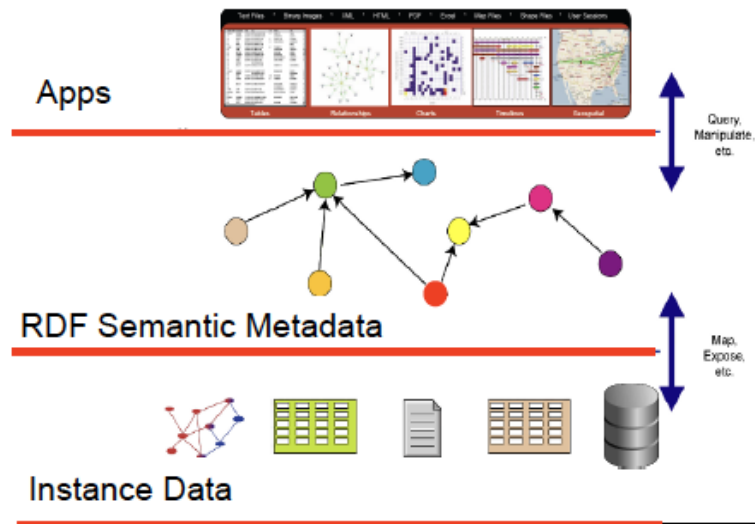


Figure 11: RDF-Based Big Data Framework [14].

There must be a separate process that takes the information from the instance data and maps these into the schema according to an agreed upon standard and semantically consistent vocabulary. The knowledge graph should also have a dictionary or thesaurus that can be readily accessed by those who would interact with the schemas. Given the international nature of the desired COP, cultural competency is desired in defining the schema vocabulary where the user is not asked to or forced to know this vocabulary but the schema developers have established which country and sector specific terms map to which schema entities, somewhat like a translation service.

The Knowledge Graph is where the current knowledge of the Space Domain resides, with descriptions concerning all of these elements of information. The way in which the information within the schema can get updated or reconciled given evidence is via the top layer of applications that run or perform queries on the schemas. One can envision one application being Space Object Orbit Determination and Prediction, for instance. One application should be validating the schemas’ data for semantic, physical, and statistical consistency. Related content and relations can be discovered by navigating connected entities, reasoning across these.

Figure 12 shows an example of the various functions that come together to go from Data to Discovery with this Big Data framework. The “customers” can be exchanged for “space objects.” The demographics for a space object can be defined as its characteristics (physical, operational, functional, kinematic, ownership, etc.).

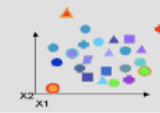
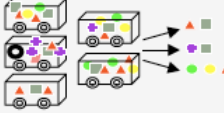

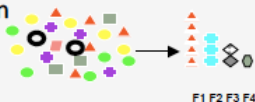
Problem Classification	Sample Problem
Anomaly Detection 	Given demographic data about a set of customers, identify customer purchasing behavior that is significantly different from the norm
Association Rules 	Find the items that tend to be purchased together and specify their relationship – market basket analysis
Clustering 	Segment demographic data into clusters and rank the probability that an individual will belong to a given cluster
Feature Extraction 	Given demographic data about a set of customers, group the attributes into general characteristics of the customers

Figure 12: Examples of Big Data Analytics [14].

Knowledge graphs are still in their infancy and it remains to be seen if they can be made to be relevant to a Space COP. Some salient research issues involve how to make the schema able to handle dynamic information which in turn may be uncertain or random. Not many know how to perform queries. There must be some competence in mapping Instance Data to the schema framework. A vocabulary and dictionary must be developed. As can be seen, there is much yet to be done to make this into a near-real-time, robust, and resilient architecture that could underpin a NATO Space COP.

A real-world example has been developed by Prof. Moriba Jah at The University of Texas at Austin, and it is called ASTRIAGraph, which can be visualized here: <http://astria.tacc.utexas.edu/AstriaGraph>. The current capability of ASTRIAGraph is as follows:

- Various sources of “Instance Data” are autonomously retrieved online and deposited into a “landing zone.”
 - Both Industry and Open Source.
- Relevant information from “Instance Data” are autonomously mapped into the schema.
 - Apps update the schema.
- An App autonomously queries the RDF Triple Store, retrieves observational data, and processes these to yield an informed orbital estimate product, and updates the appropriate schema entities.
 - Currently all Planet Flock Cubesats are processed autonomously, daily, along with Iridium 64.

4.2 Architectural Concepts for a Common Operational Picture

Since space data are disparate and complex, a Space COP will require several layers in order to effectively fuse all relevant and suitable incoming data at the appropriate levels of fusion, process them and organize them such that the decision makers can effectively visualize the entire space situation and determine courses of action if it is determined that there is a risk of loss, degradation, or disruption to space services, capabilities, or activities. Examples were discussed in the previous section.

Similar to maritime data, space data needs to be turned into understandable and actionable information. One company’s information model [16] uses real-time maritime data (such as Automatic Identification System

(AIS) messages, container information, and oil and gas industry databases) as its base layer for data inputs. It then takes the real-time data inputs, processes all types of data, fuses them and analyzes them into a metadata layer. The company then uses machine learning to determine normal shipping lanes and normal ship behavior at sea and near/in harbour and provides anomaly detection to the clients (such as when a ship veers from its predicted and normal approach to harbour).

Figure 13 shows an example of how Maerospace, a Big Data company, gathered maritime data and then, through a layered approach, integrated, synthesized and processed that data to provide a useful visualization of that data for the operators (Figure 14).

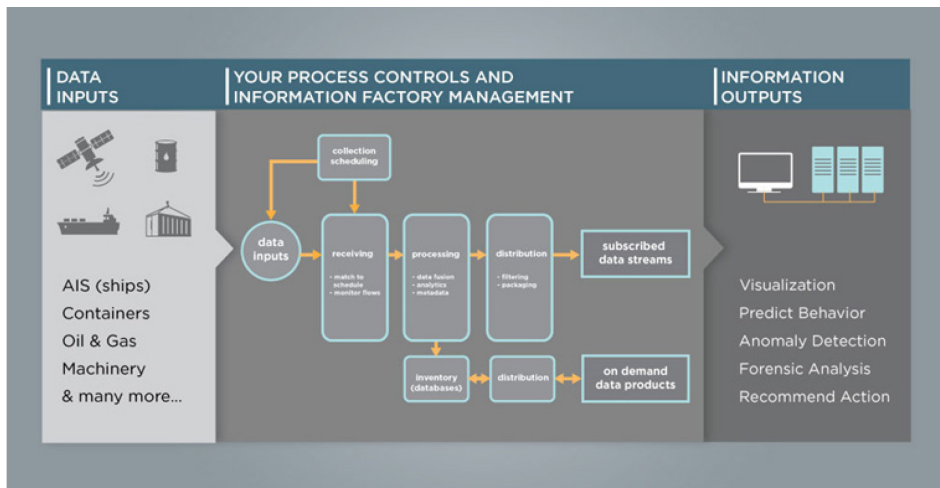


Figure 13: Data Fusion. Data is gathered and fused into an operational picture [16].



Figure 14: Local Maritime Operating Picture.

In Project Eyes on the Seas, various sources of information help to create a layered view of fishing-related activity.

Project Eyes on the Seas also provides a good example of maritime data being synthesized and analyzed, in a cost-effective and efficient way, to address problems related to ocean governance, enforcement, and

monitoring [17]. To monitor illegal fishing, Project Eyes on the Seas combines satellite monitoring and imagery data with fishing vessel databases and oceanographic data to detect suspicious fishing activity. Information is gathered from the Automatic Identification System (AIS) for vessel tracking, Synthetic Aperture Radar (SAR) satellite imagery, and vessel databases. Computer algorithms detect vessel movements and patterns, and provide alerts to the maritime operators (or Maritime Watch Centre) when there is anomalous activity.

Figure 15 shows a Project Eyes on the Seas screen grab giving an overview of the world's vessel traffic and shipping routes.

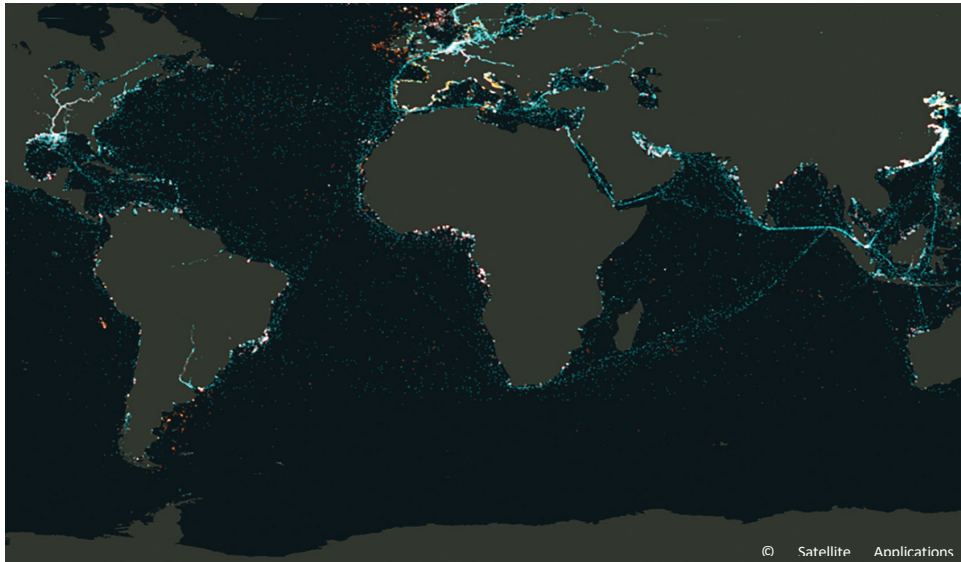


Figure 15: Global Maritime Operating Picture [17].

A similar approach to maritime domain awareness could also be used for space situational awareness and space object behaviors, for example. A satellite would have a known orbit. Should that satellite change its orbit, operators could be alerted to this anomalous behavior. This would be useful if a satellite is identified by a country to have a particular mission, but then exhibits behavior contrary to its stated mission. Another example would be satellite orbiting in geosynchronous orbit. Most satellites orbit the equatorial plane at three basic altitudes (analogous to shipping routes). When a satellite alters its orbit from its established altitude, operators could be alerted.

4.3 Information Security and Assurance

In today's world of global reliability on information, the transit and storing of that information and the growing occurrence of cyber-attacks, there is a need to protect data that is coming into, stored and used in a NATO common operating picture and also ensure that the data are reliable, integral and free of malicious content. Although the establishment of a NATO common operating picture of any sort will be dependent upon member nations sharing their information, all information needs to be adequately protected while transiting and while being fused into the common operating picture.

The main functional domains that were identified to carry critical challenges about Information Security and Assurance (ISA) were:

- NATO member nations' data source domains;

- NATO COP's data acquisition domain;
- NATO COP's data fusion domain;
- NATO COP's final product domain; and
- NATO COP's end-users' domain.

Although some of them could be implemented in the same NATO infrastructure/entity, we refer to them separately to focus on their specific challenges given their functional goals.

All domains will answer to a basic overall requirement of cyberspace protection from any intrusion and information access. As the level of security of a structure is strongly affected by the level of security of its weakest part, it is fundamental that all entities in charge of each domain agree on a set of standards, procedures, solutions and methodologies to bring the cyber-risk down to an acceptable level.

The ISA of each NATO member nation's data source domain falls under the sovereignty of the specific member.

Concerning the protection of the cyberspace from intrusion, as speculated by the Canadian DRDC Space COP Team, the domain of any country would require compartmentalization and numerous data diodes to mitigate risks at acceptable levels and to accomplish effective information sharing between countries.

Concerning the protection of the source data to be shared, *ad hoc* agreed encryption (e.g., QKD-based) and transmission protocols will protect the shared data, anonymizing some characteristics of the space objects or RFI data when applicable, permitting to promptly identify any security events/incidents and trigger the appropriate incident management procedure.

All NATO COPs functional domains will be under NATO Alliance responsibility, abiding by NATO cybersecurity policy *in primis*. To enforce a robust, near-real-time and secure processing of the COP, NATO could consider the application of the blockchain technology.

The NATO COP's data acquisition domain is in charge of acquiring the source data from NATO member nations according to the agreed transmission protocols and ISA requirements, triggering the incident management procedures as applicable. This is a critical function aiming to accept only "valid" source data, the risk being to compromise the COP environment for decision makers. Artificial intelligence could be a valid support in this phase, given the Big Data to be treated per unit of time.

Special attention shall be paid to the NATO COP's end-users' domain. The cybersecurity of this functional domain is affected by more parameters than the other functional domains, e.g., the accessibility to end-users' terminals, and the embedded security of those equipment which shall be attentively considered in the overall risk management activities, the consequences being possible eavesdropping and corruption of COP data.

4.4 Role of Standards

Standards with the broadest reach typically provide the most benefit. A similar NATO effort, DGIWG-907 Imagery and Gridded Data Roadmap, applied standards from ISO from a range of data interchange, data processing, sensors calibration, graphical interfaces, and systems interoperability. Industry consortium standards form the Open Geospatial Consortium provides data interchange and interoperability. NATO STANAGS filled the gap when industry standards were not yet available to meet the interoperability standards.

Besides industry standards legacy military standards also apply, particularly in the astrodynamics where military has been out front since the beginning of space object tracking.

NATO should prioritize the use of standards from International Organizations, Industry groups, and *de facto* industry standards. But this NATO COP effort should help test and identify the most beneficial, expose gaps, and recommend areas of improvement.

4.5 Challenges of Displaying the Space Domain

One fundamental difference of displaying the space domain is it cannot be confined to a tactical/operational Area of Responsibility (AOR) as easily as can be accomplished for air, land and sea domains. Space assets, as well as space-based threats, are simultaneously both strategic and tactical by nature. Space domain information cannot fully be considered in the narrow scope of a specific battle space. A standard view of the space domain must be developed in context with the information display of the cyber domain.

Respecting the need to be interoperable with the existing operational pictures, displaying the space domain will require a certain adaptability to the different user groups. A layered architecture that considers user rights and requirement might be necessary.

Resolving the explicit requirements for a standard view is beyond the scope of this technical activity, but will eventually become critical to address. As addressed in the recommendations of this activity, collaborative initiatives among NATO operators, planners and the S&T community will be important in the future to get this correct.

The next challenge from the above characterizations of a COP is the essential need for “current” and “relevant” data and information. The operational tempo anticipated in future conflicts, especially those involving peer competitors, may be extremely high (fast). To effectively survive and prevail in such operational environments will require extremely timely information for decision making. Data and information that has become Overcome by Events (OBE) will be clearly useless inputs to a common operational space picture.

The challenge for a multi-sourced common picture is determination of the appropriate dwell while awaiting all relevant information to be acquired, before pushing out data to the common picture. Fusion of information takes time, particularly for the adjudication of conflicting information. As more and more data and information streams become viable candidates for fusion and incorporation into a COP, the greater the potential dwell before a common picture meeting decision-making confidence requirements is achieved. Currency of space domain awareness data and information will be a cornerstone of the viability of any NATO common space operational picture. From a technical perspective, the SDA data collection strategy will be ideally driven by decision-making requirements and maximizing the required information to obtain a body of evidence of behavior(s) attributable to specific threats and/or hazards. Multi-source information fusion should seek to build decision-making confidence by fusing information that seeks to eliminate threat and hazard ambiguities.

Very much related to information currency is the concept of relevancy. The space domain, like the other operational domains, is a complex, multi-dimensional and potentially high ops tempo environment. There are many things, activities, conditions, situations, contexts. to be sensed, measured and communicated. Not all of that information, no matter how accurate or precise, is necessarily relevant to operational decision making. Attempting to pull/push too much data and information into an environment responsible for creating a COP runs the risk of congestion of critical information networks and overloading fusion processes, thus precluding timely receipt of critical information. There must also be a capability of incorporating latent or lagged information without the need of re-processing all of the sources received prior to that time. Measures of confidence or probabilities must be assigned to all bodies of evidence of space domain behaviors, to rigorously and properly inform relevant decision-making processes.

The last significant challenge from the above characterization of a COP is the explicit requirement that it should enable “awareness.” The concept of awareness in this context will require substantial dialog to ensure a

common perspective and subsequent capability requirements with respect to a common space domain awareness picture. In its simplest of operational definitions, awareness is matching perception to the reality. Situational awareness has been defined by numerous authors but perhaps the most applicable to the space domain is the following: “perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future” [14]. If one considers the space domain as the sum of all “situations,” then this definition can be applied in a similar manner for space domain awareness wherein the volume of “space” is substantially larger than for each of the “situations” within the space domain.

Operationally, awareness must be achieved and sustained across the continuum from individual, localized events and situations (e.g., at the individual satellite or space user level), increasing in scope through aggregate space architectures and constellations (e.g., the GPS constellation) and finally the totality of the space domain. The challenge going forward for NATO is the determination of the scope of the required awareness of the space domain sufficient to meet the decision-making requirements of both the NATO command elements as well as that among the individual members’ sovereign command elements. Localized awareness of space “situations” (e.g., collision probability on an individual space asset, or an instance of RF jamming of a satellite communication link) may be accomplished through localized Space Situation Awareness (SSA) functions. The driver behind information needs should be uniquely based upon the threats and hazards of concern to decision makers.

One of the biggest sources of discrepancies and inconsistencies in SDA is the fact that different users tend to have different SDA needs and even data, and furthermore different interpretations of what space objects and events are. This is what some would call Linear-Based Production (LBP). Those who would provide tools and solutions to SDA problems develop these in a very focused and tailored fashion. The issue arises when a set of users attempts to infer a collective understanding of the Space Domain from the output of these disparate tools and algorithms and invariably due to the inconsistencies in object description, data formats and standards, and even the physics and underlying assumptions involved in processing various data, yield ambiguous or errored collective interpretations at best. In fact, five different users may believe that they are observing five different space objects even when the supplied data may have all been generated by only common space object.

One way to overcome this is in the instantiation of what is called Object-Based Production (OBP) whereby the relevant users all agree on a common set of standards, definitions, constants, etc. with which to calibrate, collect, exchange, fuse, and exploit a variety of data and their products. Along with this, assumptions and caveats in models and processes can all be made to be consistent. In this way, disparate users driven by their own unique needs and requirements can infer what they need to from the data but when interested in a common picture, will achieve this given the agreement on what was previously described.

Another major source of error is that the data and products either have no measure of ambiguity, or when attempting to gain a common picture, the various measures of uncertainty are not interrelated in any way. For instance, how does one combine an “error bar” with a covariance, or with an opinion or belief? What does one do with conflicting evidence? Is the ambiguity, however modelled or represented, realistic, meaning, does it accurately represent and describe the actual error distribution or manifestation. Uncertainty and ambiguity are simply the absence of Information or Knowledge. This can vary from one user to another and introduces complexities.

5.0 CONCLUSIONS

This report documents the work of the NATO Science and Technology Organization’s SCI-279 Task Group addressing the technical considerations for enabling a NATO-Centric Space Domain Common Operating Picture (COP). The overall objective was to enable a shared space domain awareness to maximize deployment of mission resources and afford maximum use and protection of space capabilities and services

throughout the Alliance. Ultimately, the customers/consumers of SDA will shape their requirements and manifest them in appropriate doctrine, tradecraft and standards.

The purpose of the SCI-279 Task Group was to assemble a team of subject matter experts to conduct the first exploration and characterization of enabling technical considerations for a future NATO capability to generate/create a common SDA picture shared across NATO. As the first NATO investigation into this topic area, this effort was not intended to develop specific technical or institutional recommendations, but rather to begin the process of identifying, among other things, anticipated technical challenges requiring R&D, the scope of the technical disciplines and interfaces for assimilation and fusion of disparate data types and sources, and potential end-user operational application requirements. The findings and outcome of the Task Group are manifested in a set of recommendations to further evolve and refine the collective NATO understanding of where NATO SDA requirements are headed.

The SCI-279 Task Group has provided an opportunity to establish an initial NATO Community of Interest (COI) on NATO space domain awareness. As sponsored via NATO STO, inherently this COI represents a NATO-level perspective on this topic area underwritten by the national expertise. This cadre of experts is a resource that can be built upon and leveraged by the various NATO agencies and organizations chartered with identifying, acquiring and operating NATO mission capabilities.

This activity is intended to explore the technical boundary conditions and anticipated fundamental enabling technical considerations and requirements for developing and evolving the capacity within NATO to achieve a NATO common space domain picture. In addition, this activity has the purpose of identifying necessary technical research and development investments and collaborations within NATO as well as initiating and informing a dialog within the NATO leadership and operational planners on the nature and anticipated future needs within NATO for space domain awareness capabilities.

Due to the sensitive considerations associated with sharing sovereign space asset health and status information as well as hostile space order of battle and status within the Alliance, inclusion of those topics as part of a NATO common space domain operational picture are not anticipated to be addressable for the foreseeable future.

In addition, in recent years there has been an increasing number of bilateral and multilateral agreements established between and among some of the NATO Alliance members (and, in some cases, with nations not part of NATO) to share space object tracking information of greater fidelity and timeliness than can be obtained from publicly (including commercially) available sources (see Ref. [19], for example). The SCI-279 Task Group does not address the institutional nature of those agreements specifically, although the incorporation of space domain awareness information of that sort may be a portion of the data and information contribution from one or more NATO nations.

Within the NATO organizations and agencies, little attention has been paid to Space Domain Awareness (SDA) requirements in the past since, as mentioned above, this has been the sovereign purview of the member nations. The NATO Centre of Excellence (COE) organization, the Joint Air Power Competence Centre (JAPCC) has published a few articles on SSA [20], [21] and the NATO Bi-Strategic Command's Space Working Group has addressed SSA in its report on NATO space dependencies [22]. The NATO STO activity SCI-229 Task Group addressed the role of space weather in NATO space situational awareness and concepts for operator tools for detection and interpretation of potential space weather effects on NATO operations [23]. The SCI-238-SM (Specialists' meeting on NATO space dependencies, [24]) and the SCI-268-SM (Specialists' meeting on NATO future space S&T needs, [25]) also highlighted the need for NATO to have the ability for comprehensive space domain awareness.

A similar data and information integration challenge has been faced within the NATO ISR community. Because of the disparate types and sources of ISR data being provided to NATO from the member nations, a

collaborative group was established to develop guidelines, common processes and ultimately standards to enable the integrated collection, fusion and dissemination of ISR data and information within NATO. The work of the Joint Capabilities Group for Intelligence, Surveillance and Reconnaissance (JCGISR) offers a potential model for collaboration on standards, architectures and interoperability with respect to integrating national-sourced space information and data. The SCI-279 activity has attempted to leverage some of the lessons learned from the JCGISR experience to guide some of the thinking on how to approach the space data challenge within NATO.

5.1 Summary Observations and Recommendations

The following are the six summary observations and recommendations cutting across those three focus areas that resulted from the Task Group:

Observation: The common space domain awareness requirements of the NATO Alliance to achieve maximum exploitation and preservation of its space capabilities are not well understood, nor have they been formally discussed or documented.

Recommendation: Conduct strategic analyses of the NATO requirements for space domain awareness involving its military planners, operators, space service (e.g., SATCOM, PNT, ISR) providers as well as providers of space domain awareness data, products and services.

Observation: Currently there are no NATO standards for describing space objects or events, or for processing and dissemination of data and information related to the space domain.

Recommendation: Develop an initial set of foundational standards for characterizing and applying space domain related data, products and processes critical to enabling and preserving NATO space activities.

Observation: Currently no commonly agreed upon processes or models for fusion of space domain data from disparate sources exist that can be applied to anticipated future NATO needs.

Recommendation: Articulate the requirements for initial space data fusion capabilities and the initial investments and focus that should be pursued consistent with anticipated NATO requirements for space domain awareness.

Observation: Throughout NATO member nations there is uneven technical and operational experience with space domain data collection, processing, dissemination and application that hinders both maximum exploitation and preservation of NATO space capabilities.

Recommendation: Expand the sharing of tradecraft, data and experiences throughout the NATO space capability providers, S&T community, and NATO military trainers, planners and operators.

Observation: Within NATO there has been no shared experience with the collection, fusion and dissemination of space domain data or information to provide a basis for understanding the opportunities and challenges of achieving a NATO common space domain operating picture.

Recommendation: Seek opportunities for experiments and field trials involving shared collection, processing and dissemination of space domain data and products to facilitate a common understanding within the Alliance of the opportunities and challenges ahead.

Observation: The integration of space domain awareness into NATO military planning and operational decision making is limited principally due to a minimal degree of operational art involving space.

Recommendation: Undertake, via NATO S&T elements, modelling and simulation analyses of the military utility of various decision-making options involving space domain awareness as well as exploration of technical solutions enabling timely and effective integration of space domain awareness into NATO military planning and operations.

6.0 REFERENCES

- [1] NATO: SCI-238 Final Report: Long-Term Requirements Study. Enclosure 1 to 1500/SHJ5CMD/08-205478 5000 TC-70 TT-3425/Serial: NU0059 Dated: 23 October 2008.
- [2] NATO: Report of SCI-238-SM Specialists' Meeting on NATO Space Dependencies. AC/323(SCI-238)TP/544, published January 2014.
- [3] United States Department of Defense. Space Operations. US Joint Publication 3-14, April 2018.
- [4] NATO STO: Space Domain Awareness Concepts and Approaches to Support NATO Operations. STO-EN-SCI-292, July 2016.
- [5] Stauch, J., and Jah, M. Unscented Schmidt-Kalman Filter Algorithm. *Journal of Guidance, Control, and Dynamics*, 38(1), 117-123, 2015.
- [6] Azimirad, E. and Haddadnia, J. The Comprehensive Review on JDL Model in Data Fusion Networks: Techniques and Methods. *International Journal of Computer Science and Information Security*, vol. 13(1), 53-60, January 2015.
- [7] The University of Texas at Austin, Moriba K. Jah. <https://sites.utexas.edu/moriba> and <https://www.ices.utexas.edu/research/centers-groups/cast/>. (Accessed November 2020).
- [8] Jain, A.K. (Fellow, IEEE), Ross, A. (Member, IEEE), and Probukar, S. (Member, IEEE). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, 4-20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.
- [9] UK Royal Academy of Engineering, Global Navigation Space Systems: Reliance and Vulnerabilities. London, March 2011, <http://www.raeng.org.uk/publications/reports/global-navigation-space-systems>.
- [10] Vizard, F. Safeguarding GPS. *Scientific American*, 14 April 2003.
- [11] Out of Sight. *The Economist*, 27 July 2013 and \$32K Penalty Proposed for Use of a GPS Jammer by an Individual, U.S. Federal Communications Commission, FCC 13-106, 2 August 2013.
- [12] Wallace, B.J. Considerations for, and Approach to, Developing a Space Common Operating Picture (SCOP) Technology Demonstrator. Defence Research and Development Canada Reference Document, in publishing process, June 2017.
- [13] Project 05BA, Space Situational Awareness, ADM(S&T) Project Management Plan. May 2017.
- [14] Lopez, X., Wu, Z. Mining Big Data with RDF Graph Technology. https://download.oracle.com/otndocs/tech/semantic_web/pdf/semtech_datamining_v8.pdf. (Accessed November 2020).
- [15] Esteva, M., Xu, W., Simone, N., Gupta, A., and Jah, M., (2020) Modeling Data Curation to Scientific Inquiry: A Case for Multimodal Data Integration. In: Proceedings of the 2020 IEEE Joint Conference on Digital Libraries (JCDL2020), Xi'an, China, August 1 – 5, 2020. <https://doi.org/10.1145/3383583.3398539>.
- [16] MaeroSpace Inc., Maerospace Information Factory™. <http://maerospace.com/our-model/>. (Accessed November 2020).

- [17] Project Eyes on the Seas, http://www.pewtrusts.org/~media/assets/2015/03/eyes-on-the-seas-brief_web.pdf. (Accessed November 2020).
- [18] Endsley, M.R. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, 1995, 37(1), pp. 32-64.
- [19] ExoAnalytic Solutions, Inc. www.space-track.org. (Accessed November 2020).
- [20] Wiedemann, C. A Model of the Space Debris Environment. *The Journal of the JAPCC*, Edition 20, Spring/Summer 2015, p. 46.
- [21] Neumann, S. Space. *The Journal of the JAPCC*, Edition 20, Spring/Summer 2015, p. 22.
- [22] BiSC Space Working Group Report on NATO Space Dependencies to the NATO Military Committee. 2014.
- [23] NATO: Space Environment Support to NATO Space Situational Awareness, Final Report of STO-TR-SCI-229. NATO Science and Technology Organization, December 2018.
- [24] NATO: NATO Space Capability Preservation (A Day Without Space). In: Proceedings of SCI-238 Specialists' Meeting. NATO Science and Technology Organization, AC/323(SCI-238)TP/544, 2013.
- [25] NATO Space: S&T Developments to Enhance Resiliency and Effectiveness of NATO Operations, Final Report of Specialists' Meeting SCI-268-SM. NATO Science and Technology Organization, STO-MP-SCI-268, June 2014.

Appendix 1: APPROACH AND ASSUMPTIONS

This appendix describes the approach and assumptions taken by the SCI-279 Task Group in its consideration of the technical enabling requirements for a NATO common space domain operating picture. The Task Group was approved in September 2014 by the Science and Technology Board, and kicked off in October 2014 following the deliberations of an Exploratory Team (SCI-ET-003). The Task Group has conducted technical and coordination meetings as follows:

- 2014 October Paris, France (Eutelsat Headquarters);
- 2015 March Kalkar, Germany (German SSA Centre and Joint Air Power Competence Centre);
- 2015 June London, United Kingdom (University College London);
- 2015 October Copenhagen, Denmark (Technical University of Denmark);
- 2016 March Paris, France (NATO CSO); and
- 2017 July Paris, France (NATO CSO).

The Task Group was compartmentalized into three subgroups to focus on the main space domain awareness components addressed in this effort; space object surveillance and tracking, space environment (weather) and radio frequency inference to satellite communications. The Task Group met several times (see above) to discuss the higher-level issues, provide material and updates throughout the effort period.

Due to the absence of any NATO precedence for a common environment for space-related information, the Task Group spent several of its initial meetings working through the major issues and concepts perceived to be involved in the eventual development of a common space domain picture. These discussions were valuable since there had been no previous dialog within the NATO space community addressing the potential requirements, applications, and challenges – both technical and institutional.

To help to focus the discussions and articulation of the environment in which NATO may find a common space domain awareness picture useful, a set of scenarios were developed. Recall that a purpose of SDA is to provide decision-making processes with a body of evidence of behavior(s) attributable to specific threats and hazards. This means that any SDA scientific and technological roadmap must begin with specific threats and work “backwards” to determine the required information and information sources that support decision-making processes concerned with those threats. These are captured in the following scenarios in Section 3.2, which are intended to provide hypothetical operational environments in which both the NATO command structure as well as the command structure of each of the member nations might benefit from a common operational picture. These scenarios do not address the comprehensiveness or lack thereof of space operational pictures maintained using sovereign sources of space domain information and data.

The Task Group used several working assumptions about NATO, NATO’s use of space, and the relationships among the Alliance members with respect to space. It is recognized that some of these assumptions may need to be reconsidered or become partially invalid in time, but the critical work required by the Task Group is to develop a notional framework that could be employed for any scenario deemed of concern to NATO space capabilities and/or dependencies.

- The space domain is expected to become more complex in terms of technology-driven capabilities, global proliferation of space capabilities, contributions to the global information grid, and adversarial capabilities to degrade, disrupt, deny or destroy space capabilities upon which NATO is reliant.
- The space domain will increasingly become more important to NATO operations as well as more complex in terms of the role that it will play among the sovereign forces provided to the Alliance.

- NATO will not acquire, as NATO, space hardware capabilities for the foreseeable future. In addition to space assets per se, this also includes assets for tracking or monitoring space objects, collection of space environmental data, and collection of radio frequency interference. Alliance members will provide all capabilities in this regard with the potential exception of space domain information from non-aligned nations and commercial entities.
- A shared, common military knowledge of space domain awareness will be necessary to fully leverage any common space domain awareness capability provided to the Alliance from its members and partners.

Appendix 2: SCENARIO DESCRIPTIONS

The following scenarios were used by the Task Group throughout its deliberations to help focus and communicate the concepts and technology required to establish a future NATO common space domain awareness operational picture. These scenarios are hypothetical and designed to make highlight some of the more important requirements and issues. They are not intended to depict any specific projected real-world situation in which NATO is expected to be engaged.

For purposes of these scenarios, the following applies:

- 1) Space debris in all orbital regimes, especially in the GEO belt, is increasing and many objects are suspected to exist which are not yet cataloged or identified given that there are a significant number of detections that cannot be reconciled (correlated or associated) with known objects.
- 2) Solar activity has been increasing over the past week culminating in a coronal mass ejection which projected an extremely large quantity of charged particles out into deep space. A significant amount of the charged particles collided with the Earth's electromagnetic field and penetrated the ionosphere.
- 3) Space capabilities provided to support NATO operations conduct preplanned satellite overflights to obtain satellite imagery for reconnaissance purpose.
- 4) Amberland is a fictitious and evolving space-faring state with the following capabilities:
 - a) Rudimentary capability to conduct active space debris removal; and
 - b) Low Earth Orbit (LEO) satellites equipped with high-resolution, electro-optical sensors.

Scenario 1: “Loss of Satellite Communication”

NATO has set up an expeditionary force next to Amberland. To conduct operations, NATO requires SATCOM to support command and control of its assigned forces. For this purpose, commercial satellite communications services are made available. An outage has occurred on a critical, primary communications satellite, which is in a geosynchronous orbit. The NATO has become aware of a loss of communications between SHAPE and special operations forces on ground. The commercial SATCOM operator confirms that it has lost contact with its satellite.

While dependent on SATCOM to conduct its mission, the NATO does not have any means to analyze the root cause of the communication loss. Space domain awareness insights provided by national resources would have helped to answer the following questions:

- What was the current space weather impact on operational satellites?
- Was there a conjunction with another satellite or piece of debris?
- Did the Amberland space debris removal asset maneuver towards and approach the communication satellite?
- Are new pieces of debris detected near the SATCOM satellite, which might be indicative of a break-up (collision, explosion, other)?

Scenario 2: “Overflight Warning”

The NATO command decides to move ground forces closer towards the border with Amberland. A few hours after the involved forces have left a NATO base, Amberland public media reports on NATO's aggressive and provoking actions against its country. Media stations broadcast high-resolution images of NATO's ground forces leaving the base including detailed characterization of the forces' composition and equipment.

The availability of information, the moment of surprise and the need to disguise the next tactical step are still as important as it was in the past. Even without violating a border, satellites have the capability to conduct reconnaissance very effectively on a possible opponent.

Space domain awareness would have given the NATO Commander the ability to predict the position of Amberland's Low Earth Orbit satellites equipped with high-resolution, electro-optical sensors. The orbital data, which were provided by a NATO member state to the NATO common space object catalog would have indicated the 8-minute overflight window, the Amberland reconnaissance satellite had to acquire the images. A short delay in deploying the forces would have concealed the movement altogether.

Due to the physical laws of space, satellites are predictable. The knowledge of the future position of an opponent's reconnaissance satellite can be significant. This information can be used to hide, to deceive or in contrast to project military power. Not only the propagated position of such a satellite is of importance, but also the payload capabilities and limitation (e.g., optical vs. radar).

Scenario 3: "GPS Accuracy"

An abnormal movement of forces coming from Amberland has crossed the border and started to attack an industrial area with mortar fire. The NATO Commander orders a combined air operation over the mortar sites. To limit any collateral damages, the operation includes a reconnaissance mission by Unmanned Aerial Vehicles (UAVs) and GPS-guided ammunition.

The coronal mass ejection has led to a massive degradation of UHF communication and GPS accuracy. As a result, one UAV aborted its mission and returned to base on a preprogrammed route and two GPS-guided air-to-ground missiles missed their target causing minor collateral damage.

Part of space domain awareness is to have an unhindered understanding of the space environment and its impact on those space-based assets necessary to conduct military missions. Solar activity can have a significant impact on space and terrestrial infrastructure. While coronal mass ejections of charged particles allow for a certain warning time, the impact of solar radiation occurs too quickly to be predicted. The consideration of solar events during the military planning cycle with the forecast for radiometric degradation and GPS dilution of precision has become critical.

Scenario 4: "Contingency Awareness and Response to Adversarial Action"

During an air policing mission along the Amberland border, a mid-air collision occurred with one NATO aircraft going down in Amberland territory. The NATO Commander received approval to conduct a cross-border operation to extract the isolated personnel. An urgent request for satellite imagery of the crash site could not be fulfilled and as such, the rescue mission had to be delayed by several hours.

Space situational awareness would have informed the NATO Commander that Amberland used its active debris removal satellite to physically take custody of the NATO assigned reconnaissance satellite. This proximity maneuver was detected by a NATO member's ground radar sensor and shared with the common SDA database. Amberland justifies its action as an act of self-defence, threatening to use anti-satellite weapons to destroy any satellite that they perceive as a threat. Space situational awareness allows a prediction of the catastrophic impact on a variety of satellites within the respective orbit regime, if a satellite would be destroyed creating a huge debris cloud. This knowledge would have a significant impact on strategic military threat assessment and contingency planning.

REPORT DOCUMENTATION PAGE			
1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-SCI-279 AC/323(SCI-279)TP/931	ISBN 978-92-837-2256-4	PUBLIC RELEASE
5. Originator	Science and Technology Organization North Atlantic Treaty Organization BP 25, F-92201 Neuilly-sur-Seine Cedex, France		
6. Title	Technical Considerations for Enabling a NATO-Centric Space Domain Common Operating Picture (COP)		
7. Presented at/Sponsored by	Final report of RTG SCI-279.		
8. Author(s)/Editor(s)	Multiple	9. Date	December 2020
10. Author's/Editor's Address	Multiple	11. Pages	56
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	Space domain awareness; Space situational awareness; Space environment; Space weather; Radio frequency interference; Space operations; Space debris; Space surveillance; Satellites; Space; Orbits; Common operating picture		
14. Abstract	This report documents the work of the NATO Science and Technology Organization's Task Group (SCI-279-TG) addressing the technical considerations for enabling a NATO-Centric Space Domain COP. NATO has recognized the critical reality of its dependence upon space capabilities and on ensuring that NATO operations maximize their leverage of space. A critical element of ensuring the availability and efficacy of these space capabilities is the availability of a common operational perspective of the space domain throughout the Alliance and its partners.		





BP 25

F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cs.o.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 et 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 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
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

Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

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 01 Liptovský Mikuláš 1

SLOVENIE

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

TURQUIE

Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanlıklar – 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>).



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



**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 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
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

Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport “Comparto A”
Via di Centocelle, 301
00175, Rome

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 01 Liptovský Mikuláš 1

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 Bakanlıklar – 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>).