Development of a Civil Military Interface in Europe for Galileo

L. Tytgat, J. I. R. Owen and P. Campagne

Satellite navigation has demonstrated its ability to enhance the safety and efficiency of multi-modal transport systems and act as a stimulant to economic growth and commercial development. The decision of the Transport Ministers to proceed with the definition stage of Galileo currently being funded by the European Commission and the ESA GalileoSat programme will include the complex question of security and defence considerations. Initial studies were completed over the past year in a Civil Military Interface study and by the GNSS Forum for Security and Defence Considerations. This paper presents the findings of the Civil Military Interface study undertaken for the European Commission, DGVII, that identified the security and military implications of a civil operated and controlled satellite navigation service for Europe.

KEY WORDS

1. GNSS. 2. Military Needs. 3. Civilian Needs. 4. Policy.

1. MILITARY ISSUES. The availability of a global navigation service that offers high accuracy and integrity brings significant benefits to many different categories of user. Several user categories need a reliable and accurate service that provides safety from malicious degradation. Galileo is intended for use by a diverse set of users and therefore includes high-integrity signals. While the benefits of a high-integrity service are numerous, the drawback lies in its susceptibility to misuse by hostile third parties. Misuse can manifest itself in two forms. Aggressors can either use the signal for the purpose of attacking their enemies (for example, with guided weapons), or they can corrupt the signal to deny the full benefit of the service to its intended *bona fide* users. A need clearly exists to prevent subversive use of the service and to protect the service from hostile intrusion.

Use of commercial-off-the-shelf (COTS) satellite navigation receivers in surveillance and precision-guided weapon systems is a concern to defence analysts. GPS was designed by the US DOD to correct the errors of inertial navigation system in long-range weapon systems. The Russian GLONASS was designed to perform similar functions. GPS contains a controlled access service (CAS) to reduce the capability of its misuse in hostile weapon systems, and the accuracy of the open GPS Standard Positioning Service (SPS) is degraded by the use of selective availability (SA). Introduction of differential systems has negated the military advantage of SA. Lobbying from the civil community has resulted in a Congressional decision to remove SA by 2006, and the US DOD must substantiate the requirement for SA annually from 2000 onwards. Further improvements planned for GPS will result in SPS GPS providing an accuracy of approximately 5 m by 2010. Use of GPS within critical US infrastructure means it cannot be turned off without severe economic

disruption. To ensure the military advantage of GPS is maintained, Congress directed the US DOD to develop means of denying hostile forces use of precision navigation from satellite systems. However, denial of satellite navigation signals to preserve security means that it is likely that accurate navigation and positioning data is degraded or denied to legitimate users over large geographic areas.

The European Union has treaty obligations to ensure safe transport of goods and people. Galileo will be a strategic asset for the EU to provide the means for a safe transport system. The Commission's concern over the conflicting requirements for safety of transport and defence and security requirements led to the requirement for a Civil Military Interface study. It should be noted that the Commission do not hold competence for two significant policy issues that affect the design and operation of a GNSS, frequency management and defence which both remain with the nations.

2. MILITARY CONCERNS. The study obtained the views of military representatives from many EU and non-EU states and NATO members. Although there is widespread concern over the availability of precise navigation data from GNSS, the risks of its potential misuse in times of peace are acceptable to defence forces. However in times of tension, crisis or war, where national security was threatened, any open or controlled access service not under allied military control, and potentially useful to a hostile force, would be jammed. Traditionally, States have placed their radio-navigation service, transport infrastructure, seaways and airspace under military control in times of acute crisis or war. Whilst it is extremely unlikely that any European State would deny GNSS signals in advance of the closure of its transport systems, due to their lack of control over GNSS transmissions, several States indicated there might be occasions when they would jam the signals without notice. The military highlighted their requirement to train under realistic combat conditions, carry out equipment testing and evaluate their capabilities.

During peacetime, there are requirements in all EU States to announce any disruption of radio-navigation services. Such notification is given to the aeronautical community by NOTAMs and by NOMARS to maritime users. The problem is the notification of 'other' users for whom there is no formal communications channel. Recently the BBC issued a warning on national news bulletins concerning potential problems to GPS users from the 1023 week clock roll-over, but this was treated as a general news item rather than a formal warning to users. Spill-over from jamming in adjacent regions where for self-defence reasons jamming is active without notice is a prime concern. Due to the low signal level and signal structure of the current GNSS signals, a jammer is likely to affect any users within its line of sight.

Prior notification of jamming in times of crisis, tension and war could compromise military operational security and is unlikely to be given. Obviously, no prior notification is available on jamming by any hostile forces or from interference as occurrence of the latter is unintentional. These issues are summarised in Table 1. Two major requirements were identified for an interface between the civil operators of Galileo and the military commands, concerning disruption to the signal-in-space (SIS), and the implementation and control of a Controlled Access Service (CAS).

3. DISRUPTION TO GNSS SIS. Three potential sources of disruption to GNSS SIS can be envisaged:

Table 1. Comparison of civil and military requirements in times of tension, crisis or war.

Characteristic	Civil requirement	Military requirement
Accuracy	Maximum possible.	Degradable when required.
Notification of Degraded Service	As fast as possible to maintain safety of life.	Not always possible if this compromises operational security.
Monitoring	Would wish to monitor performance over wide area.	Would wish to monitor performance over smaller area/theatre of ops. May not pass on information all of time.
Jamming	Jamming highly undesirable.	Would wish to jam as need dictated
Anti-Spoofing	Anti-spoofing capability desirable.	Not desirable, unless being used by military for operations.
Control Access Service	Good for anti-spoofing and recovery of user charges but cannot be certified for ICAO or IMO under current procedures.	Good if different user levels, since can switch out different user groups, but concerns over security.
Military use of service	Only desirable for cost mitigation and arms export.	Not generally considered necessary due to availability of GPS.

a. Unintentional Disruption: where warnings would not and could not be given, as the cause is accidental radio interference or system errors.
b. Hostile Actions: Disturbance caused by those with malicious or hostile intent, where prior warning of disruption is highly unlikely, although it could be given subsequently if detection and information systems were in place. Disruption could include terrestrial and airborne jamming and spoofing, information warfare or physical attack.
c. Friendly Military Actions: Disruption caused by entities generally sympathetic to legitimate operation of civil system, when there is a security or defence need to generate jamming signals over a local area or geographic area. Types of disruption identified include terrestrial and airborne jamming, spoofing and requirements for accuracy degradation.

Given that the disruptions are not all within the control of EC or allied military commands or a civil operator, it becomes apparent that monitoring of the SIS is necessary regardless of any policy adopted by allied military powers. What is important, is that a safe method should be employed to identify disruption and notify the disruption to safety-critical users. The density of monitoring networks should reflect both the level of risk and level of importance. The monitoring network should perform real-time monitoring of the SIS, to identify system errors, interference, and jamming. It is interesting to note that Europe could in future have such a system, at relatively low cost as an initial step, by combining information from the maritime DGPS stations, the EGNOS Remote Integrity Monitors, (RIMS) and future Local Area Augmentation Systems (LAAS) stations to be implemented by civil air traffic service providers.

Detection of unintentional interference is the responsibility of national Radio-Communications Agencies. Most nations have some fixed monitoring sites and

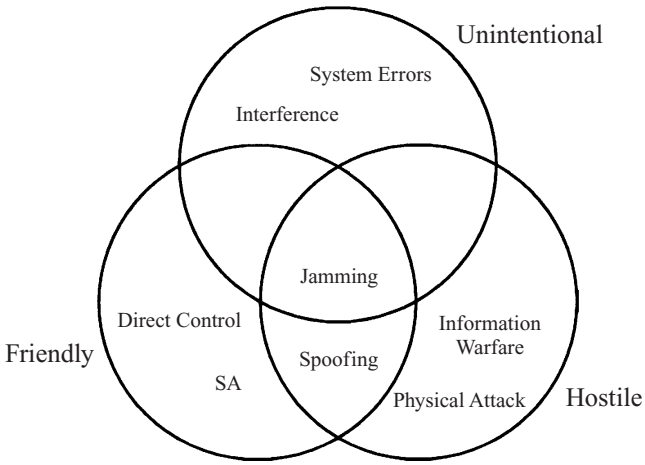

Figure 1. Summary of forms of disruption.

mobile response units. Priorities and typical response times in dealing with interference are for safety-of-life and emergency services (within 24 hours), secondly to assist businesses affected by interference (within one week), and finally to deal with other interference complaints (within one month).

The time taken to recognise that a GNSS receiver is not performing, that the reason is interference-related and to request the Radio-Communications Agency to undertake an investigation is clearly outside the alert times normally associated with safety-of-life applications. Problems of interference identification could be considerably compounded if the interference is intermittent or specific to a local area not covered by a monitor. To provide some perspective of the potential size of the problem, there are some 500 annual occurrences of malicious interference with Air Traffic Management communications in the UK alone. Timescales to remove interference from GNSS is unlikely to be less than a few hours. The study identified that military units were well placed to assist in identifying interference problems and their location. The information required from the military by the service operator should be embodied in appropriate MOU/MOA at international level, and could be embodied in treaties.

4. CONTROLLED ACCESS SERVICE. Requirements for a CAS were expressed by several States for high-integrity operations including use for security and defence. CAS techniques are the only means to satisfy secure requirements for a signal that cannot be spoofed, and provide a means to recover costs from the system by charging users. Indeed, the US developed their CAS on the funds Congress voted for a means of collecting user charges. The EU communications on Galileo outlined requirements for two CAS including:

a. Selective denial of the SIS to specific groups of users at times of tension, crisis or war,
b. Ability to introduce a charging mechanism for users requiring services additional to those offered by the basic open service,
c. European civil control of the system via the CAS,

d. Compatibility with US operation of GPS,
e. A complementary addition to GPS to improve satellite availability for military operations,
f. An alternative to military GPS for European States, who do not have an agreement for PPS GPS with the US, or to those currently using PPS GPS should the US ever withhold access to this service.

A CAS can be incorporated into GNSS by the following functions and technologies:

a. Switching the system off,
b. Encryption of the SIS with a hierarchy of encryption keys where access to some users can be denied by revoking key validity. The use of encrypted signals provides high-security users with protection from spoofing,
c. Controlling access to full SIS accuracy by pseudo-random degradation of accuracy of SIS, and use of encryption techniques, to enable authorised users equipped with suitably-keyed receivers to reconstitute the navigation message. Unauthorised users would be able to receive the degraded signal only,
d. Denial of signal reception on local, area or regional basis by use of jamming.

However there are several implications for the introduction of a CAS:

a. The need for a European cryptographic and security agency;
b. The need for a European facility to manage access to a CAS,
c. Security and military involvement,
d. Legal and institutional issues due to military involvement in the system as ICAO and IMO have steadfastly refused to certify a cryptographic system,
e. Cryptography is regarded by several States including France, Germany and US as an armament and is placed on their munitions list, severely restricting exports,
f. Cost.

5. CRYPTOGRAPHIC GENERATION AND MANAGEMENT REQUIREMENTS. A European GNSS 2 with a CAS will require the development of cryptographic algorithms and keys. Generation of cryptographic materials for security and state applications is performed by national agencies closely linked to government. The development of cryptographic algorithms and the sharing of cryptography management by more than one State is a new issue. Under the mandate given by the transport ministers to the Commission to establish the Galileo Steering Committee, the issues of an appropriate organisation within Europe to undertake key management and key distribution are being discussed.

6. SECURITY/MILITARY INVOLVEMENT. There are two issues in the implementation of a CAS that have military implications; firstly, security to ensure the cryptography is not compromised, and secondly, management through the lifecycle to ensure that access to CAS is controlled.

Implementation of a CAS into Galileo raises issues over proliferation of military capability. Use by ICAO and IMO is questionable under their current charters as standards have to be open and by definition, standards for encrypted systems are classified. Also, there are legal issues in some states, such as the US, where there are legal restrictions concerning cryptography.

The EC does not have 'competency' for defence matters. Control of European GNSS in times of tension, crisis or war, will require development of the common defence policy under the Treaty of Amsterdam. In order that a civilian operated Galileo can be controlled and managed in accordance with the sensitivities for the security of EU member states, it is recommended that a collaborative mechanism be developed with military authorities. A way forward suggested in the study was for the Western European Union to be the conduit for a civil-military interface with the following roles:

a. During peacetime, to provide a means to co-ordinate military activities that could cause interference with civil use of GNSS,
b. To participate in the co-ordination processes with the similar centres being established in the US for GPS,
c. To participate in the operation and management of European GNSS and ensure in times of crisis, tension or war, GNSS is operated in a manner that reflects any threats to European States,
d. To provide security and defence inputs to a monitoring facility that can provide real-time availability and interference data of GNSS over the European region,
e. To provide a security structure for CAS implementation and operation. Incorporation of a CAS into a European GNSS will result in the EU owning an asset with strategic potential. Defence and military authorities of the Member States require a structure to co-ordinate the operation and management of a European GNSS to ensure it can react to potential threats,
f. To provide a means to approve particular users and safeguard the system against its use for purposes detrimental to the EU and the security of its Member States,
g. To provide links with other GNSS (military) operators.

ACKNOWLEDGEMENT

The study for the European Commission DGVIIA was undertaken by a team led by Navigation Systems, DERA (UK) with FDC (FR), TELEMATICA (GE) and IESSG (UK).