Security and Potential (Anti-) Terrorism Aspects of High Resolution Earth Observation Data

*Fabio Tronchetti**

Abstract

The use of high resolution space earth observation data is certainly beneficial for a broad array of civil purposes but, at the same time, raises numerous legal questions related to the possible misuse of such data. An area of particular concern is that of security, as the dissemination and utilization of high resolution space products can potentially undermine the security of states both at international and national level. For example, in the hands of terrorists, these data can be employed to threaten public order. The security implications of high resolution space earth observation data are magnified, on one side by the increasing availability of these data and, on the other side, by the fact that access to them is provided by both states and private operators.
Legal and technical regulations and procedures to prevent the misuse of high resolution earth observation products are already in place; however, their ability to effectively counteract the growing security threats associated with the utilization of these products can be questioned. The purpose of the present paper is to analyze the extent to which the law' currently does, viz. will, viz. should regulate the security implications and the potential misuse of data, both by governments private subjects, e.g. terrorists or hacker groups. In doing so, the paper will explore the feasibility of introducing protective mechanisms, such as 'firewalls' and criminalization of leaking data, in a comprehensive manner into the space sector.

1 Introduction

High resolution satellite images are a useful but dangerous tool.[1]
On one side, thanks to their remarkable accuracy, they find application in a wide spectrum of civil areas such as facility management, land use planning,

* Fabio Tronchetti, Associate Professor of Law, School of Law, Harbin Institute of Technology, China; Adjunct Professor of Comparative National Space Law, School of Law, University of Mississippi, United States.

1 A description of the characteristics of high resolution satellite images is provided in I. Dowman, G. Konecny, K. Jacobsen, R. Sandau, High Resolution Optical Satellite Imagery, Whittles Publishing, 2012.

precision agriculture, location of ground water and water management, transportation, emergency services, environmental impact assessment.[2] On the other side, because of the same technical characteristics that make them so valuable from a civil perspective, high resolution satellite images hold a potentially destabilizing effect both from an international and national point of view.[3] Indeed, they may reveal sensitive information about a certain State, such as the movement and position of its troops on the ground or the location of its military facilities and weapons deposits, that ultimately threaten its national security. If this information fall into "wrong hands", either those of an enemy State or a terrorists group, they may be used as a powerful means to enhance the deadliest nature of an attack against the former State (or its troops). The risks to national security associated with access to high resolution images are gradually expanding due to the largest availability of these images on the market, the role of internet and the presence of private operators that distribute these products on a worldwide basis. It is, thus, not surprising that States have put in place measures to preserve their national and foreign policy interests in particular by controlling the activities of high resolution satellites operators and data providers, limiting the spatial resolution of the images released on the market and restricting distribution of and access to high resolution satellite products.

The purpose of the present paper is to assess the risk that the release of high resolution images poses to national and international security, evaluate the ability of national remote sensing legislation to deal with and mitigate such risk, and discuss whether additional measures are needed. The paper argues that national legislation, despite not being able to eliminate all threats associate with the distribution of high resolution images, does an adequate job in preserving national (and international) security interests. Nevertheless, in the light of some recent legislative developments in the US, enabling private remote sensing operators to sell very high resolution satellite images, some amendments to the existing licensing conditions regulating the activities of these operators may be advisable.

---

2 Generally, on remote sensing see J.B. Campbell, Introduction to Remote Sensing (3d edition). New York: Guilford Press, 2002.

3 On this point see J.I. Gabrynowicz, The Land Remote Sensing Laws and Policies of National Governments: A National Survey, prepared for U.S. Department of Commerce/ National Oceanic and Atmospheric Administration's Satellite and Information Service.

2 The 21st Century: Worldwide Accessibility to High Resolution Satellite Images

The term high resolution satellite images refers to high spatial and geometric resolution images collected by a satellite.[4] Although there is no uniform definition of "high resolution", images with a resolution ranging from 5.8 meters to well under 1 meter are generally catalogued as "high resolution". For example, the newest commercial satellites such as World-View 3 and GeoEye-1 are capable of generating respectively 31 cm and 41cm resolution panchromatic and 5ft (1.65m) multispectral (color) imageries. High resolution imagery is similar to aerial photography but provides coverage for larger areas, more quickly, and do not face the restrictions deriving from flying within national airspaces.

Until recently access to high resolution images was reserved to a restricted number governments which either operated high resolution satellite systems or purchased high resolution products from their allies. Nowadays, the situation has completely changed: virtually anybody, including private individuals, with internet access and a credit card may acquire high resolution satellite images from a wide array of providers located in the US, Europe, Germany, India, etc.

The present environment is the result of political decisions and legislative measures that facilitated the involvement of the private sector in the remote sensing sector and pushed for the commercialization of remote sensing products.

The first fully private high resolution satellite, IKONOS, was launched in 1999 by the then SpaceImaging, later renamed GeoEye. Notably, GeoEye has been recently incorporated in DigitalGlobe which, thus, remains the sole private operator as well as distributor of high resolution satellite products in the US. [5]

Importantly, the involvement of private entities in the remote sensing business is not limited to the US. For example, the Canadian high resolution satellite RADARSAT-2 (highest resolution is 1 m in Spotlight mode and 3 m in Ultra Fine mode) is operated by Macdonald, Dettwiler and Associates, which also distributes RADARSAT-2 images. [6] Another example is represented by the Pléiades constellation, which consists of two very-high-resolution optical Earth-imaging satellites (0.50 m resolution images). The private company Spot Image is the official and exclusive worldwide distributor of Pléiades products and services under a delegated public service agreement with the French Space Agency (CNES). Similarly, in Germany the

4 See at http://www.ssec.wisc.edu/airportexhibit/files/side4.pdf
5 See at http://www.digitalglobe.com.
6 See at http://gs.mdacorporation.com/SatelliteData/Radarsat2/Radarsat2.aspx.

TerraSar-X and TanDEM-X high resolution satellites are operated by the German Aerospace Centre but Airbus Defence and Space distributes their products on a worldwide basis.[7]

3 Commercialization vs. Security: a Fundamental Dilemma

A crucial issue affecting the high resolution satellite sector is how to reconcile the commercialization of high resolution satellite products with the preservation of national (and international) security interests.

Selling high resolution satellite images and related products to the broadest array of national and international customers is, of course, a primary business strategy of high resolution satellite operators and data providers, particularly those of private nature. However, it is in practice also a vital need. Remote sensing is not a self-sustaining industry. Private operators require support from their governments, either in the form of financial contribution, partnership or with the government and its agencies acting as primary customer of the operator's services. Thus, the global release of remote sensing products, including those of high resolution nature, is the only way to ensure the long-term sustainability of a (private) remote sensing business, especially considering the level of competition among providers of high resolution services.

Nevertheless, the increasing availability of high resolution satellite images rather inevitably threaten national (and international) security. Until satellite imagery at high resolutions were strictly in the hands of governments, there were little security concerns as access to and dissemination of them was tightly controlled in the interest of national security. Nowadays, due to presence of private operators distributing high resolution satellite products worldwide as well as the increasing competition among these operators, the possibility that these products might fall into the hands of terrorists groups or 'rough'States and be used to purport attacks against the national State of the data provider or to undermine its national security in a broader sense, exists. This may, theoretically, occur in several ways, for example by: 1) direct purchase of an image or product; 2 indirect acquit ion through the purchase by a third party; 3) un-authorized access to the provider's informatics system and images storage.

In order to safeguard national security and preserve foreign policy relations and interests States have taken measures to control the activities of private remote sensing operators and the distribution of high resolution satellite images and products. Such a control is undertaken by means of licenses which apart from authorizing a certain subject to operate a satellite or to commercialize high resolution images, establish detailed conditions under

[7] See at http://www.astrium-geo.com/terrasar-x/.

which such activities should be carried out. Usually, licenses impose restrictions on the spatial resolution of the images to be distributed and on the countries or subjects to whom these images can be distributed. Licensees are requested to screen every request from a security point of view, verify the identity of the customer (this is often done pursuant to a 'black list'of potential terrorists), ascertain the purpose of its purchase and the intended use of the image. Certainly, under the existing rules, the licensee plays a pivotal role in ensuring that the distribution of high resolution images does not endanger national security or destabilize international relations. However, licensing authorities are entitled to monitor the authorized activities and their compliance with the terms of the license through inspection and access to data storage. In case of violation licensee can face administrative and financial fines and, in case of serious violations, criminal charges.

4 International and National Legal Framework

a) *Preliminary considerations*

International law provides fundamental but general principles regulating the operation of remote sensing satellites and the collection and distribution of images of the Earth from space. National law provides the licensing procedure for private remote sensing operators and the conditions governing the commercial release of remote sensing products.

b) *International law*

International law recognizes States with the right to freely launch and operate remote sensing satellite as well as to 'sense'the Earth from space. The freedom of 'passage'in outer space and the right of sensing, which were first proposed by the United States, have been accepted by the international community and incorporated in Article I (2) of the 1967 Outer Space Treaty[8] and in the UN Remote Sensing Principles.[9] In short, States need no authorization to carry out remote sensing activities from space and are not obliged to obtained a permission from the sensed State before sensing its territory. Nevertheless, as per Principle IV of the Remote Sensing, remote sensing activities "shall be conducted on the basis of respect for the principle of full and permanent sovereignty of all States (countries) and peoples over their own wealth and natural resources, with due regard to the rights and

[8] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies, 18 U.S.T. 2410; TIAS 6347; UNTS 205 (hereinafter referred to as "Outer Space Treaty"). Article I (2) reads as follows

[9] UNGA Res. 41/65 of 3 December 1986, Principles Relating to Remote Sensing of the Earth from Space.

interest of other States (country)....Such activities shall not be conducted in a manner detrimental to the legitimate rights and interests of the sensed State."A relevant question is whether the selling of a very high resolution image of a State's territory, for example showing sensitive facilities, may be considered a conduct detrimental to its legitimate interests and a threat to tits national security.

In terms of the distribution of remote sensing images and products, including those of high resolution nature, the Remote Sensing Principles establish the principle of nondiscriminatory access of the sensed State over data and products concerning its territory. [10]Accordingly, 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 terms, provided that it requests them. However, the sensing State does not have to obtain prior authorization from the sensed State before selling images of its territory to third parties. Importantly, Article VI of the Outer Space Treaty makes States internationally responsible for the space activities of their nationals and requires them to authorize and control those activities. This Article provides the legal foundation for the setting up of licensing regimes for private remote sensing operators.

5 Selected National Remote Sensing Legislation

a) *United States*

The United States has the most developed remote sensing legislation of the world; indeed, starting from 1984, it has formulated a series of laws, policies, and presidential directives regulating remote sensing activities.

The foundation of US Remote Sensing Law is constituted by the 1992 Land Remote Sensing Act: the Act is complement by the 1994 Presidential Directive PDD-23, the 2003 Remote Sensing Policy and the 2006 National Oceanic and Atmospheric Administration (NOOA)'s Final Rule on the Licensing of Private Land Remote Sensing Space Systems.[11]

US remote sensing policy is characterized by two elements: 1) the promotion and support of private involvement in the remote sensing sector; 2) the national and international distribution of remote sensing products. The US government not only financially supports US private remote sensing operators, such as DigitalGlobe, but it also purchases the majority of their data. Furthermore,

[10] Principle XII, Principles Relating to Remote Sensing of the Earth from Space.

[11] For a description of US remote sensing law see J.I. Gabrynowicz, One half century and counting: the evolution of US national space law and three long-term emerging issues, 4 Harward Law & Policy Review 405 (2010), J.I. Gabrynowicz, The perils of Landasat from grassroots to globalization: a comprehensive review of US remote sensing law with a few thoughts for the future, Chicago Journal of International Law (2006).

legal roadblocks to the development and operation of commercial satellites with resolution in the area of 1-2 feet have been removed.

The preservation of national security interests and foreign policy obligations related to the operation of remote sensing satellites and the distribution of remote sensing products are of paramount importance for the US. Significantly, the 2006 NOOA Rules on Licensing of Private Remote Sensing points out that: "The regulations in this part are intended to: (1) Preserve the national security of the United States; (2) Observe the foreign policies and international obligations of the United States; (3) Advance and protect U.S. national security and foreign policy interests by maintaining U.S. leadership in remote sensing space activities."

The main instrument to protect national security and foreign policy interest is the license. Under US remote sensing legislation every (private) land remote sensing operator is requested to obtain a license from NOAA, which is the agency responsible for licensing and regulating the remote sensing industry. License applications are reviewed by the competent authorities based on their potential threat to US national security and foreign policy interests.

First of all, licensees arerequired to maintain operational control from a domestic location at all times, the ability to override commands, to keep an archive of their activities/transaction and to make these data available for inspection. Secondly, licenses may contain a series of conditions restricting the operations of the commercial systems in order to limit collection and/or dissemination of certain data and products, for example in terms of resolution and time of delivery. Until recently, commercial operators were prevented to sell images with a spatial resolution better than 0.50 m. Importantly, every license application is reviewed on a case-by-case basis and specific conditions are set up individually for each operator. On a case-by-case basis the US government may require additional conditions. Significantly, the Secretary of Commerce, in consultation with the Secretaries of State and Defense, has the authority to "require the licensee to limit data collection and/or distribution by the system to the extent necessitated by the given situation"(the so-called "shutter control") or to give priority distribution to the US government. While the shutter control provisions has never officially been utilized, many scholars claimed that it was effectively utilized when the US acquired all the IKONOS images of Afghanistan before the US campaign against the Taliban militias.

Compliance with the licensee conditions is made by the Secretary of Commerce. He/she can take enforcement measures, such as inspection, audit, size of data, and demand the US Attorney to issue an order of injunction to suspend or terminate the license. In addition, violator may be assessed a civil penalty by the Secretary of not more than $10,000 for each violation. Each day of operation in violation constitutes a separate violation. US remote sensing law does not included specific criminal consequences but the violator may face criminal charges based on other US legislation.

b) *Germany*

German remote sensing activities are regulated under the 2007 German Act on Satellite Data Security. The Act, which was directly connected with the preparation and launch of the first German high resolution satellite, TerraSar-X, has a double purpose: 1)
to safeguard the security and foreign-policy interests of the Federal Republic of Germany in connection with the dissemination of satellite-generated earth remote sensing data particularly on international markets; 2) to create legal certainty for companies interested in satellite data marketing.[12]The TerraSar-X project (as well as its sister project TanDEM-X) is based on a collaboration between the public and private sector in the form of a Public Private Partnership (PPP). The satellite is operated by the German Space Agency (DLR) while the private company EADS Astrium holds exclusive commercialization rights. Data can be sold to the private and public sectors both domestically and internationally.
The Act is applicable to High-Grade remote sensing systems operated by German nationals or foreign legal persons register in Germany.[13] High-Grade remote sensing systems are those systems capable of acquiring data of particular high information content.
The Act sets up a double licensing procedure, respectively for operators of high grade remote sensing systems and data providers. Licensees have to comply with a series of conditions aimed at preserving national security and facilitating control by the licensing authorities.
The core of the Act is represented by the procedure for dissemination of data, which is especially relevant in case of first-time distribution. Every data request must undergo a sensitivity review aimed at assessing the possibility of harm being caused to the vital security interests of the Federal Republic of Germany, to the peaceful co-existence of nations or to the foreign relations of the Federal Republic of Germany.[14] This review is performed and falls under the full responsibility of the data distributor. In doing so, the provider must follow a predetermined set of procedures and criteria without any power of discretion. Factors to be taken into account when undertaking a sensitivity review include: a) the identity of the customer; b) the content of the product; c) the target area; d) the time elapse between data request and acquisition; e)

[12] B. Schmidt-Tedd/M. Kroymann, Current status and recent development in German remote sensing law, 34(1) J. Space L. 97 (2008).

[13] Section 2 (4) of the German Act on Satellite Data Security defines High-Grade Remote Sensing Systems as "a space-based transport or orbital system, including the ground segment, by means of with data about the earth are generated, where its sensor is itself/sensors are themselves technically capable either alone or in combination with one or more other sensors of generating data with a particularly high information content within the meaning of Para (2)."

[14] Section 17.2.4, German Act on Satellite Data Security.

location of the ground segment to which the data is to be transmitted. The data provider is obliged to document and record any transaction for possible official audit/inspection.
If the request is deemed to be "non-sensitive", the distributor is free to deliver the data; on the contrary, if the transaction is "sensitive", the data provider cannot automatically sell the data/image and shall request a permit from the governmental authority, in this case the Federal Office of Economics and Export Control, BAFA). The Federal Office then conducts a case-specific review to evaluate whether the customer request would endanger the security of the Federal Republic. If the risk is excluded, a permit is issued for the data provider to comply with the request. Another possible result of the review is to rule out a risk if the data request is altered slightly, for instance, lowered resolution, time delay, reduced processing quality of the data, or the omission of certain target areas. In such cases, the authorities issue conditional authorizations. If the risk is still deemed high despite potential conditions, the permit will be refused.
The operator and the data provider are requested to make sure that the transmission of commands/data is carried out by means of a method declared secure by the German governmental authority. Furthermore, these subjects shall provide information, documentation and enable inspection when the responsible authority so requires. The data provided must give priority to request for dissemination of data from the Federal Republic of Germany in case of exceptional (defense and security related) circumstances.[15]
Depending on the gravity of the violation of the license terms, the licensee may be charged with administrative or criminal offenses. The former are sanctioned with a fine ranging from 50 to 500 thousands euros, while the latter is punishable with a fine or a term of imprisonment of up to five years.[16] Criminal offenses are deliberate acts (such as the dissemination of data without license or the failure to undertake the sensitivity check) that undermine the national security and foreign policy obligations of the Federal Republic of Germany.

c) *Canada*

The 2007 Remote Sensing Act is the main document regulating Canadian remote sensing activity. The Act establishes rules for the operation of remote sensing space systems and for the dissemination of images and products.
The adoption of the Act was prompted by the involvement of the private sector in the remote sensing business and the need to ensure that the commercialization of remote sensing data would not endanger Canadian

[15] Section 21, German Act on Satellite Data Security.
[16] Sections 28 and 29, German Act on Satellite Data Security.

national security and foreign policy interests. A decisive factor were the facts that: a) the new RADARSAT-2 satellite was owned and operated by MacDonald Dettwiler and Associates Ltd. (MDA); b) the high resolution SAR [17] images that RADARSAT-2 was able to produce represented a potential threat to the security of Canada and its allies.

The core of the Act is represented by the licensing process and conditions as they enable control over the activities of remote sensing operators, particularly those of private nature. As far as the operation of a satellite, the Act emphasizes that they shall be secure from cradle to grave. In other words, positive control of a satellite shall be maintained at all times throughout its mission life, for example through appropriate command uplink security measures and security protection of ground infrastructures. The Act stresses that the so-called "controlled activities", including (*a*) formulating or giving a command to a remote sensing satellite of the system; (*b*) receiving raw data from a remote sensing satellite of the system;

(*c*) storing, processing or distributing raw data from the system; (*d*) establishing or using(i) cryptography in communications with a remote sensing satellite of the system, or(ii) information assurance measures for the system, shall be secure and undertaken by authorized system participants.

In terms of the distribution of data, the Act makes a distinction between "raw data"and "remote sensing products". Commercialization of the former shall be strictly controlled and undertaken pursuant to the provisions of the Act and the license. Raw data from a SAR system are, indeed, very sensitive and may reveal information that can be used against Canada or its allies. Therefore, as a general rule, licensees are only allowed to communicate raw data to authorized persons, namely the system participant. There are two exceptions to this rule: first, raw data shall be communicated to the sensed State on a non-discriminatory basis; second, the Minister of Foreign Affairs may authorize the communication of raw data to persons other than the system participants. In this case the Minister may decide that such a release be done only under a legally enforceable agreement, entered into in good faith, that includes measures respecting their security or their further communication. The licensee must make sure that the recipient of the data comply with such agreement.

As far as "remote sensing products"are concerned, licensees are free to distribute them; however, the Minister may restrict such distribution and impose specific conditions to it.

Similar to the US legislation the Minister of Foreign Affairs is entitled to require the licensee to interrupt services (shutter control) and to grant

[17] Synthetic Aperture Radar (SAR) can penetrate cloud cover and be used to image at night –in short they can provide all weather/day-night coverage.

Canada priority access to data and products in case of emergencies related to national security and foreign relations.
The Canadian authorities control the activities of the licensee through inspections, audits and request of documentation. In the event of breach of the license's conditions the license may be suspended or terminated. Furthermore, penalties may be decided. [18] Normally, the Act sanctions violations with administrative monetary penalties that range from $ 5,000 to 25,000. More serious offenses, such as operating a satellite without license or disobeying an order of suspension, may be prosecuted in criminal court and sanctions from $ 25,000 to 50,000 and an imprisonment up to 18 months.

d) *France*

France launched its first Earth observation satellite, SPOT-1, in 1986. SPOT-1 has been followed by six additional satellites, the most recent ones being the high resolution SPOT-6 and SPOT-7 offering images with a panchromatic resolution of 1.5 meters. Recently, the very high resolutions Pleiades 1A and Pleiades 1B, capable of producing images with a panchromatic resolution of 0.5 meters, were launched. While the satellites are initiated and operated by the French Space Agency (CNES), the commercialization of data and remote sensing products is the task of a private law company, Spot Image.
Until 2008 France did not have dedicated space legislation, including one governing remote sensing activities. Nevertheless, the French government exercised control on the Spot Image commercial policy in order to ensure protection of national interests and respect of international obligations of France. [19]A crucial role was played by an informal working group called GIRSPOT, composed of representatives from various Ministries. GIRSPOT was entitled to make reports on specific situations that could necessitate restrictions to the commercial activities of Spot Image but lacked the power to impose directives to Spot Image (which remained the responsibility of the Prime Minister). [20]Restrictions were imposed with regard to foreign receiving stations or related to data representing protected and sensitive French areas, locations of French or foreign allies troops.
On 22 May, 2008, the French Senate adopted the French Space Operation Act. The Act, which establishes a legal framework governing French space activities, contains provisions relevant to the operation of remote sensing satellites. Title VII of the Act, entitled space-based data, deals with the authorization procedure of space data provider (Article XXIII), the control of and the eventual conditions imposed by the governmental authorities (Article XXIV)

[18] Sections 23, 38-45, 2007 Remote Sensing Space Systems Act.
[19] For an analysis of French remote sensing law see P. Achilleas, French remote sensing law, 34(1) J. Space L. 1 (2008).
[20] *Id*. at 6.

and the possible penalties (Article XXV). Basically, every French person or every person based in France who intends to operate a space-based data system is obliged to declare it to the French government. The competent authority must ascertain that the proposed activity does not harm fundamental interests of the Nation, particularly defence matters, foreign policy and international commitments of France. To this end, it may at any time prescribe measures that limit the activity of the primary space-based data operators, which are necessary to safeguard these interests. An operators can be fined up to 200.000 euros if it fails to declare its activity or violates the restrictions imposed by the authority. Title VII of the French Space Operation Act has been expanded by means of the Decree n°2009-640 (9 June 2009) relating to space operations.[21] The Decree specifies: a) the technical characteristics of the concerned data; b) the competent administrative authority (The Secretary General for Defense and National Security ; c) the types of restriction measures the Government may take. For example, the Government may prevent the distribution images showing "sensitive"areas, limit the resolution of the images (French operator are forbidden from selling images with a spatial resolution lower than 0.50 m), order the suspension (shutter control) or the permanent interdiction of activities.[22]

6 Remote Sensing Legislation and Security: an Assessment

The previous sections have described the legislative measures adopted by States to reduce the security risks associated with the distribution of (high resolution) satellite images. These measures are, obviously, not able to elimination all dangers that this distribution encompasses. The truth to be said, a certain level of risk is inherent distribution of high resolution images; indeed, there is always the possibility that a leak of these images may occur or that data providers moved by the purpose of profit might disregard the restrictions on the distribution of data imposed in their license. A certain level of discrepancy among the security-related measures adopted at national level is also discernible.

Despite these limits national legislation does an adequate job in reducing the risks related to the distribution of satellite and achieving a fair balance between the need to protect national security and foreign policy interests and to commercialize remote sensing products. As analyzed, national remote sensing legislations set out numerous mechanisms to make sure that the sale of (high resolution) remote sensing products does not endanger national security interests, including encryption of signal, licensing process, control

[21] Décret n°2009-640 du 9 juin 2009 portant application des disposition prévues au titre VII de la loi n°2008-518 du 3 juin 2008 relative aux opérations spatiales

[22] Article V, Décret n°2009-640.

over the licensee's activities, restrictions to the sale of data. Certainly, a crucial role is to be played by the data provider. However, it is to be expected that a data provider does not endanger the interests of its own country and that it does comply with the license's restrictions. Failure to do so would not only lead to administrative and possible criminal consequences for the provider, but would also seriously affect, if not permanently terminate, its business activities in the remote sensing sector. Licensees establish very clearly what a licensee/data provider can or cannot do, for instance the kind of data that it can distribute, their quality, purpose and their recipient. In the event of a first-time data request or if the request raises security concerns it is to be expected that the provider would demand its licensing authority for advices.

It is important to point out the adoption of more stringent licensing operation conditions, even if theoretically possible, should not be recommended, as they would be detrimental to the commercial activities of the remote sensing operator and data provider. Arguably, there are not too many options to improve national and international security in connection with the commercialization of remote sensing products. If the goals would be to preserve the (global) security of sensitive areas or building, data providers of high resolution satellites images from different countries could meet and agree not to sell images certain sensitive locations. While theoretically feasible, this possibility would be difficult to implement due the difficulties in agreeing on what is "sensitive"and the fact that providers/States may hold different approaches. Another option would be for States to agree on the same level of spatial resolution that their licensed private operators could sell. Although this strategy could minimize the dangers associated with the distribution of high resolution images, it would take away any form of commercial edge from operators.

Solutions similar to those put in place during the 2001 Afghanistan campaign do not seem to be feasible, as the number of data provider is so wide that acquiring all data over a location is unrealistic.

Arguably, only at national level it is possible to exercise an adequate control and enhance the overall security related to the sale of remote sensing products. In this respect, States could strengthen controls over their licensees, requires the licensee to verify compliance with the distribution agreement, ask the collaboration of the country where the recipient is located, and clearly include in the national remote sensing legislation criminal consequences. Ultimately, however, there does not see too much that it can be done to enhance security more than what already exists.

7 Recent Developments

On June 11, 2014, report spread that the US government had relaxed restrictions on the resolution of commercial imagery.[23] US remote sensing companies are now entitled to all images with a resolution higher than 0.50 m, the previous limit. The decision was the consequence of an initiative taken by the seller of high resolution images DigitalGlobe which, in view of the foreseen launch of its high resolution satellite Worldwide-3 capable of generating images of 0.31 cm resolution (launched on 13 August, 2014) demanded the US to lower its license restrictions. After consulting with various agencies and security experts, the US government accepted this request. Pursuant to this decision DigitalGlobe became immediately allowed to sell black-and-white images as sharp as 40 centimeters in resolution, and color images with 1.6-meter resolution, to all customers (prior to the decision DigitalGlobe had to degrade the quality of images with a resolution higher than 50cm.). Furthermore, 6 months after the launch of WorldView-3, DigitalGlobe could commercialize black and white images of 25 centimeters resolutions and 1 meter color imagery. Notably, also has Thales Alenia demanded the French government to lower the limits for the distribution of high resolution satellite images.[24]

The possibility for DigitalGlobe to sell such very high resolution satellites images has obvious consequences from a security point of view, as previously the US government did not want the public to have access of images from space of that detail. It is also noteworthy that the 6 months moratorium on the release of images with a resolution up to 25 cm was due to permit the review and implementation of any measures that may be necessary to address national security concerns, foreign policy interests, and international obligations.[25]One, however, cannot expect great changes in the way national and international security are protected with regard to the distribution of very high resolution data. DigitalGlobe is still bound by the same rules described above, insofar as it cannot sell images that threaten national security, foreign interests, and international obligations of the US, every image requests has to go through a terrorists list and the government retinas the right of shutter control. Nevertheless, in view of the exceptionally high resolution of images NOAA may reconsider the terms of the DigitalGlobe's license, so as to minimize the risks for national security and the security of US

[23] See at www.digitalglobeblog.com/2014/06/11/resolutionrestrictionslifted/.

[24] See at http://www.spacenews.com/article/military-space/37204satellite-imagery-firms-in-us-and-europe-pushing-for-permission-to-sell.

[25] See statement by Tahara Dawkins, director of commercial remote sensing regulatory affairs at NOAA, as reported in http://www.spacenews.com/article/civil-space/40898digitalglobe-wins-approval-of-relaxed-operating-restrictions-with-proviso.

allies. For example, in order to protect US troops the license could contain an obligation not to sell any image of US troops involved in sensitive missions or a prohibition not to commercialize images showing foreign sensitive locations as indicated and requested by US allies. In any case these theoretically new licensing conditions should not undermine the commercial edge that DigitalGlobe has compared to other data providers with regard to the resolution of the images that it sells.

8 Conclusion

The commercial distribution of high resolution satellite images on a global basis is potentially threatening from a national and international security perspective. Consequently, States have adopted regulatory measures to control the release of these images by private operators. Although it is not feasible to eliminate all dangers connected with the commercialization of high resolution products, existing national measures do a rather adequate job in mitigating and reducing them. The present paper does not recommend States to substantially modify their existing national remote sensing legislation and to adopt a much stricter approach, as such a choice would have the counter effect of suffocating the market. However, in the light of recent decision enabling US private remote sensing operators to sell very high resolution satellite images, it is recommended that the US reconsiders the licensing conditions of these operators and adapt them to the enhanced threat to nation and international security that such images pose.