

University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

Space, Cyber, and Telecommunications Law
Program Faculty Publications

Law, College of

2007

The 'S' of 'Security': Europe on the Road to GMES

Frans von der Dunk

University of Nebraska - Lincoln, fvonderdunk2@unl.edu

Follow this and additional works at: <https://digitalcommons.unl.edu/spacelaw>



Part of the [Air and Space Law Commons](#)

von der Dunk, Frans, "The 'S' of 'Security': Europe on the Road to GMES" (2007). *Space, Cyber, and Telecommunications Law Program Faculty Publications*. 8.

<https://digitalcommons.unl.edu/spacelaw/8>

This Article is brought to you for free and open access by the Law, College of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Space, Cyber, and Telecommunications Law Program Faculty Publications by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

THE 'S' OF 'SECURITY': EUROPE ON THE ROAD TO GMES

Dr. Frans G. von der Dunk*

1. Towards Global Monitoring for the Environment and Security (GMES)

In November 2001, by means of a Resolution¹ the European Union officially launched 'Global Monitoring for the Environment and Security'(GMES), the second European space programme (after Galileo²) essentially driven by the Union. The Resolution *inter alia* calls for the European Commission to coordinate with

* *Director Space Law Research, International Institute of Air and Space Law, Leiden University. This Article forms part of the Leiden Faculty of Law research programme "Securing the rule of law in a world of multilevel jurisdiction: coherence, institutional principles and fundamental rights".*

1. Council Resolution on the launch of the initial period of global monitoring for environment and security (GMES), of 13 November 2001; OJ C 350/4 (2001). See further Communication from the Commission to the European Parliament and the Council – Global Monitoring for Environment and Security (GMES): Establishing a GMES capacity by 2008, COM(2004) 65 final, of 3 February 2004.
2. See for Galileo: Council Resolution on the European Contribution to the Development of a Global Navigation Satellite System (GNSS), of 19 December 1994; OJ C 379/2 (1994); Council Resolution on the involvement of Europe in a new generation of satellite navigation services – Galileo-Definition phase, of 19 July 1999; OJ C 221/01 (1999); Council Regulation setting up the Galileo Joint Undertaking, No. 876/2002/EC, of 21 May 2002; OJ L 138/1 (2002); Communication from the Commission to the European Parliament and the Council – Integration of the EGNOS programme in the Galileo programme, COM(2003) 123 final, of 19 March 2003; and Council Regulation on the establishment of structures for the management of the European satellite radio-navigation programmes, No. 1321/2004/EC, of 12 July 2004; OJ L 246/1 (2004).

the European Space Agency (ESA) the realisation of “an operational and autonomous European capability for global monitoring for environment and security” by 2008, crucially involving a satellite system.³

Relevant data which are to form part of such a capability may, in principle, come from a number of different sources: space-based data, airborne data, and *in situ*-generated data of different terrestrial origin. However, non-space data almost by definition are generated within one national state or other, which means that applicable law and regulation in principle differs – and sometimes hugely so – from state to state, whilst generally not having developed with any specific consideration for the types of data involved in GMES either.

By contrast, outer space is an international area outside of any state’s international individual jurisdiction⁴, where operational paradigms of a principally international, even global character apply. This also has a profound impact on the legal issues closely connected to the generation of space-based data, as opposed to data generated in other modes where national sovereignty remains fully visible. Moreover, the space-part is clearly the most distinguishing factor of any GMES operation, in view also of the envisaged fundamental role of satellites, ESA⁵ and likely

3. Para. (3), Council Resolution of 13 November 2001.

4. See esp. Art. II, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (hereafter Outer Space Treaty), London/Moscow/Washington, done 27 January 1967, entered into force 10 October 1967; 610 UNTS 205; TIAS 6347; 18 UST 2410; UKTS 1968 No. 10; Cmnd. 3198; ATS 1967 No. 24; 6 ILM 386 (1967).

5. The European Space Agency (ESA) was established by the Convention for the Establishment of a European Space Agency (hereafter ESA Convention), Paris, done 30 May 1975, entered into force 30 October 1980; 14 ILM 864 (1975).

EUMETSAT⁶ in this context.

For the purpose of GMES the establishment of a core entity provisionally labelled 'GMES Authority' is envisaged. Legal basis, status, role and competencies of such a body are yet to be determined. The documents so far referring to such a GMES Authority generally discuss various types of bodies or organs that can be established under EC law. Thus, mention has been made of such options as a Joint Undertaking⁷, an Executive Agency⁸, a Community Agency⁹ or a Joint Technology Initiative

6. The European Meteorological Satellite Organisation EUMETSAT was established by the Convention for the Establishment of a European Organization for the Exploitation of Meteorological Satellites (EUMETSAT), Geneva, done 24 May 1983, entered into force 19 June 1986; as amended 14 July 1994, entered into force 27 July 1994; Cmnd. 9483; Space Law – Basic Legal Documents, C.III.1; 44 ZLW 68 (1995).

7. Under Art. 171, Treaty Establishing the European Community (Consolidated Version) (hereafter EC Treaty); OJ C 325/33 (2002). The example usually referred to, of course, is the Galileo Joint Undertaking currently preparing the Galileo operational phases. See e.g. Communication of 3 February 2004, p. 17.

8. Cf. Council Regulation laying down the status for executive agencies to be entrusted with certain tasks in the management of Community programmes, No. 58/2003/EC, of 19 December 2002; OJ L 11/1 (2003); as well as, by way of example, Commission Decision setting up an executive agency, the 'Intelligent Energy Executive Agency', to manage Community action in the field of energy in application of Council Regulation (EC) No. 58/2003, No. 2004/20/EC, of 23 December 2003; OJ L 5/85 (2004); and Commission Decision setting up an executive agency, the 'Executive Agency for the Public Health Programme', for the management of Community action in the field of public health – pursuant to Council Regulation (EC) No. 58/2003, No. 2004/858/EC, of 15 December 2004; OJ L 369/73 (2004).

9. Cf. e.g. the European Environment Agency (EEA), established by Council Regulation on the establishment of the European Environment Agency and the European Environment Information and Observation Network, No. 1210/90/EEC, of 7 May 1990; OJ L 120/1 (1990); the European Aviation Safety Agency (EASA), established by Regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing

(JTI)¹⁰.

A final important point, of a more background/political nature but so far left largely unattended (at least in public discourse) concerns the involvement of GMES in security issues, in the field of outer space where traditionally 'defence' and 'security' have never been very far away. Whilst 'security' is broadly conceived so as to include civil security, involving not only terrorist threats but also the threats posed by natural or man-made disasters, it certainly also includes the more traditional security issues of a military and defence nature. GMES, whatever the 'GMES Authority' will come to look like, will have the European Union for a father and ESA for a mother.

Here, it must be noted that ESA, in accordance with its constitutive Convention, is supposed to "provide for and to promote, *for exclusively peaceful purposes*, cooperation among European States in space research and technology and their space applications, with a view to their being used for scientific purposes and for operational space applications systems".¹¹ Traditionally this has been interpreted as a ban on ESA involvement in any space activities of a military or defence nature, but it may be noted that already with Galileo that interpretation is shifting to a broader interpretation allowing such involvement, at least as long as of a purely defensive nature (alternatively being sanctioned at the UN-level).¹²

a European Aviation Safety Agency, No. 1592/2002/EC, of 15 July 2002; OJ L 240/1 (2002); and the European Maritime Safety Agency (EMSA), established by Regulation of the European Parliament and of the Council establishing a European Maritime Safety Agency, No. 1406/2002/EC, of 27 June 2002; OJ L 208/1 (2002).

10. See Communication from the Commission to the Council and the European Parliament – European Space Policy – Preliminary Elements, SEC(2005) 664, Brussels, 23 May 2005, COM(2005) 208 final.

11. Art. II, ESA Convention; emphasis added.

Similarly, the European Union is formally supposed to limit its activities to those not involving pure defence and military issues. The EU-pillar established to deal with common foreign and security policy is a straightforward intergovernmental construction, with at best a marginal role for the Commission as supposed guardian of the overarching European interest and no role for the elaborate legislative, adjudicative and enforcement jurisdiction developed in the context of the EC Treaty.¹³ In Europe, matters of international cooperation in the areas of defence and security have so far been essentially dealt with in the context of NATO¹⁴ or at best the Western European Union (WEU)¹⁵ – which, interestingly enough, has been drawn closer into the EU structures over the past few years. Also for the Union however, Galileo represents the first case where a more active and leading role in defence and security matters is

12. One of the key services which Galileo is going to offer concerns the Public-Regulated Service (PRS), which is going to be encrypted and provided with a certain measure of technical robustness against interference, and is intended for usage by government services or specific government-monitored or government-protected services (such as telecommunication or energy networks) only. Several EU member states have already indicated that they envisage usage of the PRS also by their respective militaries, though this has not been generally accepted yet. See on the set-up of Galileo and its services e.g. the author's *Liability for Global Navigation Satellite Services: A Comparative Analysis of GPS and Galileo*, 30 *Journal of Space Law* (2004), 145-52.

13. Cf. e.g. Artt. 2-5, EC Treaty, referring to the tasks and objectives of the Community, not offering any, even indirect, reference to matters of a defence or military nature, whilst also indicating that it "shall act within the limits of the powers conferred upon it by this Treaty and of the objectives assigned to it therein".

14. The North Atlantic Treaty Organisation (NATO) was established by the North Atlantic Treaty, Brussels, done 4 April 1949, entered into force 24 August 1949; 34 UNTS 243; TIAS No. 1964; 63 Stat. 2241.

15. The Western European Union (WEU) was established in its original version by the Treaty of Economic, Social and Cultural Collaboration and Collective Self-Defence, Brussels, done 17 March 1948, entered into force 25 August 1948, and repeatedly amended in the decades since.

becoming acceptable and accepted – with GMES following closely upon its heels.

Such growing involvement of both ESA and the Union in defence and security matters raises a number of questions as regards the legal issues playing in those areas. How has the possibility of GMES-generated data being of fundamental military or security interest been dealt with? How is a proper and acceptable measure of access to such data taken care of, balancing security and military interests of GMES-backing states with the professed contribution of GMES data to enhanced environmental and civil security calling for wide access possibilities?

The current article raises two sets of issues from this perspective. On the one hand, there are general security and dual-use issues, where existing international arrangements may have a bearing on the legal context within which certain GMES services might be provided. On the other hand, an international regime exists which is applicable to access to data resulting from remote sensing which may have its effects on GMES, and the possibilities to do what it is being established for, as well.

2. Security and dual-use issues

2.1. The Wassenaar Arrangement

The Wassenaar Arrangement is a formally non-binding arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies.¹⁶ It was designed to

¹⁶ Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (hereafter Wassenaar Arrangement), Wassenaar, done 19 December 1995, effective 12 July 1996. Currently, the following states are participating states in the Wassenaar Arrangement, with the states being members of the Union and/or ESA so indicated: Argentina,

promote transparency and greater responsibility in transfers of conventional arms, dual-use goods and dual-use technologies. Participating states commit themselves to ensure through national policies and, where appropriate, national regulations that cross-border transfers of these items do not contribute to the development or enhancement of military capabilities in states not participating in the Wassenaar Arrangement.¹⁷

The decision to actually allow or deny transfer of any item, however, remains the sole responsibility of each individual participating state.¹⁸ Thus, also, export controls differ from state to state in terms of documentation required, license fees, length of time to get a license, and duration of validity of the license.

The participating states only agree to *notify* transfers and denials, as well as to *control* (transfers of) all items in the List of Dual-Use Goods and Technologies and the List of Munitions, annexed to the Arrangement.¹⁹ Controls do not apply to technology or software in the public domain, to basic scientific research or to the minimum necessary information for patent applications. The Lists have two annexes, of sensitive items and of very sensitive items respectively, to which different levels of control should be applied, and are reviewed regularly to reflect

Australia, Austria (EU & ESA), Belgium (EU & ESA), Bulgaria (EU), Canada, Croatia, Czech Republic (EU), Denmark (EU & ESA), Estonia (EU), Finland (EU & ESA), France (EU & ESA), Germany (EU & ESA), Greece (EU & ESA), Hungary (EU), Ireland (EU & ESA), Italy (EU & ESA), Japan, Latvia (EU), Lithuania (EU), Luxembourg (EU & ESA), Malta (EU), the Netherlands (EU & ESA), New Zealand, Norway (ESA), Poland (EU), Portugal (EU & ESA), Republic of Korea, Romania (EU), the Russian Federation, Slovakia (EU), Slovenia (EU), South Africa, Spain (EU & ESA), Sweden (EU & ESA), Switzerland (ESA), Turkey, Ukraine, the United Kingdom (EU & ESA), and the United States.

17. See Art. I(1), Wassenaar Arrangement.

18. See Art. II(3), Wassenaar Arrangement.

19. See Artt. II(4), III(1), Wassenaar Arrangement; also Appendix 5.

technological developments.

Finally, the participating states agree to exchange general information on risks associated with transfers of conventional arms and dual-use goods and technologies in order to consider, where necessary, the scope for coordinating national control policies to combat these risks.²⁰

As to GMES, this means *inter alia* that the products and services envisaged by GMES might well turn out to be, explicitly but especially implicitly, included in the relevant List, resulting in potential obstacles to distribution of relevant GMES-generated information for the purposes of the environment and security. Much depends here on whether the recipients of GMES-generated information would be parties to the Wassenaar Arrangement themselves, so as to 'bind' them to applicable rules with regard to transfers outside the group of parties to the Wassenaar Arrangement.

2.2. Regulation 1334/2000

The Wassenaar Arrangement as such does not recognise the European Union in any substantive manner even as all of its members, with the single exception of Cyprus, are participating states. Partially as a result thereof, within Europe the same issue was also dealt with in a more classical, legally binding format by means of Regulation 1334/2000, which sets up a regime for the control of exports of dual-use items and technology, including cryptographic items, for the Union itself.²¹ An

20. See Art. IV(1), Wassenaar Arrangement.

21. Council Regulation setting up a Community regime for the control of exports of dual-use items and technology (hereafter Regulation 1334/2000), No. 1334/2000/EC, of 22 June 2000; OJ L 159/1 (2000). The Regulation has been amended and updated by Council Regulation amending Regulation (EC) No. 1334/2000 with regard to intra-Community transfers and exports

authorisation is required for export of the dual-use items listed in Annex I (which is essentially similar to the Wassenaar Arrangement's List of Dual-Use Goods and Technologies).

If the prospective exporter is aware that an item might be used in a way proscribed by the Regulation, it is bound to apply the applicable provisions, even if it is not listed in Annex I.²² Under the Regulation, export includes transmission of software or technology by electronic media, fax or telephone to a destination outside the Union.

As with the Wassenaar Arrangement, under Regulation 1334/2000 the responsibility for deciding on applications for export authorisations lies with the national authorities. Some items on the List of Dual-Use Items and Technology (Annex 1) are not controlled if they accompany the user and are for the user's personal use: Regulation 1334/2000 "does not apply to the supply of services or the transmission of technology if that supply or transmission involves cross-border movement of natural persons".²³

The Regulation establishes a Community General Export Authorisation (CGEA) for certain exports by means of Annex

of dual-use items and technology, No. 2889/2000/EC, of 22 December 2000; OJ L 336/14 (2000); Council Regulation amending Regulation (EC) No. 1334/2000 with regard to the list of controlled dual-use items and technology when exported, No. 458/2001/EC, of 6 March 2001; OJ L 65/19 (2001); and Council Regulation amending and updating Regulation (EC) No. 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology, No. 2432/2001/EC, of 20 November 2001; OJ L 338/1 (2001). The last Regulation updates and replaces the Annexes to Regulation 1334/2000 in order to take account of, *inter alia*, changes adopted by the Wassenaar Arrangement plenary session in December 2000.

²² See Art. 4, Regulation 1334/2000.

²³ Art. 3(3), Regulation 1334/2000.

II. Annex II, Part 1, specifies that the CGEA is possible for all dual-use items listed in Annex I, except those specified in Annex II, Part 2, dealing with the more security-sensitive items. National export authorities are not automatically obliged to provide a CGEA, however, and, in any event, the exporter must comply with the reporting requirements set out in Annex II, Part 3.

For all other items, authorisation shall be granted, if so, by the member state where the exporter is located.²⁴ This authorisation may be an individual, global or general authorisation. Member states must maintain or introduce in national legislation the possibility of granting a global authorisation to a specific exporter for dual-use items valid for export to one or more specified countries. The competent authorities may still refuse to grant an export authorisation and may annul, suspend, modify or revoke an export authorisation which they have already granted.²⁵ Finally, exporters are required to keep detailed records of their exports.

Once more, with a view to GMES, the Regulation may turn out to unduly and/or inadvertently obstruct the distribution of GMES-generated products and services. Those products and services may, certainly *prima facie*, be seen as dealing with dual-use and/or sensitive software or information, and, wherever this applies, the key players in GMES – notably the Commission and the EU member states – may soon be looking for ways to ensure exclusion of key GMES products and services from the scope of the Regulation's regime.

24. See Art. 6, Regulation 1334/2000.

25. See Art. 9, Regulation 1334/2000.

2.3. The United Nations system for international security

Finally, reference should be made briefly to the general global system for dealing with international security issues, as developed in the context of the United Nations. Under the UN Charter the United Nations has been given the major task by the member states to try and establish alternatively preserve international peace and security, within the competencies allotted to it.²⁶ Those competencies to a certain extent rest with the General Assembly, which has the possibility to issue (non-binding) Resolutions as well as to assert a role in despatching peace-keeping or peace-making forces, but especially with the Security Council, which has the power to issue binding Resolutions and initiate mandatory processes in this regard.

Under this system the Security Council may, for example, impose boycotts, economic blockades or even authorise full-fledged military actions if it considers international peace and security sufficiently threatened.²⁷ Throughout the last decades, these powers have been used in such cases as the Yugoslav civil wars (*vis-à-vis* Serbia in particular), the Iraqi invasion in Kuwait in 1990, and the military actions against Afghanistan in 2002 and Iraq in 2003.

The main point to keep in mind for GMES is that, should any such measures be imposed by the Security Council in the future, the relevant GMES actors would be bound to comply with them as well. It could be imagined in particular that certain data products or services would not be allowed to be delivered to certain parties, or that certain international cooperation

26. Charter of the United Nations (hereafter UN Charter), San Francisco, done 26 June 1945, entered into force 24 October 1945; USTS 993; 59 Stat. 1031; UKTS 1946 No. 67; Cmd. 6666 & 6711; ATS 1945 No. 1.

27. Cf. Artt. 41, 42, UN Charter.

ventures with certain parties on GMES-related issues would have to be suspended or cancelled in cases where the Security Council would determine a threat to international peace and security to exist.

2.4. Concluding remarks

The 'S' of GMES results in several issues of security and dual-use character requiring discussion in this context. Data generated by GMES, or information based on such data, could very well be subjected to the legal regime, summary as it may be, applicable to international transboundary movement of security-sensitive information or become involved in international actions trying to preserve international peace and security.

In particular once GMES starts generating its 'own' data this might well entail substantial limitations to GMES operations. In the last resort, however this should not qualify as much of a real obstacle in the way of GMES. The Union and its member states were actively engaged in matters relating to sensitive dual-use technology transfers from the beginning, and have also played an active role in protecting perceived security interests elsewhere, such as in the United Nations. It is only the natural course of things that GMES will not be allowed to somehow put those interests at risk by moving beyond the parameters resulting from the politico-legal environment described above. GMES might well work as a tool and a catalyst for further European involvement in such areas, and thus evolve into the main pillar under such involvement, at least as far as outer space is concerned – that is: if at least a proper, transparent, coherent and efficient institutional framework for legal decision-making will be established.

3. Access to remote sensing data

3.1. The international regime for access to remote sensing data

One of the most fundamental rules of space law is the principle of freedom of space activities.²⁸ Consequently, using satellites for remote sensing purposes is basically allowed. The Outer Space Treaty itself only provides for a few rather general principles to which any space activities should conform, such as international cooperation, mandatory supervision and authorisation of private space activities (for which a state is held responsible without further qualification), and *bona fide* efforts to minimise harmful effects of one's space activities, for example as to the environment.²⁹

Most notably, Article I calls for the "exploration and use of outer space" to be "for the benefits and in the interests of all countries"; Article III requires such activities to be "in the interest of maintaining international peace and security"; and Article IV imposes certain limits upon the freedom to use outer space for military purposes. Under the latter Article the stationing of weapons of mass-destruction in outer space is prohibited, whereas the Moon and other celestial bodies should only be used "exclusively for peaceful purposes". In conjunction with the former clause, the Test Ban Treaties furthermore prohibit the testing of nuclear weapons in outer space.³⁰

The specific issue of remote sensing, as a sub-set of space activities, at the global level has only been dealt with in any detail by UN General Assembly Resolution 41/65, adopted by consensus on 3 December 1986.³¹ Whilst the Resolution *per se*

²⁸ See also Art. I, Outer Space Treaty.

²⁹ See, resp., Artt. III, VI, IX, Outer Space Treaty.

does not constitute binding law, its adoption by consensus, as well as the general respect accorded to its contents, leads most experts to consider those contents to reflect customary international law.³² Thus, the – relatively scarce – state practice in terms of express national regulations and policies on access to remote sensing data confirms that states generally recognise the validity of the Principles as binding law *as such*, even if the interpretations may sometimes differ considerably. One may for example refer here to the main issue of discussion under the Resolution, which is that of ‘non-discriminatory access’ to data³³ – which might at least *prima facie* impose obligations also upon GMES which considerably limit certain elements of its envisaged activities from a legal perspective.

The level of agreement on this ‘non-discriminatory access’ principle and what it means in detail is not particularly impressive.³⁴ More importantly, certainly in the European context, it was not at all considering the possible use of data for military or even security purposes, whether in the context of the non-discriminatory

30. See Art. I(1.a), Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, Moscow, done 5 August 1963, entered into force 10 October 1963; 480 UNTS 43; TIAS 5433; 14 UST 1313; UKTS 1964 No. 3; ATS 1963 No. 26; Art. I(1), Comprehensive Test Ban Treaty, New York, done 24 September 1996, not yet entered into force.

31. Principles Relating to Remote Sensing of the Earth from Outer Space (hereafter Resolution 41/65), UNGA Res. 41/65, of 3 December 1986; UN Doc. A/AC.105/572/Rev.1, at 43; 25 ILM 1334 (1986).

32. See e.g. C.Q. Christol, *Space Law – Past, Present and Future* (1991), 73; K.R. Sridhara Murthi, Space Communications and Remote Sensing Applications in Asia and the Pacific: Technology and Legal Perspectives, in *2004 Space Law Conference* (2004), 244; M. Williams, The UN Principles on Remote Sensing Today, in *Proceedings of the Forty-Eighth Colloquium on the Law of Outer Space* (2006), 3-5.

33. Cf. Princ. XII, Resolution 41/65, which will be analysed in more detail *infra*, in para. 3.2.

34. Cf. e.g. the author’s Non-discriminatory data dissemination in practice, in *Earth Observation Data Policy and Europe* (Ed. R. Harris)(2002), 41-50.

access principle or even outside of it.

ESA for example had undertaken several comprehensive satellite remote programmes until the advent of GMES, inclusive of satellite operations, data handling and data distribution, such as the two European Remote Sensing Satellites ERS-1 and ERS-2, and the more recent Envisat, and published quite extended documents on the data policy to be applied.³⁵

In none of those cases however, did such a data policy make any specific reference to specific security-related reasons for non-disclosure of data, albeit that such non-disclosure could, if need be, come to be excused as not falling within the scope of non-discrimination. Moreover, it should be reiterated that so far ESA has not been mandated, or seen, to be involved in straightforward security-related activities. Finally, at the time of neither ERS nor Envisat data policy drafting, was the level of resolution taken into consideration such that militarily-relevant usage seemed around the corner – by default any unforeseen military customers respectively usages for example would probably have to be treated as commercial customers respectively usages.

By way of comparison, however, also in the case of the United States, where there would be no principled obstacles to involvement of remote sensing in security-related areas, this conclusion would apply. Neither in the United States Land Remote Sensing Policy Act of 1992³⁶ nor in any subsequent data policy documents was reference made to security let alone

35. E.g. for Envisat: the Envisat Data Policy, ESA/PB-EO(97)57 rev. 3, Paris, 19 February 1998, drafted by the Earth Observation Programme Board of ESA. See further G. Kohlhammer, The Envisat Exploitation Policy, in *ESA Bulletin* 106 (June 2001), 128-33.

36. Land Remote Sensing Policy Act, Public Law 102-555, 102nd Congress, H.R. 6133, 28 October 1992; 15 U.S.C. 5601; 106 Stat. 4163.

military usage of data *in direct reference* to the principle of non-discriminatory access – whilst such reference *was* made at a considerable number of other places in those documents.

Thus, the examples of two rather distinct key players in the world-wide application of, for example, the Wassenaar Arrangement, already show a certain acknowledgment of the authority of Resolution 41/65 in this field, but without any connection at all to security-related remote sensing activities. This then can only be interpreted – with reference also to Article I of the Outer Space Treaty and the fundamental principle of freedom of space exploration and use pronounced by it – as meaning that such security-related usage of remote sensing data does not fall within the scope of the ‘non-discriminatory access’ principle.

In other words: one does not need to be bothered by this principle when deciding to (not) disseminate certain data from remote sensing satellites which are clearly in the military and security domain – something reinforced of course by the confinement, in the last resort, of the Resolution to remote sensing “for the purpose of improving natural resources management, land use and the protection of the environment”.³⁷

3.2. The substance of Resolution 41/65

Analysis of the substance of Resolution 41/65 further confirms the above conclusion. For a start, it acknowledges the freedom of remote sensing activities, as one particular manifestation of the freedom of space activities subject only to international law.³⁸ Further to this, the Resolution provides some important parameters for remote sensing activities.

³⁷ Princ. I(a), Resolution 41/65.

³⁸ See Princ. III, Resolution 41/65.

Firstly, it should be reiterated that the Resolution applies to remote sensing activities “for the purpose of improving natural resources management, land use and the protection of the environment”.³⁹ Since such usage arguably would not require the quality of spatial resolution of better than in the range of 10 metres, any very high resolution (VHR) data issues might fall outside the scope of the Resolution. Following from this, somewhat narrow, definition of remote sensing for the purposes of the Resolution, it excludes many activities relevant from a security perspective from its scope.

Then, Principle II provides that “Remote sensing activities shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic, social or scientific and technological development, and taking into particular consideration the needs of the developing countries”. Actually, this Principle very much supports the general establishment of GMES, although it also raises some questions as to the extent in which such benefits are to be created in a mandatory fashion.

Here, the frequently-found and rather general reference to “the benefit and (...) interest of all countries” with special consideration for the developing countries was developed further by means of another UN Resolution in 1996.⁴⁰ This Resolution left complete freedom to states “to determine all aspects” of such cooperation, and furthermore repeatedly referred to the requirement of “an equitable and mutually acceptable basis” for any activities undertaken in its implementation.⁴¹

³⁹ Princ. I(a), Resolution 41/65.

⁴⁰ Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of all States, Taking into Particular Account the Needs of Developing Countries (Resolution 51/122), UNGA Res. 51/122, of 13 December 1996; XXII-I Annals of Air and Space Law (1997), at 556; 46 ZLW (1997), at 236.

⁴¹ See Princ. 2, 3, Resolution 51/122.

Principle IV of Resolution 41/65 then deals with the core issue of satellite remote sensing: the dilemma between the freedom of use of outer space, in its particular manifestation of freedom of information-gathering making use of satellites, and the principle of sovereignty of states over their own territory, more in particular over their own wealth and natural resources. These two concepts collide where the 'sensed state' finds itself in a situation that a 'sensing state' might obtain valuable information, especially in economic terms, with regard to the territory of the 'sensed state' which that state itself does *not* possess.

A balance of sorts has been established by the Resolution, which in the final analysis tilts towards the freedom of remote sensing activities. The principle of full and permanent sovereignty, it is true, is to be respected, consequently legitimate rights and interests of the 'sensed state' shall not be harmed, and also the benefit and interest of *all* countries shall be taken into account (that is, including those of the 'sensed state').⁴² All this, however, does not alter the fact that the 'sensed state' neither has a veto to prevent it from being 'sensed', nor an exclusive, free or preferential right of access to the data, nor is it entitled automatically to becoming a partner in the relevant remote sensing operations.⁴³ This becomes especially clear when these principles are seen in conjunction with Principle XII, since for the purpose of a particular set of remote sensing data concerning its territory the 'sensed state' is no different from any other state interested in such data.

Principle XII namely provides: "As soon as the primary data and the processed data concerning the territory under its jurisdiction are produced, the sensed State shall have access to them *on a non-discriminatory basis and on reasonable cost*

⁴² See Princ. IV, Resolution 41/65.

⁴³ Cf. Princ. XIII, Resolution 41/65.

terms. The sensed State shall also have access to the available analysed information concerning the territory under its jurisdiction in the possession of any State participating in remote sensing activities on the same basis and terms, particular regard being given to the needs and interests of the developing countries.”⁴⁴

In terms of further legal parameters to the freedom to distribute remote sensing data or not, finally two further Principles contained in Resolution 41/65 are of special importance with a view to GMES, even though such importance is more directly related to the 'E' of 'environment' than to the 'S' of 'security'.

Firstly, Principle X provides: “Remote sensing shall promote the protection of the Earth’s natural environment. To this end, States participating in remote sensing activities that have identified information in their possession that can be used to avert any phenomenon harmful to the Earth’s natural environment shall disclose such information to States concerned.”

Secondly, in rather similar fashion Principle XI provides: “Remote sensing shall promote the protection of mankind from natural disasters. To this end, States participating in remote sensing activities that have identified processed data and analysed information in their possession that may be useful to States affected by natural disasters, or likely to be affected by impending natural disasters, shall transmit such data and information to States concerned as promptly as possible.”

Principle XI thus largely mirrors Principle X; the latter dealing with man-originating threats to the natural environment of the Earth, the former with nature’s threats against mankind. The main noticeable difference with Principle X is that Principle XI explicitly applies to “processed data” in addition to “analyzed

⁴⁴. Emphasis added.

information”, as opposed to mere “information”.

Neither of them, finally, alter the conclusion that military and other traditional security issues were not addressed at all by the Resolution, which therefore cannot provide any specific guidance regarding how GMES data of such a nature are to be distributed, read handled. This leaves GMES authorities, at least as far as the Resolution is concerned, with the principal freedom to decide on any distribution policy of data for military and defence purposes as they see fit; no obligation of non-discriminatory access, whatever its precise scope and reach, can interfere therewith.

3.3. The Charter on Space and Major Disasters

Of major impact in some of the areas where GMES is going to become active, the Charter on Space and Major Disasters focuses directly and exclusively on the mitigation of major disasters and their harmful effects without creating any new international organisation.⁴⁵

The Charter was established by a number of leading space agencies with operational remote sensing capabilities, initiated by ESA, one of the two ‘founding fathers’ of GMES, and the French space agency CNES in 1999 as a follow-up to the Unispace III Conference, where the potential of earth observation in the context of major disasters was prominently discussed.⁴⁶ It also represents a specific manifestation of such general principles of space law as pertaining to the benefit of all countries and the requirement to allow free and uninhibited

45. See http://www.disasterscharter.org/main_e.html. The full name is “Charter On Cooperation To Achieve The Coordinated Use Of Space Facilities In The Event Of Natural Or Technological Disasters”.

46. See e.g. Report of the Third United Nations Conference on the Exploration and Peaceful Uses of Outer Space, A/CONF.184/6 (1999), 33-7, 64.

access to data if natural or man-made disasters are at hand, as discussed above in the context of Resolution 41/65.⁴⁷

In due course, the Canadian Space Agency (CSA), the US National Oceanic and Atmospheric Administration (NOAA), the Indian Space Agency ISRO, the Argentine National Commission on Space Activities CONAE and most recently the Japanese Aerospace Exploration Agency (JAXA), the United States Geological Survey (USGS) and the Disaster Monitoring Constellation (DMC) joined, so that the Charter currently counts nine full-fledged partners.⁴⁸

The Charter, declared formally operational on 1 November 2000, aims at providing a unified system of space data acquisition and delivery to those affected by natural or man-made disasters — and thus is clearly operative in the same areas GMES envisages to address. Each member agency has committed resources to support the provisions of the Charter and thus helps to mitigate the effects of disasters on human life and property: ESA provides data from ERS and Envisat, CNES from the SPOT satellites, CSA from the Radarsat satellites, ISRO from the IRS satellites, NOAA from the POES and GOES satellites and CONAE from the SAC-C satellite.

Article 6(1) of the Charter provides that requests to adhere to it may be made by any space system operator or space agency with access to space facilities agreeing to contribute to the commitments made by the parties. In other words, it is a *de facto* prerequisite for membership to possess the capability to operate satellite systems. Such capability is not necessarily limited to earth observation satellites or instruments; “space systems for observation, meteorology, positioning, telecommunications and

47. See Art. I, Outer Space Treaty; Princ. X, XI, Resolution 41/65.

48. See http://www.disasterscharter.org/participants_e.html.

TV broadcasting or elements thereof such as on-board instruments, terminals, beacons, receivers, VSAT's and archives" are also acceptable.⁴⁹

Upon request by a "beneficiary body", the member agencies acquire the data of the area affected by the disaster from their satellites, process the data into images, analyse them further if necessary, and distribute the resulting information free of charge to those states affected by the disaster via "associated bodies"⁵⁰. It is explicitly provided that a state affected by disaster which requests access to certain data needs to contact relevant associated bodies – or "cooperating bodies"⁵¹ acting in partnership with an associated body.

The effective determination of which satellites are to provide data for a particular disaster is facilitated by prior scenario-writing, anticipating which data and information would be useful for which types of crisis. The parties shall together analyse recent crises for which space facilities could have provided or did provide effective assistance to the authorities and rescue services concerned, draw conclusions and prepare sample response plans for such future events.⁵² A scenario covers such issues as the type of sensors effective for specific disasters and selection

49. Art. 1, Charter on Space and Major Disasters.

50. Art. 5(2), Charter on Space and Major Disasters; an "associated body" is "an institution or service responsible for rescue and civil protection, defence and security under the authority of a State whose jurisdiction covers an agency or operator that is a party to the Charter".

51. Cooperating bodies include the European Union, the other 'founding father' of GMES, the UN Bureau for the Coordination of Humanitarian Affairs and other recognized national or international organizations with which the parties may have cause to cooperate in pursuance of the Charter. A "cooperating body" does not operate a space system but acts in partnership with an associated body which does; see Art. 3(5), Charter on Space and Major Disasters.

52. See Art. 4(2), Charter on Space and Major Disasters.

criteria for use of a specific satellite.

The Charter has so far helped and will continue to be of help in a large number of rather varying events; not only in developing but certainly also in developed countries. With a view to GMES then, the main consequence following from the development of the Charter concerns the respective roles of ESA and the European Union, which make it rather likely for GMES to become closely involved in Charter activities, or even actually take over the implementation of European contributions to Charter operations in the future. As the Charter, however, operates on a 'best efforts' basis and legally speaking does not constitute a comprehensive closed and binding system, it would be rather unlikely for it to result in obligations for GMES to disseminate data in case that would result in a threat to the security of the European states involved. Rather, GMES would more often than not be helpful for those states to further the cause of the Charter in bundling efficiently relevant space activities.

3.4. General humanitarian obligations

Both the international space law-rules pertinent for remote sensing and the Charter on Space and Major Disasters effectively are representations of a broader, general international law-duty for states to assist other states and their peoples in cases of larger humanitarian disasters, whether natural or man-made. As to the latter, understandably from a realistic politico-legal perspective but of course very unfortunately, these exclude those man-made disasters created by wars, persecution and other forms of violence, since in particular those states where events in these categories take place are generally unwilling to have other states come to the rescue merely on humanitarian grounds.

Since precisely those last categories of man-made disasters

are at the heart of the 'S' of 'security', reference must still be made (even if briefly) to the existence of these underlying general humanitarian principles which do, in principle, apply to security issues as well. Though they would apply also in cases not covered by either the international space law-regime or the Charter (whether *ratione materiae* or *ratione personae*), and as such would have a general bearing on a number of GMES activities, their main disadvantage from a more practical perspective is their very broad and vague content. At every turn a different set of issues and situations are at stake, making it very difficult to determine what, in any particular case, such general humanitarian duties would amount to in terms of, for example, concrete actions or measures.

Thus, to give one particularly interesting and illustrative example, the obligations to provide data to a sensed state could well come into conflict with the obligation to act for humanitarian considerations. This would arise in a case where refugees were fleeing persecution by a ruling regime in a given state, and the location of such refugees would be of equal interest to the aid agencies and to the ruling authorities – in the latter case for all the wrong reasons.

For that reason, these obligations should be best perceived as obligations-of-effort, as opposed to obligations-of-result. Their practical reach remains to be determined for each specific instance, and in the last resort they may serve more as guidelines to prefer one course of action over another if, all other things essentially equal, the first course would be more in tune with such humanitarian obligations.

3.5. Concluding remarks

For purposes of realising GMES, especially the general

international law-regime on access to remote sensing data and the more specific requirements under the Charter resting upon key GMES players such as ESA should be taken into account. In the second phase of GMES this would also apply to any satellite data directly generated from 'GMES satellites'. These regimes would considerably limit the discretion of any key GMES entity in deciding whether and how to distribute certain data under GMES.

Whoever would be in the driver's seat for GMES satellite activities should be aware of these regimes, and monitor their further development as to substantial effects on his own discretion with respect to GMES data distribution. This reverts back to the roles of, firstly, any 'GMES Authority' to be developed, and secondly, the Commission and/or the EU member states.

Once more, however, upon closer look the existing regimes do not in any essential measure provide obstacles for GMES – on the contrary, it would be surprising if the rather loosely-formulated restrictions to the freedom to (not) disseminate certain data would suddenly be applied very rigorously to a system which is generally designed to work in the favour of mankind's need for environmental and other security. The proof of the pudding is in the eating, however; and for the pudding to be digestible, a proper, transparent, coherent and efficient institutional framework for decision-making on GMES and GMES-related security and military issues is requisite.

4. Towards properly integrating the 'S' into GMES

In the final analysis, it seems that GMES will not meet with many undue legal obstacles coming from the two areas of security issues respectively data access. The inherent limitations coming from the former area are already well-known to the

member states of the Union and ESA behind GMES, and moreover leave some room for improvement when it comes to developing a proper balance between security interests in the traditional sense – which generally call for restriction of access to, and usage of, data – and security interests in the more modern sense, which generally would call for as widespread availability and usage of data. The nascent legal regime developing in the latter area on the other hand seem to be hardly relevant so far, in legal terms, for the issues surrounding the involvement of GMES in any type of security issues.

Thus, the issues are more of a fundamentally political nature, referring to the acceptability of growing involvement of both the Union and ESA in areas close to, even overlapping traditional areas of defence and military security; a development already gaining steam under the existing legal/institutional European construct, but soon requiring a more solid and appropriately renewed legal/institutional basis.

Rather than being fundamentally hindered by the existing rules of the road or in danger of operating against main relevant premises and principles – of which this article focused on the two areas coming closest at the moment to an international *legal* regime – GMES would likely even grow into a component part of that legal/institutional regime, and thus help to shape future legal developments in this field.

It might well do so, for example, by acting as a counterweight to Wassenaar-type of restrictions on data access, as they might be perceived by non-participating states from a negative perspective, and come to represent the ‘sharing side’ of European space efforts rather than the ‘excluding side’. Similarly, GMES may help to develop the loose and overtly-political regime on data access into a more legalistically-phrased, clear-cut and coherent legal regime, by its own practices as they will evolve,

and equally may help to further boost the benefits of the Charter on Space and Major Disasters to mankind.

To what *extent* GMES will actually be able to achieve such contributions then crucially depends upon the governance structure to be developed for GMES by the European member states with a view to the global context in which GMES is going to operate, including the Global Earth Observation System of Systems (GEOSS). Whatever its precise outlines, whether Joint Undertaking, Executive Agency, Community Agency, JTI or even a newly established international entity; it should be properly structured in terms of size and competencies, transparent in its decision-making and balancing of military security respectively environmental and civil security interests (wherever the two may run counter to each other), coherent in making certain the outcome binds – or at least guides – all European stakeholders, and efficient in not reinventing wheels or redoubling the efforts of organisations and bodies already involved in the field. In other words: the 'S' should be integrated properly into GMES.

In that sense finally, it is certainly appropriate to expect that GMES will be a further manifestation of the transformation of the fundamental principle of Article I of the Outer Space Treaty into practical realities: that space should be used “for the benefits and in the interests of all countries”, both developing and developed, both spacefaring and non-spacefaring.