



Space Crisis Management: Europe's Response

Report 44
February 2013

Jana Robinson



Short title: ESPI Report 44
ISSN: 2076-6688
Published in February 2013
Price: €11

Editor and publisher:
European Space Policy Institute, ESPI
Schwarzenbergplatz 6 • 1030 Vienna • Austria
<http://www.espi.or.at>
Tel. +43 1 7181118-0; Fax -99

Rights reserved – No part of this report may be reproduced or transmitted in any form or for any purpose without permission from ESPI. Citations and extracts to be published by other means are subject to mentioning "Source: ESPI Report 44; February 2013. All rights reserved" and sample transmission to ESPI before publishing.

ESPI is not responsible for any losses, injury or damage caused to any person or property (including under contract, by negligence, product liability or otherwise) whether they may be direct or indirect, special, incidental or consequential, resulting from the information contained in this publication.

Design: Panthera.cc

Table of Contents

Executive Summary	4
1. Introduction	7
2. Terrestrial Crisis Management	8
2.1 The EU's Security and Defence Policy	9
2.2 The EU Crisis Management Structures and Decision-Making	10
2.3 Terrestrial Crisis Management Case Study: EU Operations in the Horn of Africa	15
3. The Space Crisis Management Requirement	19
3.1 Defining Space Crisis Management	20
3.2 Potential Space Crisis	20
3.3 Case Study: Iran's Jamming of Eutelsat	22
4. Space Crisis Management for Europe	26
5. Conclusion	29
6. Recommendations	30
List of Acronyms	31
Annex	34
A.1 Project Methodology	34
A.2 Agenda of the Roundtable on Space Crisis Management Organised by ESPI	36
A.3 CSDP Mission Planning Process	38
Acknowledgements	39
About the Author	39



Executive Summary

The loss of important space assets and capabilities (both civilian and military) could have a debilitating impact on the world economy and global security as well as exacerbate various terrestrial crises, whether they be humanitarian or security-related. Crises in space could be triggered by natural causes (e.g. space weather and debris), technical issues (e.g. satellite malfunction, unintentional interference, inaccurate orbital prediction) or intentional disruption of satellite services and even the attack on space assets.

Although space crises caused by natural hazards or technical issues warrant genuine concern, the intentional disruption of, or damage to, space assets and systems will generally involve larger – sometimes far larger – geopolitical stakes. Management of a crisis is a complex endeavour requiring a well-crafted vision and architecture for global space security as well as a strategic approach to contextualising and responding to challenges in this environment. Indeed, any meaningful disruption of essential space functions or operations would likely require extensive not only technical, but also political, damage control.

Deliberate interference with broadcast signals, such as Iran's repeated jamming of Eutelsat signals (described in more detail in section 3.3 of this report), is a case in point. Despite the ability to technically attribute the jamming source to a territory, and notwithstanding Iran's acknowledgement that the jamming was taking place within its territory, Teheran refuses to take responsibility and Eutelsat, France, the ITU and the EU have had only limited success in resolving this precedential breach of space governance. This has obvious implications for potential space crises to come that are of far higher consequence than jamming media broadcasts, especially if European lives are at risk. Terrestrial crisis management procedures as they exist today may also prove inadequate in a serious space incident.

Competitive, and increasingly contested, the space environment is not particularly conducive to efforts to establish rules of the road and new forms of cooperation. In short, space is still perceived as an ideal arena for demonstrating a nation's pride, independence, and capabilities. Accordingly, the ability of Europe and its allies to be accepted as the

"rule-maker" is somehow diminished and often regarded as suspect by those space actors that view space as a sphere of opportunity to enhance their perceived overall strength. Communication with these actors, and achieving consensus among them, under such circumstances is often most difficult.

When defining space crisis management, it is useful to recall the three "Cs" of international relations - cooperative, competitive and confrontational – and assume that each stage of a potential conflict involves different behaviour on the part of rational actors. Employed for space, the main focus is on efforts to identify those situations that are apt to represent threats to space assets and related services. In this sense, the goal of space crisis management is to preserve a peaceful and stable space environment. In short, a key objective of an effective space crisis management regime should be preventing crises before they mature, in part through the ability to gain international consensus on a set of rules governing responsible space behaviour, along with effective verification, compliance and enforcement measures.

There are clear space-related risks stemming from heightened terrestrial tensions or mishaps, but an incident in space could likewise trigger a terrestrial conflict. It is currently difficult to anticipate the reactions of many members of the international community to a crisis in space, as different actors attach varying levels of importance to space-related capabilities. Moreover, in addition to obstacles associated with configuring domestic space crisis decision-making procedures, crisis prevention at an international level represents an even more challenging task given the limited reach of "rules of engagement" for space. Also, there is a marked difference in behavioural norms when dealing with peacetime incidents versus crisis or conflict.

The current European agenda on space security is dominated by discussion, debate and diplomacy associated with the proposed Code of Conduct for Outer Space Activities introduced by the EU in 2008, and updated in 2010 and 2012. As the Code is of a preventive nature, it would be beneficial to identify how to marry the Code's Transparency and Confidence Building Measures (TCBMs) with

space crisis management procedures. There has not been, however, sufficient discussion of – or solutions provided for – what member states might do, in reasonably precise terms, in the event that the codified rules of the space road are violated.

The implications of increasingly sophisticated counterspace systems in the hands of less-responsible or more hostile actors are still to be tabled more routinely in Europe. Adding space crisis management as a central agenda item of the broader space security regime is desirable as intentional acts of disruption could jeopardise space stability systemically. The good news is that the space policy agenda of the EU continues to evolve, opening an opportunity for establishing an EU-wide space crisis management strategy and capability.

Space crisis management needs to be underpinned by strong and persistent diplomacy aimed at preventing crises, by the accelerated development of the operational and technical capabilities to manage a crisis already underway, and the availability of effective organisational structures to facilitate sound crisis management processes. Identifying and communicating the EU's priority objectives in this arena, including through European cooperation with other space-faring governments, international organisations and in multilateral fora, will bring positive results and cost-effectiveness to the EU's efforts to protect its space assets and capabilities.

It is hoped that this report, which examines various dimensions of Space Crisis Management, will serve as useful stimulus to achieve the progress urgently required in this particular space security portfolio. The report first reviews "terrestrial" crisis management models which have, until the end of the 20th century, largely been associated with the U.S. – USSR Cold War competition, especially ensuring the non-use of nuclear weapons and supporting technologies (e.g. strategic bombers, ballistic missiles, etc.). This first section also examines crisis management within the Europe's Common Foreign and Security Policy (CFSP), and the crisis response platform of the European External Action Service (EEAS). It likewise describes the EU missions at the Horn of Africa as practical examples of the EU's crisis management operations.

The second part of the report examines the requirements associated with space crisis management and how to define them. This part also reviews potential space crises (natural as well as man-made), as well as reviewing the Iranian jamming of Eutelsat signals as a case study. It then assesses the discourse on space crisis management within

the space security community in Europe. Finally, the study provides several recommendations, summarised below, for cooperative endeavours in this area, including proposed space policy objectives and measures to bolster institutional preparedness to manage space-related crises more effectively.

As part of this space crisis management project, ESPI also convened a roundtable in March 2012 to: 1) identify available tools for space crisis prevention; 2) delineate the essential ingredients of effective space crisis management; and 3) provide realistic scenarios that could trigger crisis management responses.¹

The following recommendations are offered to better integrate space crisis management into Europe's broader space security concerns:

- Drawing on terrestrial crisis management experiences, put forward policy measures, information sharing/safeguard measures, investment strategies and other elements required for bolstering Europe's space crisis management capabilities.

EU leadership – particularly through the EEAS – is a prerequisite for an effective dialogue on space pre-crisis planning and management among the relevant European actors in space. Europe's acknowledgement of a space crisis management requirement, including the upgrading of its infrastructure, expertise and policy awareness, will advance its ability to identify space-related threats and respond to them with agility and effectiveness in a time-sensitive environment. This will involve partner governments assuming specific, complementary responsibilities in this area of space security and instituting the necessary policy measures to align more closely current space capabilities with space crisis management requirements.

- While the EU's leadership in outlining prudent next steps for space crisis management takes the most realistic course, it can only be effective if the EU defines the "chain of command" for its space security establishment and speaks to partners with "one voice." The High Representative should task the EEAS with taking the lead in creating a space crisis management architecture for addressing a range of threats (both natural and

¹ More information about the roundtable can be found at the following link:
<http://www.espi.or.at/index.php?option=com_content&view=article&id=797:29-march-2012-space-crisis-management-roundtable-convened-at-espi&catid=39:news-archive&Itemid=37>



man-made), as well as communicating with partner space-faring nations on the most effective, timely responses.

EU consistency and attentiveness concerning its policies, programmes and contingency planning will likely persuade European member states and other stakeholders to support a security-minded space agenda and make the necessary financial resources available. Centralising space crisis management at the EEAS would both signal the importance of this issue area and help streamline the chain of command on these higher velocity decision situations. Such a top-down approach would also help mobilise the complex bureaucratic processes associated with the establishment of a Space Crisis Management cell.

- The EU should start a dialogue with NATO on space crisis management and define this portfolio within their respective security mandates.

Establishing guidance concerning how the EU and NATO might jointly respond to an incident in space would be desirable. NATO ACT's report describing space-related threats, dependencies and vulnerabilities, and the development of this concept by the Multi-National Experiment 7 (MNE-7) are concrete steps in the right direction.²

- Tighten transatlantic interaction on space crisis management as part of the

EU–U.S. broader bilateral engagement and consider more robust coordination with other countries (e.g. Japan).

The EU's willingness to engage in the establishment of a transatlantic security framework to facilitate bilateral discussions on space security-related issues would likely benefit and accelerate its work programme in this area. It would also demonstrate the global relevance and importance of this issue. Examining space crisis management from the transatlantic perspective could also contribute importantly to the broader security dialogue and advance the configuration of a multilateral space security architecture.

- Undertake Europe-wide space crisis management exercises.

The EU should consider creating space crisis management exercises or simulations covering the political/strategic and operational/tactical levels of crisis scenarios, making use of existing frameworks (e.g. the EU Crisis Management Exercise (CME), EU Military Exercise (MILEX), and NATO's Crisis Management Exercise (CMX)). Such exercises or games would likely reveal gaps in pre-crisis planning as well as the ability of existing institutions and arrangements to react to various space contingencies in real time, particularly the man-made variety.

² Maj. Gen. Mark Barrett, Dick Bedford, Elizabeth Skinner and Eva Vergles "Assured Access to the Global Commons." NATO Allied Command Transformation. April 2011.

1. Introduction

Terrestrial geopolitics is shaped by geography, size, resources, political system, culture, history and population of states. States seek geostrategic influence (i.e. military, economic, diplomatic and socio-cultural advantage), through the assessment of their political ideology, hard and soft power-projection capabilities, socio-cultural values and technology. In short, geopolitics reflects the sources of state power, while geostrategy explains how to deploy it. There exists little consensus on why states seek power and various schools of thought (e.g. realism, liberalism, etc.) offer a range of explanations.³ Yet, no matter the theoretical viewpoint, clearly space has become an essential tool for strengthening the capacity of some states to advance domestic prosperity and gain international influence.

For the U.S., China, France, Germany, Japan and other select countries, space offers major strategic advantages. Indeed, many nations are now competing to derive greater civilian, commercial and military benefits from their presence in space. Protection of space assets and ensuring a stable and safe space environment is, in the first place, the responsibility of those that operate them, as well as of those that formulate space policies. The quest for a workable space regime is appearing more often on the agendas of national and international security gatherings and misconduct in space could have profound implications for terrestrial geopolitics. The reverse is also true and the most likely threats to space, at least for the foreseeable future, will be connected to heightened terrestrial tensions or conflict.

One of the central operational and political challenges is the ability to assess accurately situations in space, and to respond effectively

to emergencies and disruptive activities there. In this sense, space presents a unique challenge for crisis management.

This project seeks to examine the concept of Space Crisis Management. The study first reviews "terrestrial" crisis management models which have, until the end of the 20th century, largely been associated with the U.S. – USSR Cold War competition, especially ensuring the non-use of nuclear weapons and supporting technologies (e.g. strategic bombers, ballistic missiles, etc.). Today, crisis management often focuses on strategic questions involving a variety of international actors. Accordingly, the connection between a crisis and the use of counter-measures is more subtle. The first part of the study also examines crisis management within the Europe's Common Foreign and Security Policy (CFSP), and the crisis response platform of the European External Action Service (EEAS). It likewise describes the EU missions at the Horn of Africa as practical examples of EU's crisis management operations.

The second part of the report examines the requirements associated with space crisis management and how to define them. This part also reviews potential space crises (natural as well as man-made), as well as reviewing the Iranian jamming of Eutelsat signals as a case study. It then assesses the discourse on space crisis management within the space security community in Europe. Finally, the study provides recommendations for cooperative endeavours in this area, including proposed space policy objectives and measures to bolster institutional preparedness to manage space-related crises more effectively. The project methodology is described in Annex 1.

³ Dolman, Everett C. "New Frontiers, Old Realities". *Strategic Studies Quarterly* (Spring 2012): 80.



2. Terrestrial Crisis Management

The concept of terrestrial crisis management has largely been associated with the U.S.–USSR Cold War competition which prominently involved ensuring the non-use of nuclear weapons and supporting technologies (e.g. strategic bombers, ballistic missiles, etc.). “Nuclear” crisis management consists of structuring nuclear forces to provide a sufficient deterrent against their use by a rival (including via arms control arrangements etc.) as well as providing for strict control of nuclear forces in a crisis to prevent unauthorised or accidental use of nuclear weaponry. But nuclear crisis management involves much more than just nuclear deterrent and nuclear stockpile control. The 1962 Cuban Missile Crisis demonstrated that when a country is really tested, it uses its whole playbook of persuasion and counter-measures of whatever nature.

The Cuban Missile Crisis is considered one of the most acute Cold War clashes that involved intense interaction between the two superpowers and careful policy decision-making. This crisis represented “a period of extreme tensions between nuclear-armed states that threatened the prospect of major war”.⁴ Three conceptual models put forth by Graham Allison, using the Cuban Missile Crisis as a case study, have been widely applied to address terrestrial crisis management solutions. These models were “rational policy” (I), “organizational process” (II), and “bureaucratic politics” (III). Model I portrays a state as a single rational policy decision-maker. According to Model II, the sub-units of the government follow established procedures and produce a policy option consistent with these pre-determined steps. In Model III, a policy decision is a negotiated bargain between individuals in charge of various responsibilities within the Executive Branch of government (e.g. Secretary of State, Secretary of Defense, etc.) which often concentrate on different angles of the same issue.⁵

⁴ Lord, Carnes. “Crisis Management : A Primer”. Institute for Advanced Strategic and Political Studies. IASPS Research Papers in Strategy No.7 (August 1998). <<http://www.iasps.org/strategic7/crisis.htm>>.

⁵ Allison, Graham. “Conceptual models and the Cuban Missile Crisis.” *American Political Science Review* (Sep 1969) 63/3, pp. 689-718. <<http://www3.nccu.edu.tw/~lorenzo/Allison%20Conceptual%20Models.pdf>>.

After the Cuban Missile Crisis, unilateral and bilateral measures were adopted to assist in streamlining political processes and prevent a dangerous escalatory spiral between the two powers that could ultimately result in large-scale military conflict. These measures included, for example, improved nuclear command and control arrangements, the U.S.–Soviet Hotline, and the 1972 Agreements on Measures to Reduce the Risks of Nuclear War.

Today, crisis management focuses on strategic questions involving a variety of international actors. Accordingly, the connection between a crisis and the use of force is more subtle. In this environment, the term “crisis” can be defined as “a perception by the highest level decision-makers of a threat to one or more basic values, along with an awareness of finite time for response to the value threat, and a heightened probability of involvement in military hostilities”.⁶

Crisis management starts with prevention. In the post-Cold War era, an example of crisis prevention was the June 2000 Memorandum of Agreement between the U.S. and the Russian Federation on the Establishment of a Joint Center for the Exchange of Data from Early Warning Systems and Notifications of Missile Launches. In the Memorandum, the U.S. and Russia agreed, for the first time, to a permanent joint operation involving U.S. and Russian military personnel to enhance strategic stability between the two countries. It called for the establishment of a Joint Data Exchange Center (JDEC) in Moscow for the sharing of information derived from each side’s missile launch warning systems on the launches of ballistic missiles and space launch vehicles.

In December 2000, the U.S. and Russia signed a Memorandum of Understanding establishing a Pre- and Post-Launch Notification System (PLNS) for ballistic and space launch vehicle launches. It is envisioned to be an Internet-based system operated as part of the JDEC. Both JDEC and PLNS make provisions for voluntary notifications of satellites diverted from their orbit and space experi-

⁶ Lord, Carnes. “Crisis Management : A Primer”. Institute for Advanced Strategic and Political Studies. IASPS Research Papers in Strategy No.7 (August 1998). <<http://www.iasps.org/strategic7/crisis.htm>>.

ments that could adversely influence the operation of early warning radars. These agreements represent a rare example of detailed and comprehensive space-related confidence-building measures designed to enhance stability through transparency.⁷ The discussions on implementation of the joint U.S.–Russia launch notifications are still ongoing.

In a crisis, difficult trade-offs between various response options need to be made at the highest levels of government. Crisis management considerations involve, beyond diplomacy, sanctions and use of force, the adequacy of available intelligence and how much information is available to the public. This calculus can have both important domestic and international implications, including economic, financial, legal and command and control dimensions. Successful crisis management seeks to minimise damage/costs and maximise stability/benefits. The challenge lies in the ability to react correctly and quickly in a crisis setting.

2.1 The EU's Security and Defence Policy

According to its mandate, the EU is responsible for space crisis management at the European level. It is in the process of building a common vision for a European security strategy. The EU's crisis management activities fall under the umbrella of its Common Security and Defence Policy (formerly known as the European Security and Defence Policy), part of the Common Foreign and Security Policy (CFSP). The 'Petersberg Tasks' form a central part of the CFSP. These are crisis management tasks, both civilian and military (i.e. humanitarian and rescue tasks, peace-keeping tasks and tasks of combat forces in crisis management, including peacemaking)⁸.

Although there has been decades-long support for common security concepts (including the 1975 Helsinki Final Act, the Western European Union's 1995 Common Security Concept, relevant provisions of the Maastricht and Amsterdam Treaties, etc.), Europe's priorities in this arena have been constantly evolving in reaction to the changing nature of the European political landscape as well as the regional and global security environment.

⁷ Hays, Peter L. "Military Space Cooperation: Opportunities and Challenges." *Monterey Institute of International Studies* (July 2002): 37.

⁸ The 'Petersberg tasks' were defined during the Ministerial Council of the Western European Union (WEU) in June 1992.

The so-called European Political Cooperation (EPC), formalised in 1986 by the Single European Act (SEA), was incorporated into a limited degree of common foreign policy, initially through the Maastricht Treaty (the Treaty on European Union) of 1992. This framework was further revised at the Helsinki European Council by the Treaty of Amsterdam in 1997 (introducing the CFSP High Representative, and a common security and defence policy (labeled European Security and Defence Policy, or ESDP). The subsequent Treaty of Nice, signed in 2001 (in force since 2003) established new permanent political and military structures (i.e. the Political and Security Committee and the Military Committee).

In 1999, the European Council stated that the EU must "have the capacity for autonomous action, backed up by credible military forces, the means to decide to use them, and a readiness to do so, in order to respond to international crises without prejudice to actions by NATO".⁹ European capability objectives and operational requirements were first defined in the Helsinki Headline Goal introduced in 1999 (stimulated by the conflict in Bosnia and Herzegovina, and revised in 2004 – the so-called Headline Goal 2010) and the 2001 European Capability Action Plan (ECAP). The "Civilian Headline Goal 2008" of December 2004 (revised in 2007 in the "Civilian Headline Goal 2010") identified objectives for Europe's civilian capabilities for crisis management. The objectives included: improving the quality of civilian EU crisis management; enhancing the availability of the Member States to contribute to ESDP missions; developing instruments to improve planning and conduct missions; and achieve synergies among civilian and military aspects of the ESDP.

The ESDP was reinforced in December 2002 (at the Copenhagen European Council) by the so-called Berlin Plus arrangements, enabling the EU to access NATO assets and capabilities to conduct its operations. The Berlin Plus arrangements are the central feature of EU–NATO relations. It is a comprehensive package of agreements between NATO and the EU based on conclusions of the 1999 NATO Washington Summit. The main components include:

- The NATO-EU Security Agreement;
- Assured Access to NATO planning capabilities for EU-led Crisis Management Operations (CMO);

⁹ Cit., Annex III of the Presidency Conclusions, Cologne European Council, 3-4 June 1999. Available at: http://www.esdp-course.ethz.ch/content/ref/199906Cologne_Excerpt.htm



- Availability of NATO assets and capabilities for EU-led CMO;
- Procedures for Release, Monitoring, Return and Recall of NATO Assets and Capabilities;
- Terms of Reference for Deputy Supreme Allied Commander Europe (DSACEUR) and European Command Options for NATO;
- EU-NATO consultation arrangements in the context of an EU-led CMO making use of NATO assets and capabilities; and
- Arrangements for coherent and mutually reinforcing Capability Requirements.¹⁰

The EU can use these capabilities when NATO is unwilling to engage in an operation and all NATO members approve it. The Berlin Plus arrangements have, thus far, been activated for two EU-led operations: Operation Concordia in Macedonia and Operation EUFOR Althea in Bosnia and Herzegovina.

Naturally, the NATO–EU relationship is a work in progress as both parties have differing security emphases and member states participation as well as available resources. Operational cooperation beyond the Berlin Plus arrangement is limited and in theaters of operations where both organisations are present (e.g. Afghanistan) there is little coordination between their respective missions. That said, there are efforts underway to improve the mechanisms for such coordination. The “EU–NATO capability group”, for example, seeks to coordinate harmonisation of requirements for interoperability and the acquisition of capabilities (e.g. NATO’s Prague Capabilities Commitment¹¹ and the EU’s ECAP), as well as the development of NATO’s Response Force (NRF) and EU’s Battlegroups. There exists interaction between NATO’s Conference of National Armaments Directors (CNAD) and the EU’s European Defence Agency (EDA), as well as NATO’s International Staff (IS)/International Military Staff (IMS) and the EU’s Military Staff (EUMS). Indeed, several countries have the same military representatives for both organisations.

The EU is well aware of how the changing strategic environment is impacting on

Europe’s security, including instances of international instability in its backyard (e.g. the Middle East) as well as in more distant parts of the world (e.g. Afghanistan) and the effects of a more globalised world (e.g. interwoven economies, cyber world, etc.). The EU seeks to be a global player capable of mobilising economic, commercial, humanitarian, diplomatic and military resources to help shape the international environment.

As pointed out in EU’s 2008 “Report on the Implementation of the European Security Strategy: Providing Security in a Changing World”, in identifying Europe’s broader security objectives the EU security-related work has been linked to the United Nations (UN) objectives. This makes Europe well-positioned to provide leadership in the area of multilateral cooperation.¹²

2.2 The EU Crisis Management Structures and Decision-Making

As referenced in the previous section, the EU has been striving to assert itself as a more active and visible actor in the international arena, including by seeking to contribute to addressing regional and global security issues. Accordingly, the EU is continuously building up its own security structures and has, to date, deployed around 80,000 staff in twenty-six civilian and military operations on three continents (as of October 2012). Fourteen of these operations are currently ongoing and twelve have been completed. Seven are military missions, seventeen civil, and one (i.e. the EU support to AMIS-Darfur) is a joint civilian/military mission¹³.

The EU treats its foreign policy through a “comprehensive approach” which seeks to use all instruments available to the EU for crisis management, combining political, diplomatic, economic/financial, development aid-related activities, as well as civilian and military tools. This approach has led to the joint application of civilian and military measures and the introduction of a hybrid civilian-

¹⁰ More information about the “Berlin Plus Arrangements” can be found in the Assembly of Western European Union Fact Sheet No.14. Available at: <[http://www.shape.nato.int/resources/4/documents/14E_act_Sheet_Berlin_Plus\[1\].pdf](http://www.shape.nato.int/resources/4/documents/14E_act_Sheet_Berlin_Plus[1].pdf)>. Last accessed 09 Dec 2012.

¹¹ More information about the “Prague Capabilities Commitment” can be found at: <http://www.nato.int/cps/en/natolive/topics_50087.htm>. Last accessed 09 Dec 2012.

¹² Robinson, Jana. Enabling Europe’s Key Foreign Policy Objectives Via Space. ESPI Report 30 (February 2011). Available at: <http://www.espi.or.at/images/stories/dokumente/studies/E_SPI_Report_30_web.pdf>

¹³ See the list of EU Operations and Missions at European External Action Service website. <<http://www.consilium.europa.eu/eeas/security-defence/eu-operations.aspx?lang=en>>. (Last accessed 15 Nov 2012).

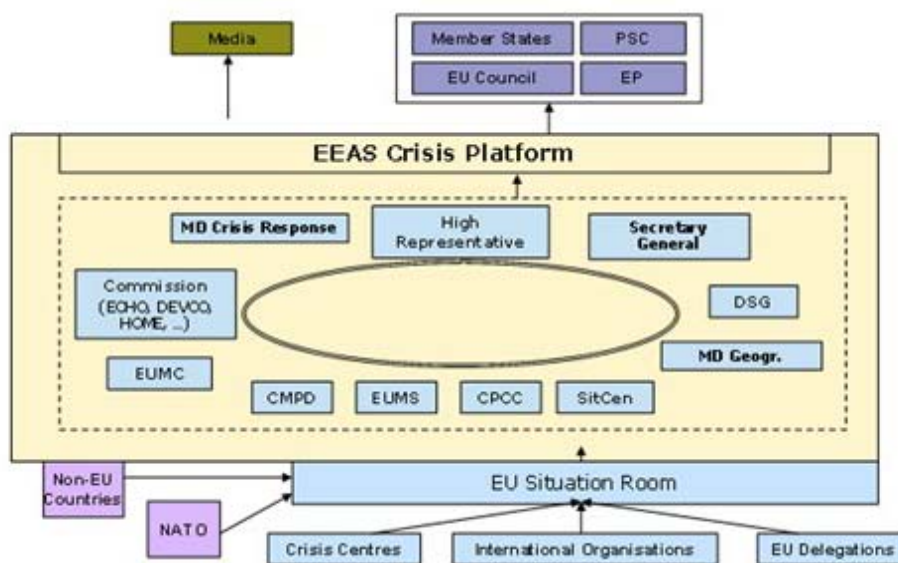


Figure 1: the EEAS Crisis Platform (source: EEAS website)¹⁵

military crisis management structure.¹⁴ The “comprehensive approach” was introduced in the 2003 European Security Strategy (ESS), which stated that: “In contrast to the massive visible threat in the Cold War, none of the new [global security] threats is purely military; nor can any be tackled by purely military means. Each requires a mixture of instruments.”¹⁶

The Lisbon Treaty permitted the EU to be involved in all stages of crisis management starting with prevention mediation (diplomatic), crisis response and post-conflict reconstruction. It has brought important institutional innovations to the EU's external actions, including the EU's acquisition of a legal status to be able to sign binding agreements with third countries and international organisations at the public international law level, as well as ratify international conventions.

As a result of the Treaty, the EU now has its own foreign policy chief (i.e. the High Representative) who can speak and act on behalf of the EU. The High Representative chairs the meetings of the Foreign Affairs Council and represents, together with the EU delegations,

the EU during meetings with third countries or international organisations.

To assist the High Representative, the European External Action Service (EEAS) has been established by merging divisions from the European Commission and the Council Secretariat as well as recruiting employees from Member States. The EEAS is the main structure responsible for the EU's CFSP, including CSDP.¹⁷ The EEAS manages the EU's “Terrestrial” Crisis Platform, involving various crisis response/management mechanisms.

The Crisis Platform aims at providing optimal operational coordination among the different components of crisis management and to ensure the coherence of EU responses to crises and enable dialogue among the various actors (including services of the European Commission).

Chaired by the High Representative, the EEAS Executive Secretary General (ESG) or the EEAS Managing Director of the Crisis Response Department, the EEAS Crisis Platform connects the elements of the EEAS crisis response/management structure. These include: the Response & Operational Coordination Department; Crisis Management and Planning Directorate (CMPD); European Union Military Staff (EUMS); Civilian Planning and Conduct Capability (CPCC); Situation Centre; the EU Situation Room; and other geographical and horizontal EEAS Departments; the EU Military Committee (EUMC) and relevant

¹⁴ Barry, Linda. “The EU's Comprehensive Approach”. The Institute of International and European Affairs (2012):1-2. Available at: <<http://www.iiea.com/publications/european-security-in-the-21st-century-the-eus-comprehensive-approach>> (Last accessed 10 Dec 2012).

¹⁵ “The EEAS Crisis Platform”. EEAS website: <http://consilium.europa.eu/eeas/foreign-policy/crisis-response/eeas-crisis-platform>. (Last accessed 17 Sep 2012).

¹⁶ Cit., “European Security Strategy. A Secure Europe in a Better World”. 12/12/2003. P.12 Available at: <<http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>> (Last accessed 10 Dec 2012).

¹⁷ See Article 27 of the Lisbon Treaty. Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:15:0013:0045:EN:PDF>> (Last accessed 10 Dec 2012).



Crisis Response Cycle

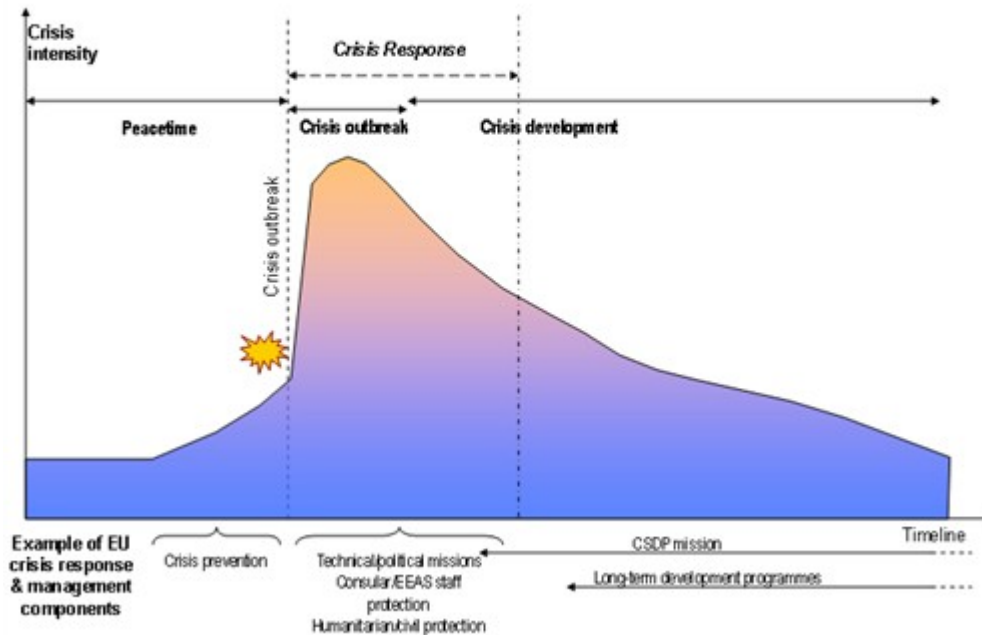


Figure 2: the EU Crisis Response Cycle (source EEAS website)¹⁸

European Commission services (ECHO, DEVCO, FPI, etc.) (see figure 1). It serves as a mechanism to implement the “comprehensive approach” to crisis management referenced above. Like any new entity, the EEAS is still in the process of refining effective coordination among various EEAS directorates (and other entities such as the EC), as well as establishing flexible and agile processes.

The EEAS Crisis Response & Operational Coordination Department assists the High Representative in coordination of the EU’s foreign policy (especially in the field of crisis management), undertakes specific missions, coordinates the work of the EEAS Crisis Platform, manages the EU Situation Room¹⁹, and follows international developments relevant to potential EU’s responses to an emerging crisis. In the event a situation is identified as

a crisis, the department calls for the attention of the Political and Security Committee (PSC), which assesses the nature of the crisis and EU’s potential involvement (see figure 2).

The EU Member States have political (through the Political and Security Committee) and operational (i.e. the forces and capacity for the missions) control over the CSDP. The Political and Security Committee (PSC) is the multinational political authority that directs and oversees the work of the Council Secretariat, the EU Military Staff (EUMS) and the personnel running the headquarters of actual operations. The planning process is key to understanding how an operation will work as it provides a conceptual bridge between the political aims and objectives on one hand and the operational means and resources on the other.

The planning process, including mission reviews, is both vertical (from the national capitals at the political/strategic level of the PSC down the operational chain of command) and horizontal (involving different functional phases). All decisions, including engagement in a crisis, have to be based on unanimity (i.e. a political consensus on a possible action), often creating tensions between what is deemed necessary versus what is politically feasible.

In order to integrate and effectively coordinate the various structures involved in Crisis

¹⁸“The Crisis Response Cycle“. EEAS website: <<http://consilium.europa.eu/eeas/foreign-policy/crisis-response/crisis-response-cycle>> (Last accessed 17 Dec 2012).

¹⁹The EU Situation Room is a permanent body that provides the worldwide monitoring, the current situation awareness, front line service for EU delegations and CSDP missions/operations, the activation of the Crisis Platform, and a support to security incident management. It is also responsible for developing cooperation and exchange information arrangements with crisis structures in EU Member States, institutions and agencies, as well as third countries and international organisations. See EEAS website: <<http://consilium.europa.eu/eeas/foreign-policy/crisis-response/eu-situation-room>>

Management in responding to even complex crises, the specific steps to be undertaken were originally developed, pursuant to the 2001 Nice EU Council decisions, in the form of so-called Crisis Management Procedures (CMP).²⁰ Over the years, the CMP have received continuous updating and review and were complemented by various planning concepts (especially concerning military/strategic planning, command and control and force generation).

In July 2003, the PSC issued a document offering "Suggestions for Procedures for Coherent, Comprehensive EU Crisis Management"²¹. The document described the CMP model, which consists of six phases (see table 1 below).

Six Phases of Crisis Management Procedures (CMP)	
1	Routine Phase
2	Crisis Build-Up/Draft Crisis Management Concept (CMC)
3	CMC Approval and Development of Strategic Options
4	Formal Decision to Take Action, Development of Planning Documents
5	Implementation Phase
6	Refocusing of EU Action/Termination of Operation

Table 1: Six Phases of Crisis Management Procedures (CMP)

If the advance planning undertaken by the PSC results in a decision to take action (i.e. the CMP's Phase One), the crisis response planning begins, including elaboration of a detailed Operation Plan (OP) for execution. Member States as well as the Crisis Response & Operational Coordination Department are involved in the routine planning.

The planning process involves political/strategic and operational/tactical dimensions. The first political/strategic step in the crisis response planning cycle (i.e. the second phase of the CMP model) is the development of a crisis management concept (CMC), a document describing the grand strategic plan that the PSC has agreed on (i.e. what to do, why, where and with whom). It contains the

²⁰ For more information see the document "Presidency Conclusion of Nice European Council Meeting, 7-8-9 December 2000". Available at: <<http://www.consilium.europa.eu/uedocs/cmsUpload/Nice%20European%20Council-Presidency%20conclusions.pdf>>

²¹ "EU Council: Suggestions for Procedures for coherent, Comprehensive EU Crisis Management", 3 July 2003. Available at: <http://esdc.mil-edu.be/index.php/component/docman/doc_download/265-suggestions-for-procedures-for-coherent-comprehensive-eu-crisis-management> (Last accessed 09 Dec 2012).

political and military assessment of the crisis situation, the overall purposes of the operation, and one or more courses of action.²²

The text of the CMC is drafted by the CMPD²³, supported by relevant units in the European Commission. Subsequently, advice on military aspects is provided by the EUMC²⁴, and on the civilian aspects by the Committee on Civilian Aspects of Crisis Management (CIVCOM)²⁵. Finally, the PSC agrees on the CMC and forwards it to the Permanent Representatives Committee (COREPER) and the Council of Ministers for formal approval.

Recent CMCs, elaborated by the CMPD and approved by the Foreign Affairs Council, include the CMC for the Regional Maritime Capacity Building mission in the Horn of Africa and in Somalia, the CMC for the Sahel mission and the CMC for the mission for the security of the airport in Juba (South Sudan).²⁶

Civilian missions planning, deployment, conduct and implementation materialise through the civilian crisis management structure, the Civilian Planning and Conduct Capability (CPCC).²⁷ There are four main areas under the civilian missions: police; border assistance management; strengthening of the rule of law; and security sector reform (i.e. civil administration and civil protection). The CPCC

²² For more information see "EU Council: Suggestions for Procedures for coherent, Comprehensive EU Crisis Management", 3 July 2003. Available at: <http://esdc.mil-edu.be/index.php/component/docman/doc_download/265-suggestions-for-procedures-for-coherent-comprehensive-eu-crisis-management> (Last accessed 10 Dec 2012).

²³ The CMPD works under the political control and strategic directions of the Member States in the Political and Security Committee and under the responsibility of the EU Council and the High Representative.

²⁴ The EUMC (established in 2001) is the highest military body set up within the Council, involving the Member States' Chiefs of Defence (represented by their permanent military representatives). It directs all military activities within the EU framework and assists the PSC on all military matters. (For more information see "Council Decision of 22 January 2001 setting up the Military Committee of the EU", available at: <http://www.consilium.europa.eu/uedocs/cmsUpload/l_02720010130en00040006.pdf>)

²⁵ CIVCOM provides information, assistance and recommendation on civilian aspects of crisis management (For more information see:

<<http://consilium.europa.eu/eeas/security-defence/csdp-structures-and-instruments?lang=en>>. (Last accessed 09 Dec 2012).

²⁶ See "Crisis Management and Planning Directorate" at EEAS website: <http://consilium.europa.eu/eeas/security-defence/csdp-structures-and-instruments/cmpd>. (Last accessed 09 Dec 2012).

²⁷ For more detailed information on the functions of the CPCC see the document: "Common Security and Defence Policy. The Civilian Planning Conduct Capability". Available at EEAS website.

<<http://www.consilium.europa.eu/eeas/security-defence/csdp-structures-and-instruments/cpcc?lang=en>>. (Last accessed 09 Dec 2012).



Director is the EU's Civilian Operations Commander.²⁸ Military operations are conducted by the Military Operation Commander. Strategic planning always involves both the CPCC and the military staff seeking to streamline the procedures.

The second response step (i.e. the third phase in the CMP model) includes the approval of the CMC by the Council of Ministers (based on the PSC's opinion) and the development of strategic options (i.e. general outlines of actions designed to achieve political objectives identified in the CMC). The EUMS²⁹ develops military strategic options (MSO) and the CPCC develops police-related strategic options (PSO) or other civilian strategic options (CSO). The EUMC and CIVCOM then comment on the strategic options and the PSC drafts a decision on the various options proposed, forwarding it to COREPER. Consultations with non-EU NATO Members and other countries also take place to ensure "that the countries potentially contributing to an EU-led crisis management mission or operation are informed of the EU's intentions".³⁰

The Council can now formally decide to act. This decision can, when appropriate, take the form of a Joint Action, "one of the legal decision-making formats available to the Councils on matters related to the CSDP".³¹ A Council Decision (CD) is a legal act by which the Council establishes the operation, appoints the Operation Commander(s) and decides on financial arrangements for the operation costs.

The next step (phase four in the CMP) is the development of the operational planning documents. At this stage, procedures for military and civilian CSDP operations diverge. The EUMC issues an initiating military directive (IMD) for military operations (drafted with the support of the EUMS and approved by the PSC) to the operations headquarters

identified in the CD. The IMD translates the CD into military guidance for the Operation Commander. The military chain of command, from this point forward, begins to develop its own set of planning documents, including the Concept of Operations (CONOPS)³² and Operation Plan (OPLAN)³³ approved by the EUMC, the PSC and the Council. The planning doctrine used for developing these documents essentially follows the NATO Guidelines for Operational Planning.

For civilian operations, the CPCC develops the CONOPS before the CD is passed in order to make the financial arrangements sufficiently clear. Afterwards, the planning authority shifts to the civilian Head of Mission who is responsible for developing the OPLAN. Similarly, CIVCOM, the PSC and the Council have to approve the civilian planning documents.³⁴

The force generation process is a separate, but parallel, process to that of the plan development. Concurrent with the CONOPS, a provisional Statement of Requirements (SOR) is produced (i.e. an overview of the means and resources that are needed in order to be able to fulfill the mission). The participating Member States pledge assets and capabilities for the operation (through a series of conferences). This process does not have a specific time constraint.

After the plan development is completed, the OPLAN validated and all mission-critical elements of the SOR fulfilled, the Council can formally launch the operation – phase five in the CMP model. The PSC holds the political control and strategic direction of the operation and makes mission-relevant decisions (e.g. revising the planning documents, including the OPLAN, the Chain of Command, the Rules of Engagement). It also appoints the EU Operation/EU Force Commanders. The PSC has to report to the Council at regular intervals.

The proper execution of the military operation is monitored by the EUMC, conducted under the responsibility of the EU Operation Commander. The chairman of the EUMC acts as the primary point of contact with the EU Operation Commander, who – together with the EUMC – reports directly to the PSC. The Operation Commander works from the Operation Headquarters (OHQ), while the Force Commander commands and maintains control of all the military in the Joint Operation Area.

²⁸ "The Civilian Planning Conduct Capability". Document available at : http://consilium.europa.eu/media/1222515/110412%20factsheet%20-%20cpcc%20-%20version%204_en.pdf. (Last accessed 09 Dec 2012).

²⁹ The European Union Military Staff (EUMS) is a Council Secretariat department directly attached to the Secretary General/High Representative (SG/HR), which work under the military direction of the EUMC and in close cooperation with other departments of the Council.

³⁰ Cit., "EU Council: Suggestions for Procedures for coherent, Comprehensive EU Crisis Management", 3 July 2003, Art 51, p. 15.

³¹ Björkdahl, Annika - Maria Strömvik, Maria, "EU Crisis Management Operations. ESDP Bodies and Decision-Making Procedures" Danish Institute for International Studies, Report No. 8, 2008. Available at: http://www.diis.dk/graphics/Publications/Reports%202008/R08-8_EU_Crisis_Management_Operations.pdf.

³² CONOPS is a concise statement of how the Operation Commander intends to fulfil his mission.

³³ OPLAN is the highly detailed script of the operation in its entirety.

³⁴ "EU Council: Suggestions for Procedures for coherent, Comprehensive EU Crisis Management", 3 July 2003, Art 80, p. 22.

In short, the Operation Commander coordinates the operation in conjunction with the military and political authorities of the EU, and the Force Commander executes the military activities of the operation. The European Union Military Staff (EUMS) acts as the Advising Body of the EEAS, providing military expertise for the HR and performing early warning, strategic planning and situation assessment in support of the operation.

The military operation can then be reviewed/refocused/terminated (phase six in the CMP model) as deemed appropriate.³⁵ The PSC is in charge of evaluating the need to refocus an EU action, including the possibility of terminating some, or all, of its elements. It is the Council, however, that takes the formal decision to refocus the action or end an operation. At this time, the process of evaluation usually starts, including discussion on lessons learned from the operations, which is provided to the PSC by the Commission to seek procedural improvements for future operations. Finally, the PSC provides an overall assessment (see Annex 3 of this Report).

The permanent crisis management structures in the EU, often with competing visions, reflect the EU's ambitions in the area of crisis management. The Lisbon Treaty gave rise to an opportunity to improve coherence and efficiency of EU institutions and provided a new tool for shaping the CFSP and CSDP.³⁶ At the same time, the number of institutional and decision-making processes required to generate a response to a crisis represents a significant challenge for effective coordination of the crisis management instruments (both military and civilian). That said, if the EU succeeds in further strengthening its "comprehensive approach" to crisis prevention and management, it will be positioned to take on the leadership role it covets.

2.3 Terrestrial Crisis Management Case Study: EU Operations in the Horn of Africa

Under the umbrella of its CSDP, the EU is currently conducting three military operations targeting the Horn of Africa and Somali region: the anti-piracy European Union Naval Force Somalia (EUNAVFOR) – Operation Atalanta; European Union Training Mission Somalia (EUTM), contributing to the training of Somali security forces; and the European Union Maritime Capacity Building Mission in the Horn of Africa (EUCAP Nestor) aiming at maritime capacity building in the region.³⁷

These three missions form an integrated effort to support the European Strategic Framework for the Horn of Africa (HoA). The Strategic Framework, adopted by the EU Council in November 2011, seeks a "comprehensive approach" in the HoA, which "includes efforts to promote political progress, improved governance, strengthening the rule of law, and responses to development and humanitarian needs".³⁸

The EU ATALANTA NAVFOR, the EUTM and EUCAP Nestor missions are described in this report to showcase the practical implementation of crisis management procedures for CSDP activities, which include interaction among EU institutional actors and Member States; the EEAS internal crisis response procedures; and the conduct of operational planning from the political/strategic level to the civilian/military level.

These missions are part of EU's broader foreign policy objectives for the region, including: the maritime capacity building needs in the Western Indian Ocean (e.g. the Critical Maritime Routes Programme under the Instrument for Stability); support for the Eastern and Southern African – Indian Ocean Regional Strategy and Action Plan against Piracy and for Promoting Maritime Security through the European Development Fund; and humanitarian aid and development cooperation. In March 2012, the EU Foreign Affairs Council activated, for the first time, the EU Operation Centre to coordinate and

³⁵ Mattelaer, Alexander, "The CSDP Mission Planning Process of the European Union: Innovations and Shortfalls." *European Integration online Papers*, 14/9 (2010): 6. Available at: <<http://eiop.or.at/eiop/texte/2010-009a.htm>> (Last accessed 09 Dec 2012).

³⁶ Hynek, Nik, "Consolidating the EU's Crisis Management Structures: Civil-Military Coordination and the Future of EU HQ". (2010). Available at: <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede260410studyfutureohq/_sede260410studyfutureohq_en.pdf> (Last accessed 09 Dec 2012).

³⁷ See "The EU Strategic Framework for the Horn of Africa: A Critical Assessment of Impacts and Opportunities", (2012), pp. 40-43. Available at: <<http://www.europarl.europa.eu/committees/en/studies/download.html?languageDocument=EN&file=76651>> (Last accessed 10 Dec 2012).

³⁸ Cit., EUTM Mission website: <<http://www.consilium.europa.eu/eeas/security-defence/eu-operations/eu-somalia-training-mission?lang=en>> (Last accessed 21 Nov 2012).



strengthen the civil-military synergies between these three CSDP missions.

The ATALANTA Mission

The Indian Ocean is the third largest volume of water in the world, covering about 20% of the Earth. Despite its vastness, reports by the International Maritime Organization (IMO) outline that the majority of the Indian Ocean pirate attacks do not occur on the high seas, but in shipping lanes near Somalia and the Gulf of Aden. The importance of the Gulf of Aden and adjacent waters concerns two main pillars of the global economy: the transportation of goods by sea and the production and export of crude oil. Accordingly, this sea and its adjacent lanes around the Horn of Africa are of vital importance, making maritime security a key element of global economic development.

The UN Security Council recognised that the deteriorating situation off Somalia's coast constitutes a threat to international peace and security, and issued a number of Resolutions related to this issue (e.g. UNSC Resolutions 1814, 1816 and 1838).³⁹ The resolutions enable states to:

- "Enter the territorial waters of Somalia for the purpose of repressing acts of piracy and armed robbery at sea, in a manner consistent with such action permitted on the high seas with respect to piracy under relevant international law;
- Use, within the territorial waters of Somalia, in a manner consistent with action permitted on the high seas with respect to piracy under relevant international law, all necessary means to repress acts of piracy and armed robbery";⁴⁰

The counter-piracy European Naval Force Somalia – Operation ATALANTA (EU NAVFOR-ATALANTA) seeks to not only prevent pirate attacks but also provide a longer-term, sustainable, solution to the piracy issue by assisting the states in the region to upgrade their anti-piracy efforts, as well as by removing some of the causes for piracy.

The Atalanta mission is managed by several EU member states with the main goal to protect shipping off of the Horn of Africa, especially vessels supplying humanitarian aid for

Somalia in the framework of the World Food Programme. Atalanta's mandate began in 2008 and has been extended twice, in 2010 until December 2010 and in 2012 until December 2014.

The mission mandate is based on the Council Joint Action 2008/851/CFSP, based on various UNSC Resolutions and provisions of international law.⁴¹ Based on Article 1 of the document, the EU military Operation Atalanta is conducted to contribute to:

1. "The protection of vessels of the World Food Programme (WFP) delivering food aid to displaced persons in Somalia (and the protection of African Union Mission in Somalia (AMISOM) shipping."
2. "The protection of vulnerable vessels cruising off the Somali coast, and the deterrence, prevention and repression of acts of piracy and armed robbery off the Somali Coast."⁴²

In practice, EUNAVFOR-ATALANTA conducts three types of mission: 1) escorts of WFP ships; 2) escorts of convoys that traverse the International Recommended Transit Corridor in the Gulf of Aden; and 3) routine patrols with the purpose of detecting pirate ships and deterring acts of piracy.⁴³ The mission area (some two million square nautical miles) spans from South of the Red Sea to the Gulf of Aden and the Western part of the Indian Ocean, including the Seychelles and Somali coastal territory as well as its territorial and internal waters.⁴⁴

Capacity for the operation is provided by EU Member States⁴⁵ by contributing Navy vessels (surface combat vessels and auxiliary ships), Maritime Patrol and Reconnaissance Aircraft (MPRA), Vessel Protection Detachment (VPD) teams, military staff for the OHQ in Northwood, UK, and onboard units.⁴⁶ Sev-

³⁹ See e.g. S/RES/1838 (2008) of 7 October 2008, S/RES/1846 (2008) of 2 December 2008, S/RES/1851 (2008) of 16 December 2008, S/RES/1897 (2009) of 30 November 2009, S/RES/1918 (2010) of 27 April 2010, S/RES/1950 (2010) of 23 November 2010, S/RES/1976 (2011) of 11 April 2011, S/RES/2015 (2011) of 24 October 2011, S/RES/2020 (2011) of 22 November 2011.

⁴⁰ Cit., S/RES/1816 (2008) of 2 June 2008.

⁴¹ For the Legal Basis of Operation Atalanta, see the list of relevant resolutions and decisions available at EEAS website: <<http://www.consilium.europa.eu/eeas/security-defence/eu-operations/eunavfor-somalia/legal-basis.aspx?lang=en>> (Last accessed 10 Dec 2012).

⁴² See Article 1 of the Council Joint Action 2008/851/CFSP of 10 November 2008. Available at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:301:0033:0037:EN:PDF>> (Last accessed 10 Dec 2012).

⁴³ See Remuss, Nina-Louisa, Space Applications as a supporting tool for countering piracy, ESPI Report 29, (October 2010), p 63. Available at: <http://www.espi.or.at/images/stories/ESPI_Report_29_onl_ina.pdf>

⁴⁴ For more detailed information see EUNAVFOR website. <<http://www.eunavfor.eu/>> (Last accessed 18 Dec 2012).

⁴⁵ Ibid.

⁴⁶ For more information see the Document "EUNAVFOR OPERATION ATALANTA" Available at: <<http://eunavfor.eu/wp-con->

eral non-EU European countries have also provided their assets for this operation, including Norway, Croatia and Montenegro. The funding of Operation Atalanta is shared (through the Athena Mechanism – a mechanism for managing operations with military and defence implications) among the EU Member States, according to their GDP. Besides the European naval forces, several others are also present in the zone, including the NATO Maritime Group, Russian, Indian, Japanese and Chinese vessels.⁴⁷ Through the cooperation with the European Union Satellite Centre (EUSC), space assets have also contributed to the mission objectives (e.g. by the monitoring of pirate operating bases, the Somali border, and possible terrorist training camps, the identification of potential pirate camps on the Somali coastline and offshore islands; etc.).⁴⁸

European Union Training Mission Somalia (EUTM)

Somalia is faced with major challenges to its stability, including the threat of clan-based Warlords, a sustained campaign on the part of the extreme Islamist Al Shaabab (AS), famine, and piracy. The EU, in order to assist Somalia and its Transitional Federal Government (TFG), launched the EUTM Somalia through the EU Council Decision of 31 March 2010, based on UNSC Resolution 1872 (2009) to provide, in partnership with Uganda, training support to the Somali Army.⁴⁹ The UNSC Resolution emphasised the importance of the re-establishment, training, equipping and retention of Somali security forces and urged Member States, regional and international organisations to offer, among other things, technical assistance for

the training and equipping of the Somali security forces.⁵⁰

The Council Decision authorised the EU Mission Commander to “release the activation order (ACTORD) in order to execute the deployment of the forces and start execution of the mission” (CD’s Article 3). The mission was launched in April 2010, and has just completed its second mandate, running from August 2011 to December 2012. By the end of the mission it was to train over 3000 soldiers, non-commissioned officers (NCOs) and officers who will assist in expanding the Somali government’s remit to areas outside Mogadishu.⁵¹

The mission has the following main elements:

- Mission Headquarters are in Kampala as the training of Somali forces takes place mainly in Uganda
- EUTM Somalia operates in coordination with other international actors, mainly the UN, African Union Mission in Somalia (AMISOM) and the U.S.;
- The mission’s main focus is on Command and Control and, with the purpose of transferring EU training expertise to local actors, the self-training capabilities of the Somali NSF, together with supporting international humanitarian laws and human rights.⁵²

Twelve EU Member States contribute personnel to the mission. The Commander of the mission periodically updates the PSC, the EUMC/Chiefs of Defence (CHODs) and Defence Minister on the latest theatre situation. There is also interaction with other mission stakeholders (i.e. the UN, AU, AMISOM, US, UPDF, and EU Delegations) to ascertain that the mission complies with the broader concept of the EU Strategic Framework for the Horn of Africa and Somalia.⁵³

tent/uploads/2011/08/20121011_Informationbroschure_english.pdf> (Last accessed 10 Dec 2012).

⁴⁷ Together with EU NAVFOR ATALANTA, the OHQ has created two international data transmission networks that can be used by all the international actors involved in the fight against piracy in the Somalia region: the Maritime Security Centre – Horn of Africa (MSCHOA) which provides all relevant information on piracy in the zone via a website; and TEXWEB, which links up through a chat-room all the shore and sea-based authorities and all the ship engaged in counter-piracy operations, creating a real-time coordination and exchange of information. For more information see MSCHOA website.

⁴⁸ Remuss, Nina-Louisa, Space Applications as a supporting tool for countering piracy, ESPI Report 29 (October 2010). Pp. 62-66.

⁴⁹ See Council Decision 2010/197/CFSP of 31 March 2010. Available at:

<<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:087:0033:0033:EN:PDF>> (Last accessed 18 Oct 2012).

⁵⁰ See Article 8 of S/RES/1872 (2009) of 26 May 2009. For the Legal Basis of EUTM Somalia, see the list of relevant resolutions and decisions at EEAS website.

<<http://www.consilium.europa.eu/eeas/security-defence/eu-operations/eu-somalia-training-mission/legal-basis?lang=en>> (Last accessed 18 Oct 2012).

⁵¹ See “EUTM Somalia News in Brief” Available at:

<<http://www.consilium.europa.eu/eeas/security-defence/eu-operations/eu-somalia-training-mission/news-in-brief?lang=en>> (Last accessed 10 Dec 2012).

⁵² See “EUTM Somalia Fact Sheet”. Available at <http://www.consilium.europa.eu/uedocs/cms_data/docs/missionPress/files/Fact%20sheet%20EUTM%20-%20EN_March%20201201.pdf> (Last accessed 10 Dec 2012).

⁵³ See the Document “EUTM SOMALIA. A European Success Story”, p. 4. Available at:

<http://www.consilium.europa.eu/media/1728530/eutm_magazine_2012_july_final2.pdf> (Last accessed 10 Dec 2012).



European Union Maritime Capacity-Building Mission in the Horn of Africa (EUCAP Nestor)

To complement the EUNAVFOR-Operation Atalanta and the EUTM Somalia, the EU launched the EUCAP Nestor mission in July 2012 with an initial mandate of two years (and a strategic review after one year). It is a regional training mission, currently under preparation, seeking to strengthen the maritime capacities of eight countries in the Horn of Africa and the Western Indian Ocean. It is configured as a civilian mission augmented with military expertise.

Specifically, the EUCAP Nestor addresses two objectives:

- Strengthen the rule of law sector in Somalia, with an initial focus on the regions of Puntland and Somaliland. In particular, the mission will support the development of a coastal police force and the judiciary;
- Strengthen the sea going maritime capacity of Djibouti, Kenya and the Seychelles. The mission is to be extended as soon as possible to also support Tanzania.

The EU cooperates on this mission with the International Maritime Organisation (IMO), the United Nations Office on Drugs and Crime (UNODC) and the United Nations Development Programme (UNDP).⁵⁴ The CMPD was in charge of forming these partnerships to execute and deliver the mission.⁵⁵

The missions described above illustrate the EU's effort to not only actively engage, through the CSDP, in various security-related challenges, but to have in place a broader security strategy in order to achieve mission success and raise its international standing. Accordingly, the EU is in the process of revising its crisis management procedures in a manner that would improve the effectiveness of CSDP planning, decision-making, execution and evaluation. Concrete proposals are expected in the near future. The activation of the EU Operations Centre is one of concrete manifestations of this objective.

⁵⁴ See EUCAP NESTOR webpage: <http://www.consilium.europa.eu/eeas/security-defence/eu-operations/eucap-nestor?lang=en>

⁵⁵ The mission will also work in an integrated and complementary manner with other interventions of the EU especially humanitarian aid and development cooperation. For more detailed information see "Factsheet on EUCAPNESTOR". Available at: http://www.consilium.europa.eu/media/1704166/eucap_nestor_fact_sheet12072012.pdf (Last accessed 10 Dec 2012).

3. The Space Crisis Management Requirement

The growing volume of orbital debris, increasing number of space-faring nations and space aspirants, new and emerging space technologies and their proliferation to a large number of state and non-state actors all point to an increasing potential for a space-related crisis. At the same time, management of such a crisis is a complex endeavour requiring a well-crafted vision and architecture for global space security as well as a strategic approach to contextualising and responding to challenges in this environment.

It is useful to note that there are two broad categories of space-related crises: natural and man-made. The public perception of the negative effects caused by the first type of crisis would likely be fundamentally different than the second. While the public response to a terrestrial natural catastrophe is generally positive and generous, the reaction in case of man-made space trauma would probably be swift and harsh, especially as the harmful knock-on effects were calculated. Such complex and uncertain situations could be manipulated, rather than controlled, by certain political elites and public opinion. The outbreak of World War I in 1914, in reaction to a political crisis, serves as a sober reminder of escalatory spirals not necessarily desired by everybody caught therein.

The growing dependence on space assets and the limited capability to protect them, compounded by the problem of verifying activities in space, all present daunting challenges to managing a space crisis. The high level of integration of space assets into military operations, particularly in the cases of the U.S. and Russia, make these assets tempting targets. Indeed, any meaningful disruption of essential space functions or operations would likely require extensive political and technical damage control.

While the U.S. is still the most advanced space power, several other space-faring nations are seeking to increase their influence in world affairs via space. This competitive, and increasingly contested, environment is not particularly conducive to efforts to establish rules of the road for space and new forms of cooperation. In short, space is still perceived as an ideal arena for demonstrating a nation's pride, independence, and capabilities.

Accordingly, the ability of Washington and its allies (e.g. the EU) to be accepted as the "rule-maker" is diminished and often regarded as suspect by those space actors that view space as a sphere of opportunity to enhance their strength, and even challenge U.S. primacy. Communication among these actors, and achieving consensus among them, under such circumstances is difficult, if not impossible.

In tackling these challenges, it is helpful to examine some of the key causes of a possible space crisis. Patrick Lin, Associate Professor at the California Polytechnic State University, for example, reflected on a seemingly remote aspect of a potential space crisis. In his 2006 article on "space ethics", he pointed out: "... relevant lessons from history may include our recent development of cyberspace, or the Internet frontier. Without planning ahead for related intellectual property issues as well as online sales tax, Internet crimes, and other areas, the rush into cyberspace has been messy at best."⁵⁶ With regard to space exploration and exploitation he added: "What is to prevent problems on Earth from following us into outer space, if we have not evolved the attitudes, and ethics, which have contributed to those problems? ... We have already littered the orbital environment in space with floating debris that we need to track so that spacecraft and satellites navigate around, not to mention abandoned equipment on the Moon and Mars."⁵⁷ The intention of several countries to exploit lunar elements and minerals may also one day lead to a crisis should the legal status of the celestial bodies not be adequately clarified.⁵⁸

In the U.S., the Department of Defense (DOD) views the space environment as having fundamentally changed and describes it with the so-called "three Cs" (i.e. congested, contested and competitive). Space is increasingly congested due primarily to space debris, contested by a growing array of foreign coun-

⁵⁶ Lin, Patrick. Viewpoint: Look before taking another leap for mankind – ethical and social considerations in rebuilding society in space. In: *Astropolitics*, Vol. 4, 2006: Philadelphia, Taylor&Francis, pp. 281 – 294.

⁵⁷ *Ibid*: 285.

⁵⁸ Brearley, Andrew. Mining the Moon: Owning the night sky? In: *Astropolitics*, Vol. 4, 2006: Philadelphia, Taylor&Francis, pp. 43 - 67.



terspace capabilities, and competitive as more and more countries and companies operate in space.

If one accepts that the space backdrop is shaped by the “3 Cs”, an issue becomes how to best delineate the “international relations” arena where all actors in a potential conflict should be involved in its resolution. Another well-known category of “3 Cs” – cooperative, competitive and confrontational – has also been used to describe world affairs more generally and assumes that each stage of a potential conflict involves different behavior on the part of rational actors. That said, it is currently difficult to anticipate the reactions of many members of the international community to a crisis in space, as different actors attach varying levels of importance to space capabilities.

3.1 Defining Space Crisis Management

In defining space crisis management, the main focus is on efforts to identify those situations that are conducive for threats to space assets and related services. In this sense, the goal of space crisis management is to preserve a peaceful and stable space environment. There are clear space-related implications stemming from heightened terrestrial tensions or mishaps. Those terrestrial circumstances that can result in damage to, or disruption of, space-based and ground-based assets have not been fully explored. For example, many satellites are dual use, making it difficult to differentiate between friend and foe. Unlike space safety and sustainability, which have received significant attention in various venues, including the United Nations Committee on the Peaceful Use of Outer Space (UNCOPUOS), space stability and deterrence is a more sensitive challenge and requires closer examination.

In an actual crisis, it is unlikely that Allison’s above-mentioned Model I alone, where events are a result of “purposive acts of unified national government”⁵⁹, will apply. Model II, where a multiplicity of organisations follow standard operating procedures (SOP) appears to be the best solution. However, because of the limited number of incidents and crises involving space, the establishment of such procedures did not, as yet, materialise, except perhaps in the U.S.–Russian relation-

⁵⁹ Allison, Graham. “Conceptual models and the Cuban Missile Crisis.” *American Political Science Review* (Sep 1969) 63/3, p. 690.
<<http://www3.nccu.edu.tw/~lorenzo/Allison%20Conceptual%20Models.pdf>>

ship. It may well take a profound future crisis to persuade the international community to implement suitable processes, organisations and understandings regarding space security. Accordingly, Model III may also apply, as was the case during the Cuban Missile crisis, with individuals within the involved governments divining the outcome.

In addition to obstacles connected with configuring domestic space crisis decision-making procedures, crisis prevention on an international level represents an even more challenging task given the limited exercise of space “rules of engagement”. Such an undertaking would involve the promotion of behaviour that maximises the utility and stability of space and minimises the prospects for misconduct and misperceptions. This process has been underway via attempts to advance codes of conduct/rules of the road, debris mitigation, transparency and confidence-building measures (TCBMs), and other modalities. Reducing the incentives and stepping up the disincentives associated with taking destabilizing actions is the proverbial “name of the game”.

This task is becoming increasingly complex with the growing number of space-faring nations and the nature of their ambitions. As democratic countries face periodic changes of leadership, it is crucial that well-defined national priorities and procedures are firmly in place to achieve successful international negotiation and/or action (military or otherwise). This has proven elusive even among allies, let alone among all active members of space community. The connectivity between terrestrial military hostilities and space is likely the most problematic (e.g. GPS signals jamming during the Iraqi conflict and other such circumstances).

To conclude, there is a marked difference in behavioural norms when dealing with peacetime versus crisis and conflict. A key objective of an effective space crisis management regime should be preventing crises before they mature, in part through the ability to gain international consensus on a set of rules governing responsible space behaviour, along with effective verification and enforcement measures.

3.2 Potential Space Crisis

Crises in space could be triggered by natural causes (e.g. space weather and debris), technical issues (e.g. satellite malfunction, unintentional interference, inaccurate orbital prediction) or intentional disruption of satel-

lite services and even the attack of space assets.

Space Situational Awareness (SSA), a fundamental element of space operations, is required to detect various anomalies, including those connected with a satellite's designated flight path. Due to the limitations in SSA capabilities, it can be difficult to detect and attribute potentially irresponsible or hostile actions in space. This makes space crisis management more complex than the terrestrial variety, although fact-finding, of course, involves far more than just SSA. Even though space crises caused by natural hazards or technical issues are of high concern, the intentional disruption of, or damage to, space assets will generally involve larger – sometimes far larger – geopolitical stakes.

Natural Hazards, Uncontrolled Re-Entries, Collisions and Unintentional Radiofrequency Interference

Space debris, the main contributor to “congested space”, has received substantial attention from the space community at national as well as international levels. A number of space-faring nations have adopted strict space debris mitigation guidelines, including the U.S., Russia, Japan and a number of European nations. The need for steps beyond debris mitigation, such as active debris removal (ADR), has also been acknowledged as relevant and is being pursued to some extent. Significant damage to, or destruction of, space assets (e.g. the International Space Station) would not only be a disaster, but would trigger an immediate need for crisis management steps, apart from having a debilitating effect on the near-term pursuit of human space exploration.

Effects from space weather (i.e. the Sun and the solar wind) are also considered significant threats to space operations. Although satellite components are partially protected against high total doses of radiation, it is nearly impossible (and prohibitively costly) to design and manufacture a satellite completely immune from space weather variations. Solar activity, occurring during all phases of the solar cycle, needs proper monitoring and assessment, especially given the lack of ability to accurately predict space weather.

The re-entry of shut-down or malfunctioning satellites, such as the U.S. Upper Atmosphere Research Satellite (UARS), Germany's Röntgen SATellite (ROSAT), or Russia's Phobos-Grunt, have not been considered high-level risk events, but have drawn attention to the need for better communication between all involved parties, as well as with the public.

The UARS, decommissioned in 2005, re-entered the atmosphere while tracked by the U.S. Joint Space Operations Center (JSpOC). The process was managed by the National Aeronautics and Space Administration (NASA). Besides the U.S., other space-faring nations were also monitoring the satellite's descent in the last two hours as the natural forces affecting the satellite made the prediction of re-entry difficult.⁶⁰ The ROSAT re-entry, handled by the German Space Agency (DLR), followed a similar re-entry procedure and ROSAT underwent an uncontrolled re-entry into the atmosphere in October 2011.

The case of Russia's Mars probe, Phobos-Grunt, was somewhat different from the previous two examples as Russia failed to provide timely information concerning issues it was experiencing with the satellite. After the Russian side finally announced technical problems, the U.S. set up a task force to assist the management of the re-entry.⁶¹ The members of the Inter-Agency Space Debris Coordination Committee (IADC), including the European Space Agency, used orbital data from the U.S. SSN and the Russian Space Surveillance System to determine the Phobos-Grunt's re-entry path. Radar systems of Germany and France also provided orbital calculations.⁶² The whole process, as well as the Russian explanation of the cause of the failure, lacked the desired level of accuracy and transparency.

Although thus far the only one of its kind, the 2009 collision between Iridium 33 and Cosmos 2251 also demonstrated the existence of a real threat of collision between two complete satellites. In short, although there have not, as yet, been any serious injuries (i.e. at least confirmed reports) resulting from the re-entries of the above-mentioned satellites, or other space objects, these events have highlighted the need for not only establishing domestic, national procedures, but also diplomatic processes that would facilitate the smooth and efficient management of these types of events internationally, including adequate public reporting.

Radiofrequency interference can undermine key functions of satellite (i.e. telemetry, tracking and command information (TT&C))

⁶⁰ “Final Update: NASA's UARS Re-enters Earth's Atmosphere”. <http://www.nasa.gov/mission_pages/uars/index.html>. (Last accessed 09 Dec 2012).

⁶¹ Oberg, James. Open issues with the official Phobos-Grunt accident report. *The Space Review* (27 Feb 2012). <<http://www.thespacereview.com/article/2035/1>>.

⁶² Atkinson, Nancy. “Few Details in ESA's Report on Phobos-Grunt Re-Entry.” *Universe today*, 25 January 2012. <<http://www.universetoday.com/92952/few-details-in-esas-report-on-phobos-grunt-re-entry/#ixzz2lhp37ces>> (Last accessed 22 Jan 2013).



and compromise the satellite's attitude control system and propulsion system leading to deterioration of orbit, loss of core mission capability or complete loss of communication. Unintentional radio frequency interference can originate from faulty equipment, the insufficient orbital spacing between satellites and the unauthorised use of satellite space segments by carriers. Intelsat's Chief Technical Officer, Thierry Guillemin, noted: "in our experience, episodes of signals from unauthorised carriers and of cross-polarisation make up 70 percent to 75 percent of radio frequency interference cases plaguing satellite operations ... to this number you should add a 15 percent to 20 percent of cases caused by adjacent satellite interference."⁶³

Intentional Disruption/Attack

As satellites (travelling in predictable orbits) collect, transport and deliver critical information and services to users on Earth, including national military forces, intentional disruption of the information/services they provide is an attractive option to some.

Intentional jamming (e.g. active jamming of radar imaging satellites, GPS location and timing information etc.) could have damaging military implications, as well as leading to potential political estrangement. Jamming satellite ground stations (the downlinks) and the satellite receivers (the uplinks) on unprotected systems, such as commercial communications satellites, can be relatively easy.⁶⁴ As commercial communications satellites are used heavily by the military forces of some other countries, this vulnerability is relevant to the security community and allied collaboration efforts.

Besides the challenge of GEO-locating the source of interference in an area covering hundreds of thousands of square kilometres, satellite operators are sometimes confronted with a policy challenge, such as the case of the jamming of a Eutelsat satellite by a source located on Iranian territory. In 2009, several major broadcast stations were jammed for many months by systems based in Iran raising significantly the costs to the broadcasters and satellite owner-operators involved and raising fundamental freedom of information issues. Although formal complaints were filed with the International Telecommunication Union (ITU), the situation has not been resolved and the Government of Iran has made no acknowledgement of this

issue. Iran's jamming of Eutelsat is described in more detail in section 3.3 as a realistic scenario relevant to future contingency planning.

A crisis could also be caused by: directed energy (laser or microwave) attack (e.g. using Earth-based laser to dazzle the optical arrays of electro-optical imaging reconnaissance satellites; use of satellites with active, high-powered radars to degrade the electronics of adversary satellites); kinetic energy anti-satellite (ASAT) attack (e.g. direct-ascent, co-orbital); or cyber attacks (e.g. capturing or corrupting the data streams to or from a competitor's satellite).

Cyber attacks against satellites and ground stations are a growing problem and stand out as a key vulnerability that can be added to the current array of political and budgetary obstacles to enhanced security in both the space and the cyber domain. Cyber attacks permit anonymity and might result in denial of service or otherwise incapacitating an adversary's satellites at a far lower cost, as well as enabling 'listening in' spying capabilities. There are already a number of known examples of cyber attacks against satellites resulting in the degrading or temporary loss of control.

3.3 Case Study: Iran's Jamming of Eutelsat

Background

Communication systems for satellites consist of a receiver, transmitter and radio antennae. Transmissions are usually encrypted and encoded. One of the key functions of satellites that generally require only a small part of the assigned bandwidth involves TT&C. Radiofrequency interference can undermine these key functions and compromise a satellite's attitude control system and propulsion system leading to a deterioration of orbit, loss of core mission capability or complete loss of communication.

Intentional forms of radiofrequency interference include jamming (i.e. disrupting communication with a satellite by overpowering the signals being sent to or from the satellite by using a signal at the same frequency and higher power) and spoofing (i.e. mimicking the characteristics of a true signal so that the

⁶³ Verlini, Giovanni. "New Efforts to Mitigate Satellite Interference." Giovanni Verlini. *Satellite Today*. March 1, 2010.

⁶⁴ Wright, David, Laura Grego and Lisbeth Gronlund. "The Physics of Space Security: a Reference Manual". American Academy of Arts and Sciences (2005): 17.

user receives the fake (or spoofed) signal instead of the real one).⁶⁵

Jamming the downlink would involve preventing a usable signal from reaching the recipient. Receivers which are designed to receive signals from satellites in various positions (and, therefore do not have to track a particular satellite) can be jammed by placing a jammer in the broadcast/receive area of such a receiver. There are several methods for countering efforts to jam the downlink, including increasing the power of the broadcasted signal; encoding the downlink signal; designing the receivers to only receive signals from the direction of the transmitters they are to communicate with (and reject signals from other directions); or having the satellite concentrate power in a small frequency band and the receiver filter out all other frequencies.⁶⁶

The receivers on the satellites (uplink receivers) accept command and control communications. These uplinks are normally protected from jamming by encoding the signal. The signal received from the ground is subsequently retransmitted. While the military may encode the signal before retransmitting it, commercial communications satellites are more vulnerable as they often retransmit data with little processing. Moreover, they are designed to receive signals from users over broad ground area providing larger territory from which to jam the uplink.⁶⁷

Spoofing, although similar to jamming, is more sophisticated. As with jamming, spoofing requires that the signal be in the vicinity of the ground station or source of the original signal. Spoofing involves sending a false signal to the ground receiver and would require the false signal to originate either nearby or in line of sight of the receiver. Countering spoofing requires the signal to be encrypted before it is sent and unscrambled after reception, which typically makes more sense in military applications due to the added cost and limits on the amount of data that can be sent and received in this fashion.⁶⁸

As commercial and communications satellites are used by the military, their vulnerability is also relevant to national security communities. Intentional jamming is increasingly used to accomplish military, political and social objectives.⁶⁹ As state-sponsored jamming

becomes increasingly prevalent, there is likely to be increased interest internationally in scripting appropriate responses to these kinds of actions. At present, this is an underdeveloped area of security policy as well as economic policy and diplomacy.

The Issue

A notable example of intentional jamming is that perpetrated from Iranian territory toward foreign TV and radio station broadcasts via satellite. Indeed, Iran's jamming activities have been occurring for over a decade, making the country a "repeat offender" in obstructing the free flow of information. It has routinely jammed the signal of international broadcasters, including BBC's Persian TV, RFE/RL's Persian Service and Radio Farda in an attempt to prevent media coverage criticising Tehran from reaching the Iranian people. The government seems to intensify its jamming efforts during sensitive periods (e.g. the 2005 Presidential elections; 2009 anti-government protests, etc.).

By December 2009, Iran's jamming of foreign satellite transmission had become more systematic. This was especially the case prior to the February 2010 anniversary of the 1979 Revolution, when almost seventy foreign radio and television programmes transmitted via Eutelsat were interrupted.⁷⁰ The jamming continued as the Arab Spring revolutions unfolded. In fact, Eutelsat has been one of the most affected companies by jamming incidents. The negative effect on their operations doubled between 2010 and 2011, and tripled from 2011 to 2012. Eutelsat has recorded 340 jamming incidents from January to November 2012, a high percentage of which originated from Iran.⁷¹

Between May 2009 and March 2010, Eutelsat presented complaints before the France's Agence Nationale des Frequences Francaise (ANFR) and the ITU's Radio Regulations Board (ITU-R).⁷² Article 45 of the ITU's con-

<http://www.pbs.org/wgbh/pages/frontline/tehranbureau/SatelliteJammingInIranSmallMedia.pdf>

⁷⁰ "EU ready to act on Iran satellite jamming" Reuters, 19/03/2010. Available at:

<<http://in.reuters.com/article/2010/03/19/idINIndia-47063720100319>> (Last accessed 28 Nov 2012).

⁷¹ "Broadcasters condemn Jamming as Violation of Article 19", Radio Free Europe, 21/11/2012. Available at: <<http://www.rferl.org/content/journalists-in-trouble-broadcasters-comdemn-jamming/24777220.html>> (Last accessed 28 Nov 2012). See also "Satellite and Internet Jamming rises as broadcast industry seek to uphold UN Article 19", BBC Media Centre, 20/11/2012. Available at: <<http://www.bbc.co.uk/mediacentre/latestnews/2012/201112wsjammingconference.html>> (Last accessed 28 Nov 2012).

⁷² See "Eutelsat Statement concerning transmissions of BBC Persian, Deutsche Welle and Voice of America in

⁶⁵ Wright, David, Laura Grego and Lisbeth Gronlund. "The Physics of Space Security: a Reference Manual". American Academy of Arts and Sciences (2005): 118.

⁶⁶ Ibid: 120.

⁶⁷ Ibid:121-122.

⁶⁸ Ibid.

⁶⁹ "Satellite Jamming in Iran: A War Over Airwaves". A Small Media Report, PBS, November 2012. Available at:



stitution states, among other provisions, that the Member States “recognize the necessity of taking all practicable steps to prevent the operation of electrical apparatus and installations of all kinds from causing harmful interference to the radio services or communications mentioned in the provision no. 197 above.”⁷³ In other words, the deliberate jamming of another party’s satellite transmissions is a violation of the ITU’s rules and damages the satellite industry as a whole.

Although Iranian officials acknowledged the signal jamming in the summer of 2012, as well as its potentially negative consequences, the government did not assume responsibility for it. Iran’s current Minister of Communications and Information Technology, Reza Taghipour, denied his department’s involvement in jamming satellite signals, and stated that the Ministry was reviewing the case.⁷⁴ Iran’s Communication Regulatory Authority, which is the country’s sole radio and communications regulator, has also denied knowledge concerning the source of the jamming.⁷⁵

Since October 2012, the deliberate interference of several international networks from Iran’s territory has increased, obstructing – as reported by the EU – more than 500 television channels and 200 radio channels broadcasted by Eutelsat. Among the affected channels were Britain’s BBC, France 24, Germany’s Deutsche Welle and US-funded Voice of America. This deliberate interference with satellite signals was – and still is – affecting not only broadcasting on Iranian territory, but also international broadcasting to other Middle East regions.

On 4 October 2012, Eutelsat released a statement where it strongly condemned the jamming activities and appealed again to international regulatory authorities, as well as the French Government, to intervene urgently. Also in October 2012, in reaction to Iran’s refusal to assume responsibility and failure to stop the jamming, Eutelsat re-

moved nineteen of the Islamic Republic of Iran Broadcasting’s (IRIB) television and radio channels broadcasting to Iran. Intelsat followed this step by blocking Iran’s official broadcast channels in Europe since 25 October 2012.⁷⁶ That same month, the International Telecommunications Union (ITU) issued a statement condemning all types of harmful interference. The statement called on its 193 Members States “to exercise the utmost goodwill” in respecting the provisions of ITU constitution, as “any transmission which has the intent to cause harmful interference is an infringement of the ITU constitution”.⁷⁷

The Eutelsat decision to remove the IRIB channels was strongly criticized by Teheran. Iran’s Ambassador to France, Ali Ahani, after a meeting with Eutelsat’s CEO, released a statement where he affirmed that “depriving millions of viewers and listeners of television and radio programs of different channels of the Islamic Republic of Iran across the world is a blatant violation of human rights and international treaties which emphasize freedom of expression and freedom of public access to news and information”.⁷⁸ He also argued that Eutelsat’s decision was a breach of existing treaties between France and Iran, as his country was not responsible for the jamming. Moreover, Iran accused other Western countries of using double standards. Iranian Press TV reported that Eutelsat’s decision to stop the broadcasting was ordered by the European Commission.

The European Commission immediately rejected the accusations. It denounced the jamming and expressed concerns “over measures taken by the Iranian authorities to prevent its citizens from freely communicating and receiving information through TV, radio satellite broadcasting and the internet.” It likewise stated that “the EU is determined to pursue these issues and to act with a view to put an end to this unacceptable situation.”⁷⁹

Persian, via its satellites” of 17/03/2010. Available at: <[http://www.eutelsat.com/news/compress/en/2010/html/PR%201310%20statement%20BBC%20Persian_VOA\(3\)/PR%201310%20statement%20BBC%20Persian_VOA\(3\).html](http://www.eutelsat.com/news/compress/en/2010/html/PR%201310%20statement%20BBC%20Persian_VOA(3)/PR%201310%20statement%20BBC%20Persian_VOA(3).html)> (Last accessed 06 Dec 2012).

⁷³ See Constitution of the ITU: Chapter VII – Special Provisions For Radio. Available at: <<http://www.itu.int/net/about/basic-texts/constitution/chaptervii.aspx>>. (Last accessed 06 Dec 2012).

⁷⁴ “Who Is Behind Iran ‘Dangerous’ Satellite Jamming?”, Radio Free Europe, 23/08/2012. Available at: <<http://www.rferl.org/content/satellite-jammig-dangerous-health-iran/24686214.html>> (Last accessed 28 Nov 2012).

⁷⁵ Interestingly, the Deputy Minister of Iran’s Ministry of Information and Communications Technology (until 2010), Ahmad Talebzahed, also served as the chair of the UN Legal Subcommittee of the Committee on the Peaceful Uses of Outer Space (UNCOPUOS) from 2010 to 2011.

⁷⁶ “A Top Satellite Provider Cuts Off Iran State Broadcaster” Wall Street Journal, 15/10/2012. Available at: <<http://online.wsj.com/article/SB10000872396390444354004578058931263559160.html>> (Last accessed 09 Dec 2012). See also “ASL19 and the IMP examine Eutelsat’s decision to take IRIB off the air”, Iran Media Program, 13/11/2012. Available at:

<<http://www.iranmediaresearch.org/en/blog/227/12/11/13/189>> (Last accessed 09 Dec 2012).

⁷⁷ “ITU condemns satellite jamming”, Advanced Television, 29/10/2012. Available at: <<http://advanced-television.com/2012/10/29/itu-condemns-satellite-jamming/>> (Last accessed 06 Dec 2012).

⁷⁸ “Iranian Ambassador Slams Eutelsat”, Advanced Television, 31/10/2012. Available at: <<http://advanced-television.com/2012/10/31/iranian-ambassador-slams-eutelsat/>> (Last accessed 28 Nov 2012).

⁷⁹ “EU to act on Iran satellite jamming”, The New Economy, 24/10/2012. Available at:

The French government stated in November 2012 that it is "extremely concerned by the interference of satellites, which is a violation of international agreements". The findings of the ANFR – the fact that the jamming of Eutelsat satellites originated from Iran national territory – were sent to the ITU with a request to take action. In addition, the French government asserted that it was also discussing possible sanctions with its European partners.⁸⁰

Moreover, the EEAS' High Representative urged Iran to stop jamming the signal and to abide by its international legal obligations derived from the International Covenant of Civil and Political Rights and to its ITU commitments. The High Representative reiterated that Iran must "respect the universal right to free expression including the right of any individual to seek, receive and share information, irrespective of borders" and "to cooperate in the detection and elimination of harmful interference".⁸¹

Implications

Deliberate interference with broadcast signals constitutes a violation of the international legal regime (e.g. ITU Constitution's Article 45,⁸² the Outer Space Treaty's Article 9⁸³, the UN Charter's Article 19⁸⁴). At the same time, no concrete guidelines exist concerning how to prevent politically intentional jamming (and, for that matter, other intentional inter-

ference with space assets) and how to proceed when they occur.

The strong sanctions, or the threat of such sanctions, as those focused on banks, trade and gas exports employed by the EU (as well as the U.S. and UN Security Council) against Iran over its controversial nuclear programme, have, so far, had limited effectiveness. Iran continues to enrich uranium, as confirmed, for example, by a November 2012 report by UN inspectors.⁸⁵

Eutelsat's move to take off the air nineteen Iranian state-run TV and radio channels in October 2012, reinforcing other EU Council sanctions, is unlikely to cause a significant impediment to the regime's practices and people in the Middle East still have access to most of the channels operated by the IRIB (including English-language news service, Press TV, and Arabic-language al-Alam).⁸⁶ In short, Iran, a member of the UN and ITU, as well as a signatory to the Outer Space Treaty, may continue this destructive brand of "business as usual".

Despite the ability to attribute technically the jamming source to a territory, and Iran's acknowledgement that the jamming is taking place within its territory, Teheran refuses to take responsibility to resolve this issue.

The EU, notwithstanding several declarations by the High Representative and the EU Member States calling on Teheran to stop the jamming of satellite broadcasting, has not made any significant progress in altering Iran's behaviour. This involuntarily tolerant attitude could, however, produce a potential space crisis in the future far more acute than just the jamming of commercial media broadcasting. The crisis management model on display in this context may not prove a viable one to generalise for space.

<<http://www.theneweconomy.com/strategy/eu-to-act-on-iran-satellite-jamming>> (Last accessed 28 Nov 2012).

⁸⁰ "France asks ITU to take action", Broadband TV News, 12/11/2012. Available at

<<http://www.broadbandtvnews.com/2012/11/12/france-asks-itu-to-take-action/>> (Last accessed 28 Nov 2012).

⁸¹ EU points its finger to Iran for jamming the signals of European Channels in Middle East", New Europe Online, 14/11/2012 Available at:

<<http://www.neurope.eu/article/eu-points-its-finger-iran-jamming-signals-european-channels-middle-east>> (Last accessed 28 Nov 2012).

⁸² Article 45 states that "Member States recognises the necessity of taking all practicable steps to prevent the operation of technical apparatus and installations of all kinds from causing harmful interference to the radio services or communications" (see: ITU Constitution. Available at: <http://www.itu.int/aboutitu/Basic_Text_ITU-e.pdf>)

⁸³ The Outer Space Treaty's Article 9 refers to the necessity for States Parties to avoid any "harmful interference". Jamming can also be considered "harmful interference". (See: Outer Space Treaty in United Nations Treaties and Principles on Outer Space". Available at: <<http://www.oosa.unvienna.org/pdf/publications/STSPACE11E.pdf>>)

⁸⁴ Satellite jamming can be seen as a violation of Article 19 of the UN Charter. The Article states that individuals should have 'the freedom to seek, receive and impart information and ideas through any media and regardless of frontiers'. (See: Charter of United Nations. Available at: <<http://treaties.un.org/doc/Publication/CTC/uncharter.pdf>>)

⁸⁵ See "Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran" IAEA Report. 16/11/2012 Available at:

<http://www.isisnucleariran.org/assets/pdf/Iran_safeguards_report_November_2012.pdf> (Last accessed 06 Dec 2012).

⁸⁶ "EU imposes new sanctions on Iran", BBC News, 15/10/2012. Available at: <<http://www.bbc.co.uk/news/world-middle-east-19947507>> (Last accessed 28 Nov 2012).



4. Space Crisis Management for Europe

The development and utilisation of space assets for Europe's crisis management is being supervised by the EU, in close collaboration with the Member States and ESA. The EEAS, which defines the coordination and resourcing mechanisms associated with the use of space for terrestrial crisis management and "external action", has not, as yet, systematically integrated space crisis management into its operations.

The EU's security-related space activities are primarily managed by the European Commission (EC), the European Defence Agency (EDA) and the European Union Satellite Centre (EUSC). The European Space Agency (ESA) acts as the programme coordinator and procurement authority for most of these projects.⁸⁷

The EU recognises its increasing reliance on space-based systems as well as the proliferation of threats to these systems and aims at developing space monitoring capability at a Europe-wide level.⁸⁸ The 2008 Space Council resolution, as well as subsequent resolutions, emphasised the need for "a European capability for the monitoring and surveillance of its space infrastructure and of space debris".⁸⁹ To develop an SSA system at European level, the EU recognises the need to cooperate with ESA and Member States, owners of such assets, as well as to develop a proper governance and data policy to manage highly sensitive SSA data.⁹⁰

The EC's April 2011 space strategy document entitled "Toward a Space Strategy of the European Union that Benefits its Citizens", acknowledged that space infrastructure

serves both as "an instrument" which can advance the EU's security and defence needs (e.g. GMES, MUSIS, etc.), but also as "an asset" requiring protection. The main threats outlined in the document were natural phenomena, collision and electromagnetic interference.⁹¹

NATO is also an organisation relevant to Europe's space crisis management. There are different opinions as to whether Europe's space security (including space crisis management) collaboration with the U.S. should be conducted primarily through NATO. With most SSA assets owned by individual member states that remain reluctant to "contribute" such assets to NATO, some view the organisation as ill-equipped, at least at this juncture, to be the centrepiece of European space crisis management, although the NATO avenue obviously remain an important part of the puzzle when it comes to framing proper space crisis management responses.

NATO's Allied Command Transformation (ACT) located in Norfolk, Virginia, "NATO's leading agent for change, driving, facilitating, and advocating continuous improvement of Alliance capabilities to maintain and enhance the military relevance and effectiveness of the Alliance"⁹², published in April 2011 a report entitled, "Assured Access to the Global Commons". It was designed to stimulate attention within NATO to the need to maintain unfettered access to shared domains, identified by this report as including maritime, international airspace, cyber space and outer space.⁹³

⁸⁷ Schrogl, Kai-Uwe et al. "Yearbook on Space Policy - 2009/2010: Space for Society". SpringerWienNewYork (2011), pp. 100-101.

⁸⁸ See the section "Security of Space" of European Commission webpage: <http://ec.europa.eu/enterprise/policies/space/esp/security/assets/index_en.htm> (Last accessed 10 Dec 2012).

⁸⁹ *Cit.*, "Taking forward the European Space Policy", 5th Space Council Resolution (26 September 2008), p.13. Available at:

<http://register.consilium.europa.eu/pdf/en/08/st13/st13569_en08.pdf> (Last accessed 10 Dec 2012).

⁹⁰ See "Toward a Space Strategy of the European Union that Benefits its Citizens", Council Conclusion (31 May 2011). Available at:

<http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/intm/122342.pdf> (Last accessed 10 Dec 2012).

⁹¹ See "Toward a Space Strategy of the European Union that Benefits its Citizens", European Commission Communication (4 April 2011), p. 5. Available at:

<http://ec.europa.eu/enterprise/policies/space/files/policy/comm_pdf_com_2011_0152_f_communication_en.pdf>. (Last accessed 10 Dec 2012).

⁹² See "Vision Statement.", NATO's Allied Command Transformation. Available at: <<http://www.act.nato.int/>> (Last accessed 10 Dec 2012).

⁹³ See Maj.Gen. Mark Barrett, Dick Bedford, Elizabeth Skinner and Eva Vergles. "Assured Access to the Global Commons." NATO Allied Command Transformation. April 2011. Available at: <<http://www.act.nato.int/mainpages/globalcommons>> (Last accessed 10 Dec 2012).



Figure 3: Four functions of space operations as described by NATO ACT (source: NATO ACT's MNE 7 Report "Space: Vulnerabilities, Dependencies and Threats")

The interest in preserving access to these domains serves broad economic and security interests. Indeed, this report held out the possibility of this programme continuing through the Multi-National Experiment 7 (MNE-7) taking place over the course of 2011 and 2012 which is evaluating these four domains.⁹⁴

A space handbook, prepared as part of the MNE-7, entitled "Space: Dependencies, Vulnerabilities and Threats", includes, in its case study five, a focus on how space operations are conducted and managed in practice in the continuous presence of threats and hazards, and an environment of military secrecy and commercial sensitivity (i.e. how the space and ground segments of space operations are successfully managed) (see figure 3).⁹⁵

The NATO ACT report on global commons and the MNE-7 exercise is anticipated to help define the potential roles and responsibilities of member states in assuring access to these

⁹⁴ The Multinational Experiment (MNE) series have been running since 2001. Each 2-year experiment is designed to examine a topical defence and security issue and MNE 7 (the latest in the series) is focused on access to the global commons. The experiment involves 17 participating countries and NATO and runs until December 2012.

⁹⁵ "Space: Dependencies, Vulnerabilities and Threats", MNE7 (2012). Available at: <http://www.mod.uk/NR/rdonlyres/79DFAC54-D002-4B10-AEB4-73305103120C/0/20120313mne7_space_vulnerabilites.pdf> (Last accessed 10 Dec 2012).

areas for economic and national security purposes and establish a more defined role for NATO to advance allied collaboration on a range of issues, including this dimension of space security.

The current European agenda on space security is dominated by the discussion, debate and diplomacy associated with the proposed Code of Conduct for Outer Space Activities introduced by the EU in 2008, 2010, and 2012, respectively. The Code has also, over the past few years, attracted priority attention internationally. Although the EU is a relatively recent space actor at a global level, it is striving to establish policies and procedures that protect Europe's space assets. This is especially important at a time when current EU policy heavily emphasises an independent European access to, and use of, space (including Europe's next-generation launching capability, Galileo, Earth Observation, space-based terrestrial crisis response infrastructure and SSA).

There has been significant debate regarding the Code, with those opposed to the plan highlighting the lack of adequate negotiation procedure, as well as verification, compliance and enforcement provisions of the proposal, and the flexibility and exceptions it appears to grant to signatories for actions that are deemed to be in their respective national interests. It is feared that the Code will tie the hands of responsible governments and



open the door for irresponsible regimes to gain an upper hand through “cheating” or adopting a liberal, self-serving interpretation of the agreement.

As the Code is of a preventive nature, it would be beneficial to identify how to marry the Code’s Transparency and Confidence Building Measures (TCBMs) with proper space crisis management. There has not been sufficient discussion of – or solutions provided for – what member states might do, in reasonably precise terms, in the event that the identified rules of the road are violated.

Although there is no doubt that the incidental or naturally-caused space security issues are significant, the real challenge for the EU will be to address man-made threats to a secure space environment. In short, the implications of increasingly sophisticated counterspace systems in the hands of less-responsible actors are still to be acted upon in Europe.

At this stage, the individual Member States are currently better positioned to contribute

actual capability as well as political capital with regard to space crisis management planning. Politically, there are also fewer obstacles to making security-oriented decisions with regard to cooperation in militarily-sensitive space situations. Among European states, France is a leader in developing national crisis space capabilities, including communications, Earth observation and SSA.

In short, the space security (sometimes labelled “security of space”) debate in a European setting consistently gravitates back toward the challenges posed by incidental or naturally-occurring phenomena, which are less challenging issues to grapple with politically. Adding space crisis management as a central agenda item concerning space security is desirable as intentional acts could jeopardise space stability systemically. That said, the space policy agenda of the EU continues to evolve and this could open new windows of opportunity for establishing the EU’s space crisis management strategy.

5. Conclusion

Space crisis management needs to be underpinned by strong and persistent diplomacy aimed at preventing crises, encouraging the accelerated development of the operational and technical capabilities to manage a crisis already underway, and ensuring the availability of effective organisational structures to facilitate sound crisis management processes. Identifying EU's priority objectives in this arena, including European cooperation with other space-faring governments, international organisations and multilateral fora, will bring positive results and cost-effectiveness to the EU's efforts to protect its space assets.

Collaborative space crisis management needs to embody: several methods of crisis prevention; rapid detection and reporting of a threat/attack; accurate assessments of the threat; and high-tempo policy responses. Political will is an essential component of this task, including at the international level, as developing collaborative arrangements for space crisis management are at a nascent stage of development, even at a time of rapidly emerging new threats. Fortunately, several aspects of space crisis prevention, including debris mitigation, collision avoidance, SSA, TCBMs and others, are further along in being addressed, which offers firm ground for

the incorporation of counterspace and other urgently needed space security instruments.

Should an incident occur, there would likely be little to no time for "dress rehearsals" or planning/policy debates. If Europe is not ahead of the curve on these scenarios, it will be playing catch-up in a perilous environment with potentially immense stakes. Accordingly, the next few years will be especially important in not only establishing responsible norms of space behaviour, but also gaining agreement on clear procedures to deal with escalatory spirals and other unexpected contingencies, particularly of the man-made variety. An actual space crisis will likely elude abstract models and even a set of universal rules, and rather require a tailor-made solution by those actors and individuals involved. However, for that to happen in an effective way the tool box must be to hand, as no tailor can work without instruments.

That said, there is far more that can be done in the area of pre-crisis planning and closer, more security-minded discussions among key allies. Space, in its many facets, has simply become too important to day-to-day life on Earth for anything less than the sustained engagement of the highest levels of government, NGOs and the private sector.



6. Recommendations

Space is an integral component of EU's "comprehensive" approach to security and foreign policy. The following recommendations are offered to better integrate space crisis management into Europe's broader space security concerns:

- Drawing on terrestrial crisis management experiences, put forward policy measures, information sharing/safeguard measures, investment strategies and other elements required for bolstering Europe's space crisis management capabilities.

EU leadership – particularly through the EEAS – is a prerequisite for an effective dialogue on space pre-crisis planning and management among the relevant European actors in space. Europe's acknowledgement of a space crisis management requirement, including the upgrading of its infrastructure, expertise and policy awareness, will advance its ability to identify space-related threats and respond to them with agility and effectiveness in a time-sensitive environment. This will involve partner governments assuming specific, complementary responsibilities in this area of space security and instituting the necessary policy measures to align more closely current space capabilities with space crisis management requirements.

- While the EU's leadership in outlining prudent next steps for space crisis management takes the most realistic course, it can only be effective if the EU defines the "chain of command" for its space security establishment and speaks to partners with "one voice." The High Representative should task the EEAS with taking the lead in creating a space crisis management architecture for addressing a range of threats (both natural and man-made), as well as communicating with partner space-faring nations on the most effective, timely responses.

EU consistency and attentiveness concerning its policies, programmes and contingency planning will likely persuade European member states and other stakeholders to support a security-minded space agenda and make the necessary financial resources available. Centralising space crisis management at the EEAS would both signal the importance of this issue area and help streamline the chain of command on these higher velocity decision situations. Such a top-down approach would also help mobilise the complex

bureaucratic processes associated with the establishment of a Space Crisis Management cell.

- The EU should start a dialogue with NATO on space crisis management and define this portfolio within their respective security mandates.

Establishing guidance concerning how the EU and NATO might jointly respond to an incident in space would be desirable. NATO ACT's report describing space-related threats, dependencies and vulnerabilities, and the development of this concept by the Multi-National Experiment 7 (MNE-7) are concrete steps in the right direction.⁹⁶

- Tighten transatlantic interaction on space crisis management as part of the EU–U.S. broader bilateral engagement and consider more robust coordination with other countries (e.g. Japan).

The EU's willingness to engage in the establishment of a transatlantic security framework to facilitate bilateral discussions on space security-related issues would likely benefit and accelerate its work programme in this area. It would also demonstrate the global relevance and importance of this issue. Examining space crisis management from the transatlantic perspective could also contribute importantly to the broader security dialogue and advance the configuration of a multilateral space security architecture.

- Undertake Europe-wide space crisis management exercises.

The EU should consider creating space crisis management exercises or simulations covering the political/strategic and operational/tactical levels of crisis scenarios, making use of existing frameworks (e.g. the EU Crisis Management Exercise (CME), EU Military Exercise (MILEX), and NATO's Crisis Management Exercise (CMX)). Such exercises or games would likely reveal gaps in pre-crisis planning as well as the ability of existing institutions and arrangements to react to various space contingencies in real time, particularly the man-made variety.

⁹⁶ Maj. Gen. Mark Barrett, Dick Bedford, Elizabeth Skinner and Eva Vergles "Assured Access to the Global Commons." NATO Allied Command Transformation. April 2011. Available at: <http://www.act.nato.int/mainpages/globalcommons> (Last accessed 10 Dec 2012).

List of Acronyms

Acronym	Explanation
A	
ADR	Active Debris Removal
AMISOM	African Union Mission in Somalia
ANFR	Agence Nationale de Fréquences
APSCO	Asia-Pacific Space Cooperation Organization
AU	African Union
C	
CIVCOM	Civilian Aspects of Crisis Management Committee
CFSP	Common Foreign and Security Policy
CMC	Crisis Management Concept
CMO	Crisis Management Operation
CMP	Crisis Management Procedure
CMPD	Crisis Management and Planning Directorate
CNAD	NATO's Conference of National Armaments Directors
CONOPS	Concepts of Operations
COREPER	Permanent Representative Committee
CPCC	Civilian Planning and Conduct Capability
CSDP	Common Security and Defence Policy
CSOs	Civil Strategic Options
D	
DLR	Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center)
DoD	Department of Defense
DSACEUR	Deputy Supreme Allied Commander Europe
E	
EC	European Commission
ECAP	European Capability Action Plan
EDA	European Defence Agency
EEAS	European External Action Service
EEAS ESG	European External Action Service Executive Secretary General
EPC	European Political Cooperation
ESA	European Space Agency
ESDP	European Security and Defence Policy
ESS	European Security Strategy
EU	European Union
EUCAP	European Union Maritime Capacity-Building Mission (in the Horn of Africa)



Acronym	Explanation
EUCME	European Union Crisis Management Exercise
EUFOR	European Union Force
EUMC	European Union Military Committee
EUMILEX	European Union Military Exercise
EUMS	European Union Military Staff
EUNAVFOR	European Union Naval Force
EUSC	European Union Satellite Centre
EUTM	European Union Training Mission
H	
HR	High Representative
J	
JDEC	Joint Data Exchange Center
JSpOC	Joint Space Operations Center
I	
IMD	Initiating Military Directive
IMO	International Maritime Organisation
IRIB	Islamic Republic of Iran Broadcasting
ITU	International Telecommunication Union
M	
MNE-7	Multi-National Experiment 7
MSOs	Military Strategic Options
MPRA	Maritime Patrol and Reconnaissance Aircrafts
N	
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
NATO ACT	NATO Allied Command Transformation
NATO CMX	NATO's Crisis Management Exercise
NRF	NATO Response Force
O	
OPLAN	Operation Plan
OSCE	Organisation for Security and Cooperation in Europe
P	
PLNS	Pre- and Post-Launch Notification System
PSC	Political and Security Committee
PSOs	Police Strategic Options
PSSI	Prague Security Studies Institute
S	
SEA	Single European Act
SG	Secretary General
SHAPE	Supreme Headquarters of Allied Power Europe
SOP	Standard Operating Procedures

Acronym	Explanation
SOR	Statement of Requirements
SSA	Space Situational Awareness
T	
TCBMs	Transparency and Confidence Building Measures
TT&C	Telemetry, Tracking and Command information
TEU	Treaty on the European Union
U	
UNCOPUOS	United Nations Committee on the Peaceful Uses of Outer Space
UNODC	United Nations Office on Drugs and Crime
UNDP	United Nations Development Programme
UNSC	United Nations Security Council
U.S. UARS	U.S. Upper Atmosphere Research Satellite
V	
VPD	Vessel Protection Detachment
W	
WFP	World Food Programme



Annex

A.1 Project Methodology

The space crisis management project emanated from a large international conference entitled “Space Security through the Transatlantic Partnership,” co-organised by ESPI and the Prague Security Studies Institute (PSSI) in June 2011. A follow-up roundtable focusing solely on this topic was organised by ESPI (on its premises) on 29 March 2012. The roundtable, entitled “Space Crisis Management: Filling the Gaps”, is described in more detail below.

To augment and reinforce this study, interviews with professionals in the areas of space policy, crisis management and space security from ESA, the EU, the national space agencies of Europe, various U.S. space-related governmental entities, commercial operators, academic experts and non-governmental organisations were conducted prior, during, and after the Prague conference and the ESPI roundtable. Continuous in-house, open source research has likewise been conducted throughout the course of the project.

On 29 March 2012, ESPI organised, on its premises in Vienna, a roundtable on “Space Crisis Management: Filling the Gaps”. Jana Robinson, the report’s author, was responsible for this event. The roundtable participants sought to explore various means for crisis prevention, including proposals for transparency and confidence-building measures (TCBMs). Several participants indicated that Europe and the U.S. need to set their sights on the global space “enterprise” and identify ways to bring other countries into that “enterprise” in a transparent, realistic and productive framework.

Participants included Richard Buenneke, Senior Adviser for Space Policy, U.S. Department of State; Amber Charlesworth, Foreign Affairs Officer, Office of Space and Advanced Technology, U.S. Department of State; Veronica Cody, Head of Division for Concepts, Civilian Capabilities, Training, Exercises and Lessons, Crisis Management Planning Directorate (CMPD), European External Action Service (EEAS); Neal Dewar, Group Captain MA RAF, HQ 1 Gp Space Control & Battlespace Management, United Kingdom; Peter Hays, Asso-

ciate Director, the Eisenhower Center for Space and Defense Studies of the USAF Academy; Peter Hulsroj, ESPI’s Director; Jean-Luc Lefebvre, Program Manager, New Strategic Concepts, Institute for Strategic Research of “Ecole Militaire” (IRSEM); Pascal Legai, Deputy Director, European Union Satellite Centre (EUSC); Frank Mueller, Director, Space Weather Cell, German Space Situational Awareness Centre (GSSAC); Spyros Pagkratis, ESPI Resident Fellow; Jana Robinson, ESPI Resident Fellow; Jakub Ryzenko, Head, Crisis Information Centre, Space Research Centre, Poland; Frank Schrottenloher, Chief of Space Environment Mastery Office, French Joint Space Command; Shawn Steene, Deputy Director for Space Policy & Strategy Development, Office of the Undersecretary of Defense for Policy, U.S.; Sarah Tarry; Action Officer, Defence Policy and Partnership Section, NATO HQ; Phillip Verroco, Air and Space Strategist, NATO Joint Air Power Competence Centre (JAPCC); and Alfred Vogel, Secretary-General, Austria’s National Defence Academy.

The roundtable sought to delineate essential tools for effective space crisis management, as well as realistic scenarios that could trigger crisis management responses. It was generally agreed that the asymmetric nature of space – where even a small satellite off course or an incident of neglect/misconduct, can cause disproportional damage – needs to be properly taken into account. Defining the nature of a space “event” is also important when trying to assess its consequences on national or regional security and other interests as well as how best to distribute relevant information to an array of parties (e.g. policy-makers, the media, commercial operators etc.). A number of the participants argued that for collaborative space crisis management to be successful, elaborate pre-crisis planning and an effective organisational structure are essential ingredients. The workshop proceedings were integrated into the Final Report.



Roundtable participants: From left: Phillip Verroco, JAPCC; Franck Schrottenloher, French Joint Space Command; Jakub Ryzenko, Space Research Centre in Poland; Alfred Vogel, National Defence Academy, Austria; Frank Müller, German SSA Centre; Neale Dewar, RAF; Sarah Tarry, NATO HQ; Amber Charlesworth, U.S. Department of State; Spyros Pagkratis, ESPI; Jana Robinson, ESPI; Pascal Legai, EUSC; Richard Buenneke, U.S. Department of State; Peter Hays, Eisenhower Center for Space and Defense Studies; Veronica Cody, EEAS; and Peter Hulsroj, Director of ESPI





A roundtable session



A.2 Agenda of the Roundtable on Space Crisis Management Organised by ESPI

ABOUT ESPI


The European Space Policy Institute (ESPI), situated in Vienna, Austria, was established in November 2003, pursuant to a decision by the European Space Agency (ESA) Council. ESPI's fundamental mission is to provide decision-makers with informed, cutting-edge views on mid- to long-term issues relevant to Europe's space activities. It also seeks to enrich the global debate on challenging space-related issues. In this context, ESPI acts as an independent platform for developing studied positions and advancing agreed strategies. ESPI offers a number of research products, including Reports, Perspectives, two book series (i.e. Yearbook on Space Policy and Studies in Space Policy), Position Papers and Memoranda. ESPI is also a hub for researchers in the field of space policy, largely through its European Space Policy Research and Academic Network (ESPRAN). It supports the Presidency of the European Interparliamentary Space Conference (EISC) and manages the Ambassador Platform for the Central and Eastern European Region in the Integrated Applications Promotion (IAP) Programme.

ROUNDTABLE MEETING
29th MARCH 2012
08.30 – 16.00
European Space Policy Institute (ESPI),
Schwarzenbergplatz 6, A-1030 Vienna


Space Crisis Management:
Filling the Gaps

organized by




ESPI

European Space Policy Institute



Palais Fanto
 Schwarzenbergplatz 6
 (Entrance: Zaunergasse 1-3)
 A-1030 Vienna, Austria
 Tel +43 1 718 1118 -0 / Fax -99
 E-mail: office@espi.or.at
www.espi.or.at

Photo credit: AGI, Boeing, ESA, NASA, Celestrak and Fraunhofer FHR.





Overview
The accelerating global dependency on space assets has revealed some weaknesses in the ability of the international space community to manage space emergencies or "incidents". The Roundtable will focus on those prospective crises that involve space-based assets. Effective space crisis management necessitates, among other factors, understanding the origin of the crisis, the assets involved, the scope of the crisis, and the global geopolitical backdrop. Space crisis management also involves detailed operational dimensions.

The overarching objective of space crisis management is to avoid disruptive incidents or conflicts in space. Accordingly, the Roundtable participants will discuss various modalities of space crisis prevention and management. Space crisis prevention often involves the preemptive expenditure of political and diplomatic capital and taking proactive steps to address emerging problems before they mature. It also requires a careful assessment of the intentions, credibility and capabilities of the various space actors. In this connection, available tools include transparency and confidence-building measures (TCBMs), a behavioural Code of Conduct, Space Situational Awareness (SSA), and deterrence options. Concerning the latter, deterrence theory has traditionally focused on terrestrial nuclear or conventional conflicts. Accordingly, its role for space-related activities remains somewhat clouded due to far fewer precedents.

Space crisis management also comes into play after a space "event" has already occurred. Defence measures, drawing on actual counterspace capabilities (i.e. those that can disrupt or destroy, an adversary's space assets), need to be looked to if preemptive efforts should fail. This Roundtable will seek to blend prevention and defence as both are essential tools for effective space crisis management. It will also explore realistic contingencies and scenarios that could trigger space crisis management responses.

Programme

8:30 Registration and Coffee

9:00 Welcome Remarks
Peter Hulsroj, Director, ESPI

9:15 Space Crisis Prevention
Moderator: **Jana Robinson**, Resident Fellow, ESPI

- Challenges of a congested, contested and competitive space environment
- Potential crises stemming from threats to space assets
- Interface of the space and terrestrial environments
- Modalities of deterrence for space
- The status of international norms for space
- Options for improving SSA to facilitate crisis prevention and management

11:15 Coffee Break

11:30 Space Crisis Management
Moderator: **Richard Buenneke**, Senior Adviser, Space Policy, U.S. Department of State

- Labelling a crisis (issue of attribution)
- Contingency planning
- Response options
- Involvement of commercial entities
- Strategic value of collaborative diplomatic and military actions
- Institutional and operational mechanisms to react in a timely manner

13:30 Lunch

14:30 Crisis Management Scenario(s) Discussion
Moderator: **Peter Hays**, Associate Director, the Eisenhower Center for Space and Defense Studies of the USAF Academy

16:00 End of Roundtable

Roundtable is held under the Chatham House rule of non-attribution and participation is by invitation only.

List of confirmed participants

Richard H. Buenneke, Senior Adviser, Space Policy, U.S. Department of State

Amber Charlesworth, Foreign Affairs Officer, Office of Space and Advanced Technology, U.S. Department of State

Veronica Cody, Head of Division for Concepts, Civilian capabilities, Training, Exercises and Lessons, Crisis Management Planning Directorate (CMPD), European External Action Service (EEAS)

Neale Dewar, Group Captain MA RAF, HQ 1 Gp Space Control & Battlespace Management, United Kingdom

Peter Hays, Associate Director, the Eisenhower Center for Space and Defense Studies of the USAF Academy

Peter Hulsroj, Director, ESPI

Jean-Luc Lefebvre, Program Manager, New strategic concepts, Institute for strategic research of "Ecole Militaire" (IRSEM)

Pascal Legal, Deputy Director, European Union Satellite Centre (EUSC)

Frank Mueller, Director, Space Weather Cell, German Space Situational Awareness Centre (GSSAC)

Spyros Pagkratis, Resident Fellow, ESPI

Jana Robinson, Resident Fellow, ESPI

Jakub Ryzenko, Head, Crisis Information Centre, Space Research Centre, Poland

Franck Schrottenloher, Chief of Space Environment Mastery Office, French Joint Space Command

Shawn Steene, Deputy Director for Space Policy & Strategy Development, Office of the Undersecretary of Defense for Policy, U.S.

Sarah Tarry, Action Officer, Defence Policy and Partnership Section, NATO HQ

Phillip Verroco, Air and Space Strategist, NATO Joint Air Power Competence Centre (JAPCC)

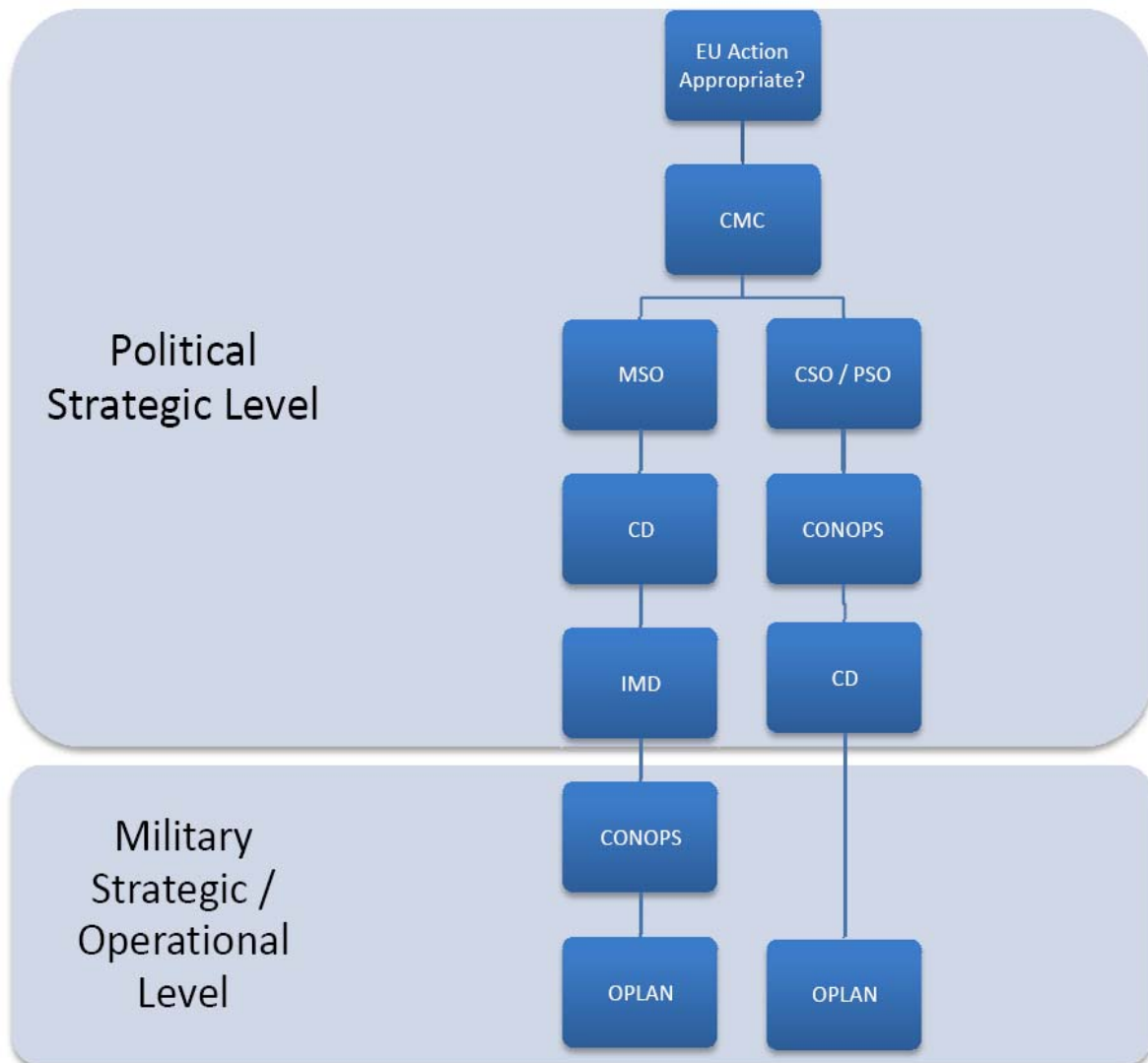
Alfred Vogel, Secretary-General, National Defence Academy, Austria



European Space Policy Institute



A.3 CSDP Mission Planning Process



Abbreviations:

CMC Crisis Management Concept
MSO Military Strategic Options
CSO Civilian Strategic Options
PSO Police Strategic Options

CD Council Decision
IMD Initiating Military Directive
CONOPS Concept of Operations
OPLAN Operation Plan

Source: Mattelaer A., (2010) "The CSDP Mission Planning Process of the European Union: Innovations and Shortfalls", European Integration online Papers, Vol. 14: Art. 9. Resource document. <http://eiop.or.at/eiop/index.php/eiop/article/view/2010_009a>

Acknowledgements

The author is grateful to the distinguished space experts from governmental and non-governmental entities, who provided valuable insights, particularly during the course of the workshop on "Space Crisis Management: Filling the Gaps" organised by ESPI on 29 March 2012. Key participants included: Richard Buenneke, Senior Adviser, Space Policy, U.S. Department of State; Veronica Cody, Head of Division for Concepts, Civilian Capabilities, Training, Exercises and Lessons, Crisis Management Planning Directorate (CMPD), European External Action Service (EEAS); Neale Dewar, Group Captain MA RAF, HQ 1 Gp Space Control & Battlespace Management, United Kingdom; Peter Hays, Associate Director, the Eisenhower Center for Space and Defense Studies of the USAF Academy; Jean-Luc Lefebvre, Program Manager, New Strategic Concepts, Institute for Strategic Research of "École Militaire" (IRSEM); Pascal Legai, Deputy Director, European Union Satellite Centre (EUSC);

Frank Mueller, Director, Space Weather Cell, German Space Situational Awareness Centre (GSSAC); Jakub Ryzenko, Head, Crisis Information Centre, Space Research Centre, Poland; Franck Schrottenloher, Chief of Space Environment Mastery Office, French Joint Space Command; Shawn Steene, Deputy Director for Space Policy & Strategy Development, Office of the Undersecretary of Defense for Policy, U.S.; Sarah Tarry, Action Officer, Defence Policy and Partnership Section, NATO HQ; Phillip Verroco, former Air and Space Strategist, NATO Joint Air Power Competence Centre (JAPCC); and Alfred Vogel, Secretary-General, National Defence Academy, Austria. Sincere thanks is also extended to Marco Aliberti, ESPI Research Intern, for his valuable assistance and contributions that proved most helpful to the completion of the report. Finally, the author wishes to acknowledge ESPI's Director, Peter Hulsroj, whose fine hand helped improve the quality of this report.

About the Author

Jana Robinson has been Resident Fellow at the European Space Policy Institute (ESPI) since December 2009. Ms. Robinson leads the Institute's Space Security Research Programme. She has published a number of articles on space security and sustainability in various journals. Prior to joining ESPI, she served as Development Director for the Prague Security Studies Institute (PSSI) from 2005–2009, a leading, Prague-based, non-profit public policy organization focused on security policy and studies. She was likewise responsible for the corporate establishment of PSSI Washington, a non-profit organization in Washington D.C., closely affiliated with PSSI Prague. Previously, she held positions

consistent with her academic background in Asian Studies. She holds an MA in Asian Studies from George Washington University's Elliott School of International Affairs, in Washington DC, specializing in Asia-Pacific security issues and space policy, and an MA in Asian Studies from Palacky University, Olomouc, Czech Republic. She received scholarships to attend the International Space University (ISU) 2009 Space Studies Program (SSP09), the 2008 Summer Mandarin Training Course at the Mandarin Training Center of the National Taiwan Normal University in Taipei, and Shanghai University in 1999–2000.

Mission Statement of ESPI

The European Space Policy Institute (ESPI) provides decision-makers with an informed view on mid- to long-term issues relevant to Europe's space activities. In this context, ESPI acts as an independent platform for developing positions and strategies.

www.espi.or.at