EUROPEAN PARLIAMENT

DIRECTORATE GENERAL EXTERNAL POLICIES OF THE UNION

BRIEFING PAPER

Policy Department External Policies

SOFTWARE DEFINED RADIO

SECURITY AND DEFENCE

October 2007

EN

This briefing paper was requested by the European Parliament's Subcommittee on Security and Defence.

This briefing paper is published in English.

Author: **Dr Stephen Pullinger**, Executive Director of ISIS Europe
Briefing paper carried out within the framework agreement between **ISIS Europe** and the European Parliament
EP/EXPO/B/SEDE/FWC/2006-10/Lot4/03

Responsible Official: **Dr Gerrard Quille**
Directorate-General for External Policies of the Union
Policy Department
BD4 06M081
rue Wiertz
B-1047 Brussels
E-mail: gerrard.quille@europarl.europa.eu

Publisher European Parliament

Manuscript completed on 2 October 2007.

The briefing paper is available on the Internet at
http://www.europarl.europa.eu/activities/expert/eStudies.do?languageEN

If you are unable to download the information you require, please request a paper copy
by e-mail : xp-poldep@europarl.europa.eu

Brussels: European Parliament, 2007.

Any opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

Contents

Page

1. Introduction **1**

2. What is Software Defined Radio and why is it different? **1**

2.1 What is radio? 1
2.2 Existing problems 1
2.3 What is Software Defined Radio (SDR)? 2
2.4 Why is this useful? 2

3. How does it relate to security? **3**

4. What is being done by EDA, Commission and Member States? **4**

4.1 WINTSEC (Wireless INTeropreability for SECurity) 5
4.2 EDA Study - SCORED 5
4.3 ESSOR Study 6
4.4 Complementarity 6
4.5 Member States 7
4.6 Bowman and tactical radios 7

5. What are the technical challenges? **8**

5.1 Developing a business model 8
5.2 Encryption and security 8

6. Strategic importance for commercial and security reasons **9**

7. Recommendations to the EP **10**

Appendix I – EU SDR Initiative 11

Executive Summary

A software-defined radio (SDR) is one that has the capability – through use of programmable hardware (handsets) controlled by software - to tune to any frequency band and receive any modulation across a large frequency spectrum.

At present, certain radio frequencies have to be reserved for particular functions e.g. the emergency services. But the proliferation of such reserved frequencies is beginning to crowd out the airwaves i.e. to create a shortage of bandwidth. SDR, however, should be able to overcome these problems through being able to achieve what is referred to as ‘cognitive spectrum management’, whereby it would be able to identify spare bandwidth flexibly on a case-by-case basis. This sharing of the spectrum that SDR allows is a very important capability.

The security applications of SDR technology cut across military and civilian spheres, covering issues related to homeland security as well as to crisis management missions overseas (most of which involve both military and civilian components). Military and other civilian first responders have mostly the same demands, so they can be supplied with the same technology. SDR is relevant not only to CFSP and ESDP, therefore, but also to third pillar issues under Justice Liberty and Security (JLS), including to any putative Homeland (internal) Security Strategy.

At European Union level, the European Commission (EC) and European Defence Agency (EDA) are working closely together (as far as pillar demarcations permit) to identify those dual-use technologies and capabilities that offer the greatest potential for both military and civil application. The two organizations have taken the effort to align their research projects, the purpose of which is to develop an SDR architecture that can be used both by the military for high-security encrypted communications or downgraded for low-security use by emergency first-responders. Hence, the EC and EDA are cooperating closely on the elaboration of the technical specification in their specific areas of competence (i.e. military security for EDA and civil security for EC) such as to assure consistency and complementary between the respective projects. Several EU Member States also now have national SDR programmes in place

Not only will SDR have profound implications for defence and security actors and policy, it will also have significant commercial potential. The US is leading the technological development, with China not far behind. It is critical that the EU exploits the commercial opportunities and is not left behind. Rather than allow the US to exploit SDR technology and strike a series of bilateral deals with individual European countries, the EU should seek to compete as an equal partner able to develop its own secure system for European requirements.

The EU should aim to be as open as possible and to apply a common European SDR standard. This standard should be shared to the maximum extent by all domains (military, security, civilian) to enable interoperability in ESDP operations.

The European Parliament has an important role to play in ensuring that the EU provides the levels of investment necessary properly to develop and exploit this technology: thereby saving lives, increasing the efficiency of ESDP and JLS operations and bringing significant financial and economic rewards.

Software Defined Radio

1. Introduction

This study will start by explaining the technology involved in software defined radio (SDR), current trends in its development and exploitation, and examine its potential application for both civilian security (such as the emergency services) and military security (battlefield communications). It will make an assessment of the current WINTSEC, EDA and ESSOR projects, and how these are inter-related. It then explores some of the technical challenges that lay ahead before considering the strategic importance of SDR for commercial and security purposes. The study concludes with some initial recommendations to the European Parliament.

2. What is Software Defined Radio and why is it different?

2.1 What is radio?

Radio is a means of communicating without wires (hence it is sometimes referred to as 'wireless'). Instead, it relies on the transmission of electromagnetic waves through space. Hence, its advantage is the independence of the receiver's location from that of the source. In order to achieve assured mobility of communication between senders and receivers, numerous radio stations are needed in order to provide full network coverage.

Particular networks can be deployed to facilitate communications between specific – a restricted group - of receivers: for example, to enable communication between police vehicles. Hence, a wide variety of different types of radio links are in use, deploying different operating frequencies, modulation techniques, and information coding formats or protocols. Types of radio include televisions, which turn the signals they receive into moving pictures and sound, cell phones, cordless phones, garage door openers, car door openers, pagers, radar, and so on.

2.2 Existing problems

Commercial wireless network standards are continuously evolving from second generation (2G) to 2.5G/3G and now further onto 4G (this is similar to the evolution in relation to an increase in computer capacity). This rapid evolution also brings problems, however. The most acute of which is that because each generation of networks differs significantly from the previous one regarding 'air-interface', subscribers are obliged to buy new radio handsets whenever a new generation of network standards is deployed. By the same token, wireless network operators are confronted with a large number of subscribers using old handsets that may be incompatible with their new network.

Moreover, because the air interface differs across different geographical areas, the deployment of global roaming facilities has been problematic. This proves very inconvenient to subscribers when they move across these boundaries. The alternative, which involves trying to build handsets capable of coping with different protocols, is a real problem too: the costs are prohibitive and the handsets too cumbersome.

2.3 What is Software Defined Radio (SDR)?

A software-defined radio (SDR) is one that has the capability – through use of programmable hardware (handsets) controlled by software - to tune to any frequency band and receive any modulation across a large frequency spectrum[1]. The hardware is able to identify the software with which it is being asked to interface and then to perform multiple tasks at the same time – in a similar way to a mobile telephone being able to act as a Global Positioning System (GPS), telephone and text sender simultaneously. In other words, it can receive and transmit a new form of radio protocol just by running new software.

In other words, an SDR can reconfigure itself appropriately for its environment and can be quickly and easily upgraded over-the-air. SDRs can talk and listen to multiple channels at the same. The obvious advantage here is that the system can be changed by bringing in new application software without any change, replacement, or modification of handsets.

This evolution in technology is leading towards the development of 'Cognitive Radio' (perhaps by 2015-2020). Such a radio would be able to look at the utilization of the radio frequency (RF) spectrum in its immediate neighbourhood and work out for itself how to communicate with the message sender for best performance[2].

2.4 Why is this useful?

At present, certain radio frequencies have to be reserved for particular functions e.g. the emergency services. But the proliferation of such reserved frequencies is beginning to crowd out the airwaves i.e. to create a shortage of bandwidth. SDR, however, should be able to overcome these problems through being able to achieve what is referred to as 'cognitive spectrum management', whereby they would be able to identify spare bandwidth flexibly on a case-by-case basis[3]. This sharing of the spectrum that SDR allows is a very important capability for which both the military and civilian worlds would benefit.

It will be possible, through software, to programme handheld SDR radios to reconfigure the characteristics of virtually any communications equipment. In other words, a wireless handset would be able to operate on different frequency bands, providing users with interoperable radios. This ability of SDR equipment to switch frequencies and transmission standards would overcome the lack of interoperability experienced with current different (mobile) radio systems. Nor would there any longer be a need to attribute bandwidth to a specified user community.

[1] Perhaps the best source of up to date information about SDR can be found at the SDR Forum - an international industry association of over 100 organizations committed to enabling the wireless Internet and advanced capabilities for civil and military systems. Its website is at: https://www.sdrforum.org/index.asp

[2] Johnny Keggler, ' Radio Families on the Tactical Scene', at: http://www.armada.ch/01-5/006full.htm

[3] Patrick Chatard-Moulin, Project Officer 'Software-defined Radio', European Defence Agency, addressing the Working group on Economic Aspects of a Common European Defence Policy (Kangaroo Group), minutes of the meeting of Wednesday 22 November 2006.

3. How does it relate to security?

The security applications of SDR technology cut across military and civilian spheres, covering issues related to homeland security as well as to crisis management missions overseas (most of which involve both military and civilian components). Military and other civilian first responders have mostly the same demands, so they can be supplied with the same technology. SDR is relevant not only to the EU's Common Foreign and Security Policy (CFSP) and European Security and Defence Policy (ESDP), therefore, but also to third pillar issues under Justice Liberty and Security (JLS), including to any putative Homeland (internal) Security Strategy.

Currently, the inability of different actors involved on the same mission to communicate with each other poses serious problems. Clearly, it is inefficient if troops from different national forces are unable to communicate with each other in the theatre of operations, just as it is if ambulance, fire and police services cannot talk to one another when tackling a civil emergency. The third dimension, crucial in so many contemporary crisis management operations, is to achieve communication interoperability between military and civil actors. SDRs are able to satisfy the needs of the military and cell phone services to be able to serve a wide variety of changing radio protocols in real time. They also offer the prospect of enhanced quality and scope of transmission and reception.

Clearly, the existing situation is far from ideal. For example, the British security services apparently lost communication, and therefore immediate operational control, when pursuing terrorist suspect John Charles Menenez onto the London underground in 2005. This pursuit, a few days after the 7 July bombings, resulted in an innocent man being shot dead. In the immediate aftermath of the bombings themselves, a lack of a digital radio network meant that many senior managers among the main emergency services, and the London Ambulance Service in particular, were forced to rely on using already overloaded mobile phone networks to communicate[4]. The director of operations at the London Ambulance Service, Martin Flaherty, acknowledged that the service had become too reliant on mobile phone technology, which clearly could not be relied upon in a complex major incident[5]. Similarly, the World Trade Centre and Oklahoma City terrorist attacks, saw local police unable to communicate directly with the fire department, which itself could not talk directly to ambulance crews.

This has led most radio manufacturers to conclude that the next big market will be the public safety sector, particularly among first responders, such as fire, ambulance, and law enforcement organizations that historically could only communicate within their own agency. Public safety organizations themselves are now examining the SDR requirements necessary to support first-responders to routine incidents and natural disasters.

[4] Andy McCue, Communication failures hampered London bombing rescues, CNET news.com, 5 June 2006
[5] Ibid.

Nor have the latest (non-SDR) battlefield communication systems found it easy to overcome technological challenges. The Bowman system that has recently been deployed by the British Army - late and over budget – has experienced many problems[6].

For the military, this technology needs to provide a capability to achieve interoperability within international coalitions that enables the forces of different European countries and other allies to communicate with one another. It also has to be able to guarantee that the security of this information was assured within a combat environment (see Section 5 for analysis of encryption challenges). Achieving such interoperability is a crucial requirement for multinational ESDP operations[7].

By bringing together computing and communications technologies SDR could eventually allow military radio systems to securely deliver voice, data and video in a variety of different formats. Beyond simple communication, an SDR could also be used, for example, to jam mobile phones that were being used to trigger explosives (a practice that was deployed by the unsuccessful terrorist attack in Glasgow in July this year).

4. What is being done by EDA, Commission and Member States?

At European Union level, the European Commission (EC) and European Defence Agency (EDA) are working closely together (as far as pillar demarcations permit) to identify those dual-use technologies and capabilities that offer the greatest potential for both military and civil application. The two organizations have taken the effort to align their research projects, the purpose of which is to develop an SDR architecture that can be used both by the military for high-security encrypted communications or downgraded for low-security use by emergency first-responders. Hence, the EC and EDA are cooperating closely on the elaboration of the technical specification in their specific areas of competence (i.e. military security for EDA and civil security for EC) such as to assure consistency and complementary between the respective projects.

When it established a project team on SDR the EDA set it the task of pursuing the “possibilities for pooling efforts and resources of interested Member States, and to investigate the need for and feasibility of a European capability to establish architectures and certify systems”[8]. The EDA subsequently requested this group to “test the viability of a collective European approach to developing next-generation SDR as a joint civil/military endeavour”[9].

The European Union is now pursuing three SDR studies:

[6] See National Audit Office Report, Delivering digital tactical communications through the Bowman CIP programme, Report by the Comptroller and Auditor General, HC 1050 2005-2006, 25 July 2006, http://www.nao.org.uk/pn/05-06/05061050.htm

[7] EDA Press Release, 21/11/2005, at: ue.eu.int/ueDocs/cms_Data/docs/pressData/en/declarations/87057.pdf

[8] EDA Steering Board decision 21 June 2005, www.eda.eu.int

[9] EDA Steering Board decision 21 November 2005, www.eda.eu.int

4.1 WINTSEC (Wireless INTeropreability for SECurity)

DG Enterprise and Industry is funding a two-year study (start 2007) – called Wireless Interoperability for Security or WINTSEC – to examine the security aspects of deploying SDR, specifically as it relates to activities under JLS. The project is funded under Preparatory Activity for Security Research (PASR), which has a particular focus on the development of a European security research agenda to bridge the gap between civil research and national and intergovernmental security research initiatives. WINTSEC, led by Thales Communications, involves over 20 organizations from 12 countries and has a budget of €3.68m[10].

The project will promote solutions that pave the way for further standardisation and refinement. It includes the support of a 'User Group', involving emergency and security end-users from six EU Member States. It will seek to address the realities of daily operations, along with complex interventions at national or multinational level. WINTSEC intends to explore a mix of complementary solutions to overcome the barriers for wireless interoperability across different security agencies[11].

Security Research is also an integral part of FP7 with a total budget of about €1.35 billion. A number of proposals are believed to have been submitted in this area, the results of the evaluation and funding recommendations can be expected in September this year, and it is strongly anticipated that this project will be developed further[12].

4.2 EDA Study - SCORED

In a complementary move, in 2007 the EDA itself has also embarked on a two-year, €1.75m study to support a long-term collective European approach to develop the next generation of interoperable SDR as a joint civil/military endeavour.

The study has two main parts, focusing on medium- and long-term objectives respectively. In the medium term the study, which seeks to complement the WINTSEC project, focuses on the military-specific technical capabilities of future SDR networks, secure system architecture, waveform development and distribution and technology building blocks.

The long-term part of the study concentrates on the future evolution of SDR and the application of Cognitive Radio-based Spectrum Management (CRSM) to meet the requirements of future Flexible Spectrum Management regulatory environments. Hence, the project is called SCORED (Military SDR Capabilities Including Applying CRSM to the Security and Defence Domains).

[10] The project partners are: Etherstack (Fr), Sagem (Fr), University of Surrey (UK), EADS Secure Networks (Fr), Elektrobit Ltd (Fi), Ericsson (Se), Rohde and Schwarz (De), Universität Karlsruhe (De), Selex Communications (It), Accrde (ES), Indra Sitemass S.A. (Es), Skysoft Portugal (Pt), Radmor S.A. (Pl), Intracom Defense Electronics (Gr), TNO (NL), Prismtech (UK), FOI (Se), JRC Joint Research Centre / IPSC – ISPRA (EU), GMV (Es), Amper Programa (Es), FEE CTU (Cz)

[11] http://www.ec.europa.eu/enterprise/security/doc/project_flyers_2007/WINTSEC.pdf.

[12] Private conversation between the author and an informed official source.

4.3 ESSOR Study

In addition, France, Italy, Spain, Finland, Poland and Sweden have proposed a €100+m, four year project – called European Secured Software Defined Radio (ESSOR) – which aims to improve interoperability between national military communication systems in Europe (and with the US).

Under the auspices of the EDA, the ESSOR study will address the following main objectives in order to give European industry the capability to develop interoperable SDR in the period from 2010 to 2015. These include:

- Contributing to the development of the European DTIB (Defence Technological and Industrial Base) in SDR through the establishment - in keeping with the US - of the normative referential required for the development and production of military SDR in Europe;
- Addressing military-related challenges;
- Complementing Commission and EDA activities in support of a coordinated European approach to SDR;
- Promoting a common defence position in SDR;
- Supporting the management of interoperability with the US and NATO.

Details of the launch of ESSOR are currently under discussion between the six contributing member states, with the intention to sign the contract before the end of the year[13].

4.4 Complementarity

The EDA will coordinate its study on longer-term military specifications and the medium-term ESSOR Project to ensure that both are complementary to the civil technology work to be carried out by the European Commission. The EDA receives relevant information from WINTSEC via designated points of contact within the industry consortium. It also holds regular meetings with Commission representatives to exchange information.

According to Javier Solana, who chaired the EDA Steering Board meeting of Defence Ministers in November 2006 (a meeting also attended by G. Verheugen, the Vice-president of the Commission and Commissioner for Enterprise and Industry):

"This is an excellent example of how we can maximize the return from our investments thanks to governments, the EDA and the [European] Commission working closely together." [14]

[13] Ibid.

[14] Javier Solana, EU Defence Ministers Club Together to Research Better Protection for Armed Forces, *EDA Press Release*, 13 November 2006.

4.5 Member States

Several EU Member States now have national SDR programmes in place, including:

- Finland, where an SDR and adaptive antenna demonstrators are being developed for the Finnish Defence Ministry based on Spectrum Signal Processing's SDR-3000 system (also being examined by Korea and Japan).
- Sweden, where the Defence Ministry is pursuing a SDR Tactical Data Radio.
- France, where the Multi-Band, Multi-Mode Radio Demonstrator has proved the feasibility of SDR, and a Poste Radio Programmable (PR2) is being developed to replace older systems.
- Spain has its own programme – TERSO.
- Italy has developed its own SDR demonstrator.

4.6 Bowman and tactical radios

The most important system (from a coalition warfare perspective), the British *Bowman* tactical communication system, is a hardware-defined radio that uses conventional single-channel technology. But there has been no coordinated effort to ensure interoperability with European partners. Indeed, one of the original key capabilities of Bowman that has been dropped is the ability to communicate data directly with allies' systems, which was aimed at reducing the risk of 'friendly fire' incidents on the battlefield[15].

Under the terms of the US/UK Joint Tactical Radio System (JTRS)/*Bowman* Interoperability Initiative, Britain is required to release to the US the *Bowman* waveforms and encryption engine, thereby allowing the US to develop software to emulate the *Bowman* system.

Given that *Bowman* is a hardware-defined radio, there really was no other viable solution, but it did have the virtue (from an export control standpoint) of protecting US SDR technology and the JTRS encryption engine. Refusal to release those technologies has prevented the development of interoperability standards for European SDRs. Britain has voiced no opposition to an approach that amounts to a black box.

The operating principles of *Bowman* are so different from those of JTRS as to make a more collaborative solution impossible, while the cost of SDRs such as JTRS remains prohibitive for the British MoD. The acceptability of black box solutions thus depends entirely on how badly the Europeans want a particular capability, and whether they think it is economically feasible to bypass the US to develop it themselves[16]. It also depends whether the Europeans want to be so dependent on US technologies. The UK has invested heavily in a technology that may soon be overtaken by SDRs that are more flexible and that allow greater independence.

[15] Andy McCue, '£2.4bn battlefield radios slammed by MPs', Silicon.com, 8 March 2007, at: http://www.silicon.com/publicsector/0,3800010403,39166246,00.htm

[16] Jeffrey P. Bialos and Stuart L. Koehl, 'The NATO Response Force Facilitating Coalition Warfare through Technology Transfer and Information Sharing', Report of a study conducted by the Center for Transatlantic Relations and Funded by the Center for Technology and National Security Policy Center for Technology and National Security Policy National Defense University September 2005.

5. What are the technical challenges?

5.1 Developing a business model

In terms of a business model, it will be important to be able to sell the software and the radio hardware for the market to develop. The EDA will ask industry to propose solutions on that topic. Issues to be considered will include:

- Consistency and convergence between different SDR certification initiatives
- What do we need to standardize?
- Articulation with US certification (JTEL)
- Optimized European certification capability
- Organisational approach (Commission, EDA, particular Member States)

Today's wireless networks are attracting a new type of hacker. We have already witnessed cyber attacks on a number of sensitive websites – such as that of the US Pentagon - and other volatile communication and data storage media. The downloadable waveform in SDR is an obvious next target. As the Swiss company Crypto warns,

"…people need to understand that wireless networks are completely insecure. Will the answer be found out in the heat of the battle… when it's too late?" [17].

5.2 Encryption and security

As is customary, issues related to security (communication security, information security, transmission security) are very difficult to handle in the multilateral international environment, and SDR is no exception. Indeed, quite the contrary. SDR-based equipment is meant to be able to operate in many different configurations depending on the specific requirements of different types of operation and even of different users. This, in turn, presents different security requirements. There are two areas for particular caution.

First, in respect of the ways that security functions would be implemented technically. It would be necessary to define system architectures that enable operation-specific or country-specific security modules to be "plugged" in, the internal implementation of which need not be revealed to any third parties[18].

The second area of caution is in respect of the political and procedural aspects related to certification and operation of SDR-based systems. It would be necessary to agree specific certification/accreditation procedures between the cooperating parties, not only at the stage of system development, production and compliance testing, but also during actual operations[19].

SDR security is addressed by the projects coordinated by the EC. It also receives particular attention within the defence community. Approaches that collectively include all EU member states, however, are rather difficult to manage. In mid-term, an approach that looks more

[17] Johnny Keggler, op. cit.

[18] Private conversation between the author and an informed official source.

[19] *Ibid.*

efficient (and, most of all, realistic) is based on multilateral *ad hoc* cooperation between a number of member states who agree to work together e.g. the ESSOR project. Within the SDR Project Team, EDA has also raised the question of a longer-term standardisation/certification strategy: it is still under discussion.

6. Strategic importance for commercial and security reasons

Not only will SDR have profound implications for defence and security actors and policy, it will also have significant commercial potential. The US is leading the technological development, with China not far behind. It is critical that the EU exploits the commercial opportunities and is not left behind.

The Global System for Mobile Communications (GSM) was a technology that originated in Europe but was exploited by the US. First introduced in 1991, by the end of 1997 a GSM service was available in more than 100 countries and has become the *de facto* standard in Europe and Asia. The commitment to, and endorsement of, open and global standards has always been key to European success in wireless communication. This approach is also relevant in relation to SDR.

The US is moving toward SDR, such as the Joint Tactical Radio System (JTRS), while most European countries are still deploying single-band radios similar to the ones the US developed in the 1970s. Attempts to create a multinational Future Multi-band, Multi-waveform Modular Tactical Radio programme foundered over issues of cost and how one might control the release of SDR and encryption technology.

The major military equipment providers in the US have products that they tout as SDRs, and they are being encouraged by the Department of Defence's JTRS Programme Office to conform to common standards and to adopt the Software Communication Architecture as the operating system for their radios.

The US presently has a Memorandum of Understanding (MOU) in place with Japan for the development of SDR technology, and is in discussions with Australia, France, Germany, Italy, the Netherlands, South Korea, Singapore, Spain, and Turkey, but these discussions have not yet passed beyond the preliminary phases[20].

It should be noted that in the case of all three European programmes commercially developed dual-use technologies have been integrated into the respective systems, in some cases leapfrogging the US technical advantage. However, merely the development of an SDR will not ensure interoperability with US forces since each SDR would still use unique, proprietary waveforms and encryption methods.

While the software basis of the new radios would make interoperability updates easier from a hardware perspective, developing a common software set would take considerable time and a degree of cooperation not yet demonstrated by the US. Until standards and protocols are adopted

[20] Jeffrey P. Bialos and Stuart L. Koehl, op. cit.

for waveforms, frequency hopping, data formatting and encryption, even the deployment of SDRs by US allies will not ensure real interoperability.

Rather than allow the US to exploit SDR technology and strike a series of bilateral deals with individual European countries, the EU should seek to compete as an equal partner able to develop its own secure system for European requirements. Hence, it will be important to provide the necessary investments in research and development at EU level, thereby pulling together the combined skills and experience from amongst all Member States with relevant expertise. It is essential for strategic and commercial reasons that the EU retains its competitive position in the SDR market especially vis-à-vis the US and Asia.

In the near future, internet and internet protocol (IP)-technology will be used in commercial data networking as well as in secure and military networks. This may lead to a total convergence of different networks. In other words, there will no longer be separate civilian networks, military networks, public-safety networks etc. Instead, we will have a network of networks where the SDR can use different communication connections and their services seamlessly and securely.

7. Recommendations to the EP

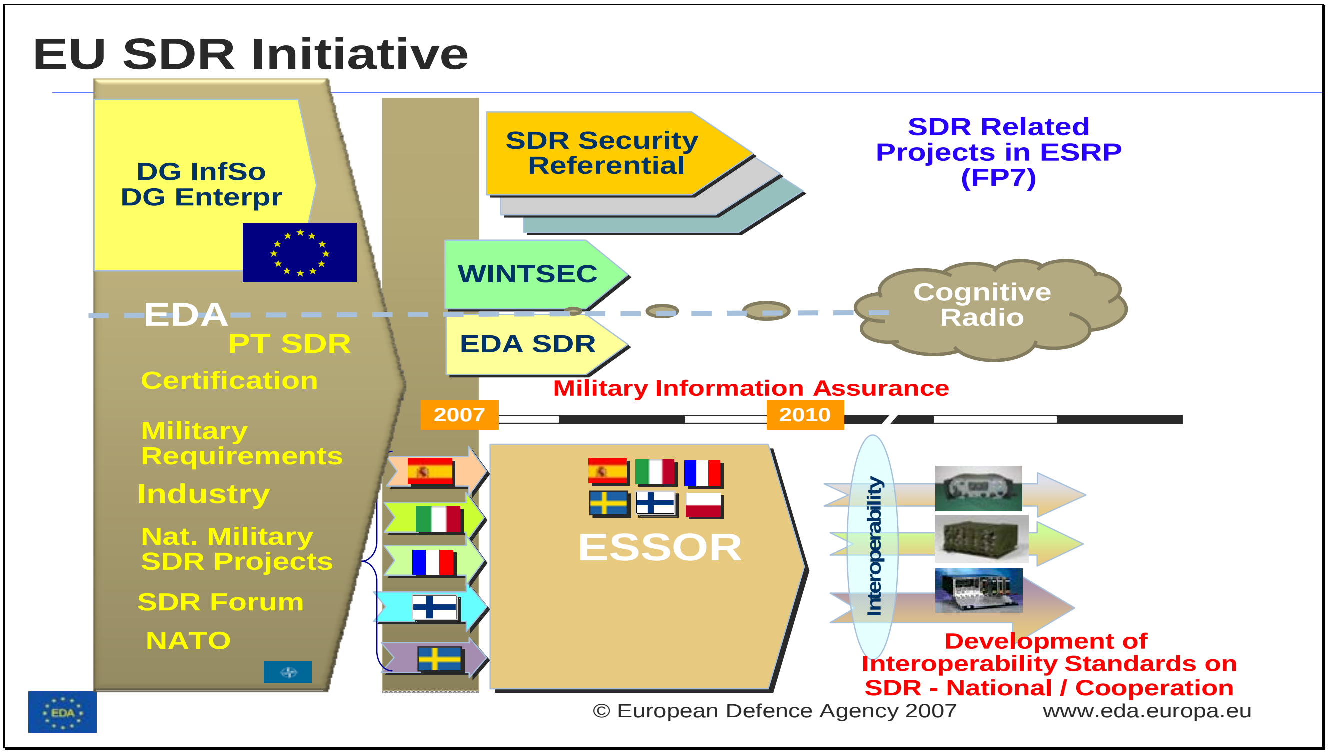
The EDA's work in trying to facilitate and develop a co-operative dialogue between civilian, security and military actors is crucial if Europe is to define and apply a common European SDR standard. Ideally, this standard should be shared to the maximum extent by all domains (military, security, civilian) to enable interoperability in ESDP operations.

As stated above, there are technical and political obstacles that need to be overcome if such a goal is to be achieved. Given the importance of establishing secure communication networks within any given operation, and that different nations are likely to be involved, the ability to define system architectures that enable operation-specific or country-specific security modules to be plugged in appear attractive. This is a technical challenge that will require further coordinated scientific research and investment. The Commission's funding of further relevant projects through FP7 should be given a high priority.

At the political level, the EU (and specifically the EDA) is faced with the perennial problem of ensuring a coherent integrated approach within a fragmented pillar system. Hence the EDA is attempting to straddle the Commission's civilian work with the military studies being conducted by the member states. Reaching agreement on specific certification procedures between cooperating member states could also prove tricky.

What is clear, however, is that SDR is a technology with enormous security-related and commercial potential. The European Parliament has an important role to play in ensuring that the EU provides the levels of investment necessary properly to develop and exploit this technology: thereby saving lives, increasing efficiency and bringing significant financial and economic rewards to the citizens of Europe.

Appendix I



EU SDR Initiative

DG InfSo
DG Enterpr

EDA

PT SDR

Certification

Military
Requirements

Industry

Nat. Military
SDR Projects

SDR Forum

NATO

SDR Security
Referential

SDR Related
Projects in ESRP
(FP7)

WINTSEC

Cognitive
Radio

EDA SDR

Military Information Assurance

2007

2010

ESSOR

Interoperability

Development of
Interoperability Standards on
SDR - National / Cooperation

© European Defence Agency 2007

www.eda.europa.eu