Armed Forces' views on Shared Spectrum Access

Topi Tuukkanen
Information Technology Division
Finnish Defence Research Agency
Riihimäki, Finland
topi.tuukkanen@mil.fi

Marja Matinmikko
University of Oulu
Oulu, Finland

Petri Ahokangas
University of Oulu
Oulu, Finland

Seppo Yrjölä
Nokia
Oulu, Finland

Miia Mustonen
VTT Technical Research Centre of Finland
Oulu, Finland

Abstract— **Recent transition from mobile telephony to daily consumption of mobile data presents the challenge of adequate spectrum availability. Besides regulators and operators, this challenge faces both public safety authorities and military as well. This paper investigates how selected spectrum sharing concepts (namely, European Licensed Shared Access (LSA) and US Citizens Broadband Service (CBRS)) support the military interests either as a Primary User (PU) or as a Secondary User (SU) and whether these concepts facilitate temporal adjustments of national defence from peace time mode of operations to hybrid warfare or to large scale homeland defence. In this paper we have shown that military spectrum needs vary from one scenario to another and that Shared Spectrum Access may support expected needs of spectrum in times of most dire stress. Both of the concepts reviewed have built in dynamism, which however does not support PU-SU role changes across tiers**.

Keywords—Armed Forces; Military, Shared Spectrum Access; Citizen Broadband Radio Service, Licensed Shared Access

I. INTRODUCTION

Rapid increases on mobile data communications as demonstrated by [1] has given rise to concerns regarding adequacy of available spectrum, challenging even existing spectrum allocations of governmental civilian and military authorities [2],[3]. The process to administer the use of limited radio spectrum for the benefit of society is captured under the notion of spectrum management. Overall global spectrum management has been arranged under the auspices of the International Telecommunications Union, a subordinate body of the United Nations. Global and regional spectrum assignments are documented within spectrum allocations maintained by the World Radio Conference (WRC) that seeks to harmonize the use of spectrum [4]. Based on that, national spectrum regulatory authorities allocate individual frequency bands to groups of users or to user organizations, normally by authorizing exclusive use, e.g., by auction.

Current spectrum management practices are static in administrative, temporal, geographical and frequency domains. Changes to allocations may take years to plan and implement. In military, the North Atlantic Treaty Organization (NATO) coordinates the use of spectrum for alliance purposes and supports national military spectrum management authorities in spectrum harmonization. Similarly, to civilian spectrum administrations NATO suffers from rigid planning and management processes [5].

Current spectrum management processes have evolved over time in support of the needs of the technological systems of the time. The elementary principle is that of avoiding and minimizing mutual interference between radio communication systems and for that purpose a number of approaches have been employed like protective guard bands, separation by geography or specifying features and normative values for modulation, transmission power or side-lobe characteristics. Many military systems are expected to adhere to such regulations even today [3].

Depicted rigid spectrum management has led to a situation where some frequency bands are utilized effectively where as some portions of spectrum remain under-utilized. With the advent of notions of Cognitive Radio and Dynamic Spectrum Access (DSA), the efficient use of the spectrum has emerged as one of the contemporary research topics, for example, employing spectrum occupancy measurements [6].

In this paper, we use the term Shared Spectrum Access to describe a situation where two or more systems of independent entities operate in the same frequency band in a specific geographic area on a non-exclusive basis in a defined sharing arrangement (cf. [7]). The use of administrative and technological approaches that enable Shared Spectrum Access have been proposed in literature, e.g., in [8] and [9], as a way to improve spectral use

This work has been partially supported by the Finnish Funding Agency for Innovation's CORE++ project in collaboration with Nokia, VTT Technical Research Centre of Finland and University of Oulu.

efficiency. Dynamic spectrum use is thus seen as one of the most important features of a potential new cognitive radio technology [10].

In order to understand the context of Shared Spectrum Access we need to recognise the term Cognitive Radio System as defined by International Telecommunications Union (ITU) as "*Cognitive radio system (CRS): A radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained.*" [11], [12], [13].

Whereas the term Cognitive Radio (CR) shall be used as a "node" as a singular element within the system instead of a "radio unit" or "radio device". According to [12], Cognitive Radio is a "*type of radio in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behaviour based on that information and predefined objectives*".

Furthermore, Dynamic Spectrum Access is defined in [10] as "*The real-time adjustment of spectrum utilization in response to changing circumstances and objectives*". Besides two categories of services (i.e. primary service vs. secondary service) current ITU regulation addresses exclusive (use) bands, shared bands and license-free bands. Reference [14] observes that "*future regulation and technology development will create a complex landscape of spectrum availability and authorization modes*". Thus it is foreseen that different regulatory schemes with various forms of spectrum sharing shall be developed over multiple frequency bands.

This paper investigates how do selected spectrum sharing concepts support the military interests either as a Primary User or as a Secondary user and do these concepts facilitate temporal adjustments of national defence from peace time mode of operations to hybrid warfare or to large scale homeland defence?

The rest of the paper is organized as follows. The introduction presents the notion of shared spectrum access within the framework of spectrum management. The second section describes the methodology applied. The third section shall present a high level temporal scope, scenarios, for the spectrum use by the armed forces. In the fourth section the most prominent spectrum sharing concepts, the Licensed Shared Access (LSA) in Europe and Citizen Broadband Radio Service (CBRS) in the US are introduced. The fifth section develops a potential set of use cases of primary and secondary users. The sixth section synthesizes our observations and proposes an option space within which armed forces can easily map specific use cases as well as a potential new research question of changing user roles dynamically. The final section summarizes the identified capability gap and proposes future research topics.

II. METHODOLOGY

The methodology, scenarios and use cases were developed through a series of multidisciplinary workshops of the CORE++ research project involving disciplines related to technology, business, policy and military. The overall methodology follows, in principle, the approach used for example in [15], whereby we shall establish scenarios as well as introduce major spectrum sharing concepts and use cases within the context relevant for our inquiry. These will be assessed to determine how they affect the potential use of

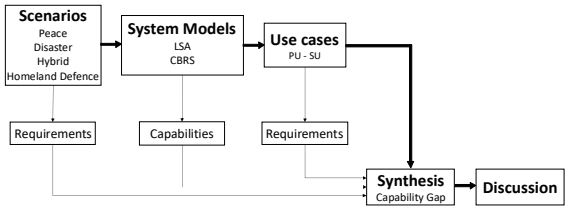

Fig. 1. Methodology used.

Outline of the methodology used is depicted in Fig.1. We shall present a conflict continuum including scenarios of peace time, large scale disaster, hybrid warfare and homeland defence. Furthermore, we shall address relevant system models based on the European LSA as well as the US concept of three-tier CBRS. Finally, drawing from [15] and [16] we develop a set of theoretical Primary User-Secondary User -use cases, of which those involving military are analysed in more detail. Our observations are synthesized into a capability gap.

III. USE OF SPECTRUM IN DIFFERENT MILITARY SCENARIOS

In general, the tasks, scope and roles of the armed forces vary greatly due to national geographical position, national strategic posture, or perceived threats, which altogether aggregated into a notion of worldview [17], influence the ways armed forces perceive Shared Spectrum Access. In this section we shall attempt to categorize the activity levels of the armed forces in national defence context in order to assess potential implications for the Shared Spectrum Access.

The reason for limiting our focus to national defence is that spectrum regulation is the responsibility of the national spectrum management authorities, in most cases a civilian government agency. For example, European Union Military Staff or NATO do not have mandate nor authority to participate to the formal decision making of the ITU's World Radio Conference, although they do attempt to harmonize military spectrum use through national military spectrum administrations. As Shared Spectrum Access is not yet current practice within national applications of military power, it shall take considerable time until Shared Spectrum Access will become routine in multinational military coalition operations.

Reference [18] presents a range of military operations in a conflict continuum from peace to war categorizing activities into

- Military engagement, security cooperation and deterrence
- Crisis response and limited contingency operations
- Major operations and campaign.

On the other hand, [19] presents a more challenging illustration of military activities in a mosaic of conflict. A more spectrum focused view is presented in [20] where a "Notional Joint Electromagnetic Spectrum Management Operations across the Phases of Operations" is depicted. Such phases are: shape, deter, seize, dominate, stabilize, enable. These references clearly demonstrate approaches applicable to major military powers but do not necessarily apply to smaller nations. Therefore, for the purposes of this paper we shall concentrate on the following generalized scenarios:

- **Peace time** including activities of territorial surveillance, maintaining readiness and training.
- **Large scale national accidents or a disaster** including assistance to civilian public safety authorities.
- **Hybrid warfare** meaning asymmetric and irregular enemy use of all elements of national power.
- **Homeland defence**, which is used here in a national defence context in a similar manner as [18] characterizes traditional warfare involving nation-states on force-on-force operations.

A. Peace time

In peace time, the national defence apparatus maintains its readiness and monitors territorial sovereignty. Maintaining readiness involves the maintenance of existing capabilities and acquisition of new or replacing capabilities. Although we do not here need to go through all military capability areas of Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, Interoperability [21], a few observations can be made.

Military hardware is expensive and is often specifically tailored to meet military requirements (inter alia hostile electronic warfare). Therefore, the lifecycles of military equipment are long, even decades, when compared to contemporary Commercial-Off-The-Self (COTS) mobile telephony devices [22]. Vacating frequencies this equipment use is therefore a time consuming and expensive exercise at minimum, in some cases due to propagation conditions, potentially impossible. The conclusion therefore is that, as regards the spectrum already assigned to military, the posture of the armed forces is bound to be that of the incumbent or Primary User. Whereas when new procurement or new acquisitions are considered, the posture of the Secondary User may become possible if clearly articulated beforehand.

The use of spectrum for the purposes of monitoring territorial integrity may in some cases be location dependent (border regions, high readiness air bases) and thus may allow some flexibility to consider new spectrum access approaches, e.g., with geographic restrictions.

In most armed forces the regular peace time manning levels remain significantly lower than what is being planned for an all-out war. Peace time forces regularly train and exercise in garrisons and regular exercise areas. Although large scale exercises can and will be organized, these seldom are of such scope that spectrum occupancy measurements could provide credible predictions to the true spectrum needs of the armed forces in times of war. Thus armed forces' spectrum needs are in peace time significantly lower than in times of crises and therefore traditional regulatory approaches, spectrum planning and spectrum access methods have sufficed, although this is rapidly becoming challenged [3].

B. Large scale national accidents or a disaster

The very nature of this scenario is that, regardless of national level of preparedness, these events do occur at times and locations unknown beforehand [23]. Response to such events is highly dynamic in organization and deployment of both military and public safety units and has a high demand for reliable communications that does not interfere participants yet facilitates inter-authority interoperability, coordination and cooperation [24]. In planning and preparations for such circumstances, the armed forces would be well advised to consider public safety authorities' role as a Primary User, at least on Ad Hoc-basis. This would present an administrative as well as technical challenge for the Shared Spectrum Access concept to facilitate authorized dynamic adjustments limited in time, geography and frequency domains that most probably would influence both network as well as end user devices and systems.

C. Hybrid Warfare

Hybrid Warfare is understood to consist of different modes of warfare including conventional capabilities, irregular tactics and formations as well as terrorism and criminal activities being conducted by both nation-states and non-state actors [25]. It is a mode of conflict that challenges the traditional notions of military thinking and warfare as it specifically targets strategic weaknesses of the democratic society in general as well as socio-cultural weaknesses of the target population.

The concept definition of "hybrid war" has, however, been contested in [26] due to a failure to capture the importance of non-violent actions in a conflict. Such non-violent action in terms of Shared Spectrum Access could be, just as an example, Primary User Emulation Attacks. Reference [26] observes that the term "Grey Zone" has emerged as a mode of conflict between traditional war and peace, yet remaining below the threshold of war. Although not as widely used as the term Hybrid War, Grey Zone captures in its essence the gap between peace time legal frameworks, jurisdictions, mandates or authorities and emergency or military powers many nations have in preparation for a large scale national homeland defence scenario. Despite the ongoing debate on the concept of hybrid war or grey zone, one aspect seems to be common: the challenge for the target to develop a consistent perception of the fact and character of the conflict taking place.

For our purposes we observe that traditional binary distinction between peace and war has led to a spectrum regulatory regime to adopt regulatory frameworks, in regard to the military use of spectrum, that are static, even rigid, in the assumption that such regulation may become overturned

in times of war by changes to war time powers and authorities. The concept of hybrid war/grey zone seriously challenges this notion.

In this type of scenario eruptions of violence can be expected even in urban populated areas, for example by the so called little green men or 'polite people' [27]. This would require the civilian public safety authorities to be able to operate within the contested area thus challenging attempts by the military to take over the spectrum used by Mobile Network Operators (MNO).

Overall, this scenario implies that a three-tier approach (covering alternating roles of military, public safety authorities and MNOs) to spectrum access would be beneficial but would need to be complemented by a facility to rapidly authorize and implement a change of one-tier users to another tier and vice versa.

D. Homeland Defense

Here we use the term Homeland Defence in a national defence context referring to traditional warfare involving nation-states and force-on-force operations. National armed forces are brought to full alert and reservists (i.e. National Guard) have been called up. Unless the scale and scope of hostilities is limited, for example aimed to initiate a so called "frozen conflict", there shall be challenges for the defender to attempt to limit hostilities into a front line. On the contrary, high mobility land operations directed into the depth of defender are more the norm.

Thereby civilian spectrum administration shall have major difficulties to geographically limit the needs of the armed forces to acquire more spectrum. Armed forces would also need to expand the (in peace time limited) operated frequency ranges to facilitate spectral manoeuvrability in order to counteract enemy electromagnetic warfare activities (inter alia to avoid interception or hostile jamming).

Many nations have plans or legislation for such circumstances to authorize military to take over, not only the lines of communication, but also to alter the use of assigned frequencies. In this kind of a scenario there is little or no incentive for armed forces to adopt the posture of Secondary User. Even if the changes in regulatory frameworks and authorities are implemented, and even if the equipment used would be able to efficiently use rapidly expanded allowed spectrum, a third challenge arises, namely that of internally generated mutual interference.

This phenomenon is rarely if ever encountered in peace time exercises (because of budgetary or treaty size restrictions), but one only has to imagine a major decisive land battle into which the defender musters a significant striking force to conduct a decisive counterattack. This variation of the scenario would bring attacking mobile (read dependent on wireless communications) military units and formations from different branches and even regional commands amidst into the defending formations. Since military is highly hierarchical by nature [28], it is reasonable to assume that defending and counterattacking units would either have completely separate frequency assignments rendering them mutually non-interoperable or they would have overlapping frequency assignments thus causing serious interference to each other. This would be an obvious business case for a Cognitive Radio and DSA.

IV. SPECTRUM SHARING CONCEPTS

Although Spectrum Sharing has been widely researched, also including concerns and views of the armed forces as shown in [3] and [8] among others, only a limited number of initiatives have eventually reached maturity to be incorporated as a policy or included in regulatory frameworks. Such concepts are for example wireless access systems operating in TV broadcast band [29], the LSA in Europe [30], and the CBRS in the US [31].

Reference [32] presents potential spectrum sharing options in two dimensions. First axis is a continuum between unlicensed, low Quality of Service and low cost to the other end of exclusive use/licensed –end, where Quality of Service can be guaranteed but at higher cost. The other dimension is between vertical sharing where actors, systems and technologies are disparate as compared to horizontal sharing where actors, systems and technologies are resemblant.

Drawing further from the [32], the [33] differentiates spectrum usage scenarios from regulatory frameworks. Identified three regulatory framework domains were Primary User Mode, Licensed Shared Access Mode and Unlicensed Mode. Furthermore, [33] presents five spectrum usage domains of: dedicated licensed spectrum (exclusive use), limited spectrum pooling (horizontal sharing), mutual renting (horizontal sharing), vertical sharing and unlicensed horizontal sharing.

Wireless Innovation Forum has in [34] and [35] broken spectrum sharing concepts, in a continuum, into five distinct levels ranging from exclusive use, static spectrum sharing, managed shared access, dynamic spectrum sharing, to pure spectrum sharing and unlicensed use of the spectrum.

For the purposes of this article we shall concentrate on the concepts of the European LSA (level 2A in [35]) and the US CBRS (level 3B). Both the LSA and the CBRS concepts are based on the premise to improve spectrum utilization efficiency. This is achieved by enabling additional users to have access to portions of the spectrum in time and space where incumbent user is not using that part of spectrum. These concepts and technologies remain under development as can be seen in [36] as well as [37] and [38] respectively.

A. Licensed Shared Access

In 2012 the European Commission (EC) communicated the view promoting spectrum sharing within wireless industry [39]. This was followed by development of the concept of LSA defined as a regulatory framework to allow a limited number of additional licensed users to have access to a frequency band assigned to the incumbent user, within the scope of sharing rules ensuring all authorized users retain specific Quality of Service [30].

The LSA concept is based on the notion that incumbent shares assigned spectrum with licensee in conformity with a

pre-negotiated sharing framework and sharing agreement. The intention is that this would guarantee both incumbent and licensee protection from harmful interference with predictable QoS. The Architecture of the LSA itself is comprised of two major elements to protect the incumbent as shown in Fig. 2.

LSA Repository (LR) stores entries of the information on the availability, protection requirements and the use of spectrum in addition to operating terms and rules. The LSA Controller (LC), intended to operate within the LSA Licensee's domain, manages the mobile networks access to the spectrum based on spectral availability information provided by the LSA Repository.

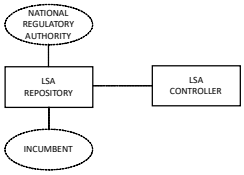

Fig. 2. LSA Architecture Model [39].

Within the LSA Concept the interaction and of a LR and a LC is essential. The concept allows for the existence of multiple incumbents, even changes to the LSA Sharing Framework are authorized. Furthermore, the concept supports scheduled or on-demand changes to the protection requirements of the incumbent [40]. In cases when LR-LC connectivity is lost, a number of fall-back measures the LC may initiate have been identified, but need to be further defined within the Sharing Arrangement between Incumbent and LSA Licensee. Therefore, the notion that the LSA Licensee vacates the spectrum resource must be properly addressed administratively beforehand [36].

The LSA system for 2.3-2.4 GHz band has been validated in field trials [41]. LSA concept's expansion to other frequency bands (700-800 MHz) is also under investigation [42]. The development of the concept to the 3.6-3.8 GHz band continues as demonstrated by [43]. In this band it is foreseen that the variations in the incumbent's use of the spectrum are less dynamic, therefore the concept is being expanded with the notion of guaranteeing LSA band availability for a certain time in the specified region. This is expected to support new innovative use cases.

B. Citizen Broadband Radio Service

In 2012 the [44] put forward a spectrum-sharing discussion in the US. Concurrently with the LSA policy deliberations in Europe, the CBRS concept started to gain interest in the US as an alternative spectrum management approach. Whilst standardization process continues within the Wireless Innovation Forum [38] the CBRS concept has adopted a three-tier authorization framework in in 3.55-3.70 GHz band bands albeit the framework itself could be expanded to other frequency bands too [38]. The three layers CBRS consists of are the Incumbent Access (IA) layer, the Priority Access (PA) layer and General Authority Access (GAA) layer.

Existing primary operations, including authorized federal users, are operating in the IA layer, whereby incumbents are protected from harmful interference of other CBRS users by exclusion zones and by a dynamic Spectrum Access System (SAS). Critical public safety, governmental user and utilities are foreseen to be operating within the PA-layer. These users may be granted a temporary authorization to operate within a specified area and are protected from harmful interference from the GAA layer. Residential Internet service providers and business may be entitled to use the spectrum on opportunistic license-by-rule regulatory basis without interference protection within the GAA layer.

The SAS, basically similar in function to the LSA Controller and LSA Repository, enforces all policies and procedures retrieved from the FCC Database. The incumbent user may inform the SAS of intended spectrum usage. The SAS determines and provides the Citizen Broadband Radio Service Devices (CBSD) with the permissible channels, frequencies and transmission power levels at their location, yet enforcing Exclusion and Protection Zones. The SAS assigns dynamically specific GAA channels to users. PA and GAA frequencies are dynamically determined and assigned at a specific location by the SAS that also controls the interference levels. Furthermore, the SAS controls and monitors the exclusion zones to protect higher layer users. It stores and manages user information. High level functional architecture of the CBRS, based on [45] and [31], is depicted in Fig. 3.

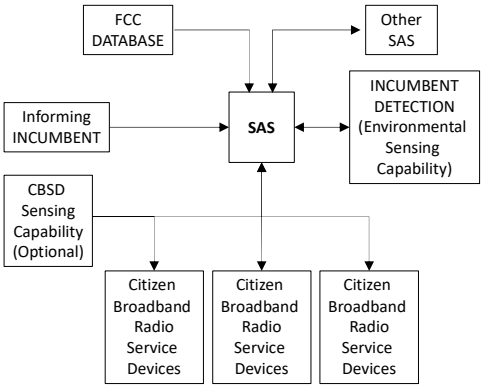

Fig. 3. High level functional architecture of the CBRS.

In contrast to the European LSA, the CBRS concept allows and in some cases may require, the use of a specific Environmental Sensing Capability (ESC) to monitor spectral environment for incumbents and to inform the SAS to direct lower priority users to vacate that specific part of the spectrum. The SAS communicates with the ESC to obtain information about Incumbent User transmissions, and if IA activity is detected, the SAS instructs commercial tier CBSDs to move to another frequency range or cease transmissions within a specified time frame [31].

The confidentiality of the sensitive military incumbent information will be ensured through strict operational security requirements and corresponding certification for the ESC elements and operator authorization. Furthermore,

device level environmental sensing capability is already included in the concept although yet optionally.

The incorporated dynamism of the CBRS concept is further underpinned by the flexible administrative process on spectrum licensing the FCC has adopted.

V. Use Cases: Primary User versus Secondary User

In this section we shall develop a set of use cases based on the notion of Primary and Secondary Users. Furthermore, we infer from the earlier section of scenarios three specific user groups that do have a valid claim to spectrum, namely armed forces (denoted below as MIL), public safety authorities (PS) and legitimate civilian spectrum users, for example Mobile Network Operators (denoted as CIV). These categorizations yield a space of nine theoretical alternative use cases as depicted in Table 1. For the purposes of this paper we shall concentrate on those use cases involving armed forces (bold in the Table 1).

Table 1. Potential Spectrum Sharing Use Cases (Primary User - Secondary USer)

MIL-MIL	**PS-MIL**	**CIV-MIL**
MIL-PS	(PS-PS)	(CIV-PS)
MIL-CIV	(PS-CIV)	(CIV-CIV)

Furthermore, we assume that the main reason for applying such use cases would be the relatively low utilization of spectrum by the Primary User and that the Secondary User has the requirement for additional spectrum and means to implement shared access concept in appropriate manner relevant to the use case.

The notion of Shared Spectrum Access in MIL-MIL case refers to armed forces' internal sharing of spectrum. Although conceptually beyond the traditional notion of Shared Spectrum Access it is definitely a case of Dynamic Spectrum Access and as already pointed to in our analysis of scenarios, armed forces would be well advised to continue research of DSA.

The use case of MIL-PS has potential for application in all scenarios presented earlier. If applied, this use case would protect military from harmful interference by public safety authorities even if operating within same geographic area at the same time, as is bound to happen, for example, in the presented hybrid warfare case. Besides, this use case would improve spectral use efficiency in lower end of the conflict continuum (peace, disaster) by allowing public safety to take advantage of underutilised military spectrum, yet recognizing the ultimate military function of national defence in the higher end of conflict continuum. In the lower end of the conflict continuum, system and network level incumbent protection suffices. In the higher end of the conflict continuum it is reasonable to assume that access to system or network level incumbent protection mechanisms would be seriously hampered by battle damage. Therefore, latter scenarios point towards the requirement for the Secondary User (public safety) to adopt end-user device level incumbent protection mechanisms. As such, this use case would allow military existing inventory of systems and equipment to cohabitate with new developed and procured public safety systems.

The use case of MIL-CIV has potential for application in the lower end of the conflict continuum. Similar arguments apply to his use case as to the MIL-PS case with the observation that it seems commercially doubtful to implement incumbent protection mechanisms to all civilian end user devices. Armed forces may, however, adopt this posture in specific cases of limited frequency bands, limited geographic areas or limited in time, if Secondary User otherwise guarantees incumbent protection.

The use cases of PS-MIL and CIV-MIL provide the armed forces with additional spectrum. This may apply, for example, in remote rural areas, where public safety or mobile networks have little use for the specific frequency (due to nationwide allocation of spectrum) and that might be useful for armed forces for testing and training purposes as examples. In these cases, incumbent protection does not need to be exactly real-time although public safety would need rapid reaction times by the secondary user to vacate the spectrum. As such, implementing this use case for specific circumstances would need little or no modifications to existing or future inventories of systems and equipment.

VI. RESULTS

The capability of dynamic short-term changes and automatic reconfiguration of radio infrastructure as well as user equipment is the key differentiator between Shared Spectrum Access concepts as compared to static sharing concepts, e.g. in the Industrial, Scientific and Medical (ISM) spectrum bands. For MNOs a potential implementation of the LSA will require relatively small modifications to their current inventory of mobile broadband infrastructure and network, whereas opportunistic GAA layer and sensing functions will necessitate a more complicated SAS system within CBRS concept.

The needs for the spectrum by the armed forces varies greatly over time depending on the scenario. Spectrum occupancy measurements cannot provide credible picture of such needs as armed forces are rarely, if ever, in such composition as to invoke all required elements of national military power that use spectrum. Shared Spectrum Access concepts themselves are agnostic of the types and roles of different potential user groups (MIL, PS, CIV).

As a baseline, a Secondary User needs to have some form of basic service level or spectrum already in its inventory, before striving for additional underutilized spectrum, if only to provide a minimum level of QoS to its customers. For such an operator, the Shared Spectrum Access is a complementary approach. However, it is technically possible, although questionable if commercial operators would emerge based solely on secondary access to spectrum.

Large existing inventory of legacy systems places armed forces to maintain current exclusive/primary use modes of spectrum access. New acquisitions and procurement may in specific cases allow for shared secondary access in peace time including disaster recovery scenarios. Large scale

disasters and natural catastrophes call for interagency cooperation and information exchange, supported by shared spectrum access of the public safety authorities as temporary primary user.

Hybrid warfare scenario seriously challenges the notion that by changes in legal frameworks, the military could adopt new spectrum. Firstly, such approach would not (administratively) meet rapid reaction times needed. Secondly it is doubtful if existing legacy systems can use new parts of spectrum. Thirdly, in this scenario military cannot be the sole user of spectrum as public safety authorities may need to operate within the same combat zone. This scenario points to the notion of changing the roles of user groups, i.e. Primary User to Secondary User and vice versa as depicted in Fig. 4. In the figure the hybrid war and homeland defence are compressed into a phase labelled as *combat.*

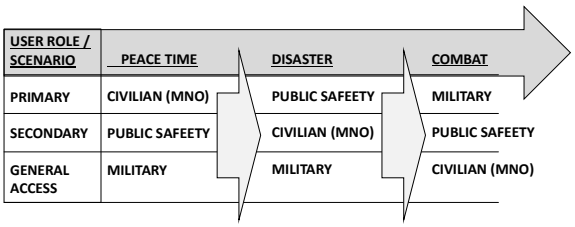

Fig 4. Adjustment of user roles in different scenarios.

The Shared Spectrum Access concepts reviewed support scheduled or on-demand changes of the incumbent protection rights but to change the roles of Primary and Secondary Users needs further research.

Dependent on the worldview the armed forces adopt, homeland defence scenario provides military no operational incentive to relinquish exclusive access, on the contrary, new spectrum may be needed. Military internal Dynamic Spectrum Access would be especially applicable for the armed forces' mobile land tactical communications and may include incumbent protection solutions at the system, network and end-user device -levels. Implementing this use case could provide a deployment path for armed forces to adopt Cognitive Radio technology while recognizing yet remaining life-cycles of their existing inventory of systems and equipment.

Within the Shared Spectrum Access concepts, the baseline has been that of providing secondary user access to underutilized parts of spectrum. However, both concepts reviewed, the LSA and the CBRS, have built-in mechanisms for the incumbent to inform the system on changes in the spectrum needs, even dynamically. This gives rise to the question, what if the military would be the incumbent in most systems and in most bands (e.g. by regulation) of the spectrum but would relinquish his protection requirements in peace time? If national regulators adopted this approach as a national baseline, rapidly changing spectrum needs by the military could be implemented fast by changing policy and configuration data as an input to the LR or to the SAS.

Even if armed forces itself would not adopt Shared Spectrum Access as such, the proliferation of similar approaches among Mobile Network Operators will necessitate new planning methods and procedures within civilian spectrum regulatory authorities, which are bound to reflect also on military spectrum management. Combining viewpoints already presented in section IV.A, military spectrum administrators face spectrum sharing option space depicted in Fig. 5.

Spectrum sharing option space is placed along a continuum that begins from unlicensed, unregulated, ideal common use along the horizontal axis where the ultimate opposite is licensed exclusive use mode. In vertical direction we have either "horizontal sharing" among similar actors and technologies as opposed to "vertical sharing" among different actors and different technologies. The third dimension is that of primary user versus secondary user, in our case concerning the armed forces. As the notion of primary or secondary user is somewhat ambiguous in the technically regulated sharing domain, the option space is constrained into 2 extremes and2+4 potential spectrum sharing alternatives.

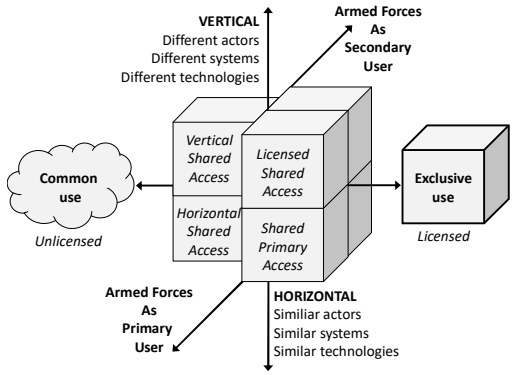

Fig 5. Spectrum Sharing Option Space of the Armed Forces.

Vertical shared access denotes technically regulated sharing between different types of actors or technologies which is exemplified by the unlicensed public use of the Television White Space frequencies for broadband wireless data [46]. Horizontal shared access denotes technically regulated sharing between similar users or technologies, example being wireless local area networking (802.11) within the ISM band.

In the Fig. 5 Licenced shared access denotes Shared Spectrum Access concepts intended for different actors or technologies. Examples of the LSA and the CBRS have already been presented. In this option space armed forces may have the role of either Primary or Secondary User. This option space has been covered in this article. Shared Primary Access (also known as co-primary sharing) refers to a case where two or more incumbents with equal access rights share their spectrum bands in a common pool. Similarly, as above, the armed forces may have here the role of either Primary or Secondary User. In order for the armed forces to obtain

access to large contiguous portions of spectrum for wartime electronic warfighting needs, this option space would need to be further explored.

VII. DISCUSSION

This high-level conceptual review is based on generic view of the armed forces with emphasis on homeland defence. The worldview of the armed forces may be different, for example, focusing on expeditionary operations, and in such case our results should be separately validated.

In this paper we have shown that military spectrum needs vary from one scenario to another and that Shared Spectrum Access may support expected needs of spectrum in times of most dire stress. The Shared Spectrum Access concepts reviewed are yet under development, but the CBRS already has a three-tier approach built in. Both of these concepts have built in dynamism, which however does not support PU-SU role changes across tiers. This warrants further studies. Furthermore, military internal Dynamic Shared Access has military operational potential, exploitation and implementation of which needs further research.

REFERENCES

[1] Cisco, "'Global Mobile DataTraffic Forecast Update 2015-2020, Accessed 21.1.2017,", 1.2.2016.

[2] T. Lehto, "'Spectrum being fought over - shall corporate income rule over government needs (in Finnish)," *TiVi*, 12.6.2016.

[3] S. Chan, "'Shared Spectrum Access for the DoD," *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 524-534.

[4] ITU, "'Collection of the basic texts of the ITU adopted by the Plenipotentiary Conference,", February 2011.

[5] NATO, "'STO-TR-IST-077 Cognitive Radio in NATO," *AC/323(IST-077)TP/497*, 22 Jan 2014.

[6] M. Höyhtyä and et al., "'Spectrum Occupancy Measurements: A Survey and Use of Interference Maps," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2386-2414.

[7] A.M. Wyglinski, M. Nekovee and T. Hou, "'Cognitive radio communications and networks: principles and practice,", 2009.

[8] I.F. Akyildiz, W. Lee, M.C. Vuran and S. Mohanty, "'NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer networks*, vol. 50, no. 13, pp. 2127-2159.

[9] Q. Zhao and B. Sadler, "'A survey of dynamic spectrum access," *IEEE Signal Process.Mag.*, vol. 24, no. 3, pp. 79-89.

[10] J. Hoffmeyer, "'A Roadmap to International Standards Development for Cognitive Radio Systems and Dynamic Spectrum Access,", 2012.

[11] ITU, "'Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)," *ITU-R SM.2152*, 2009.

[12] IEEE Standard, "'Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management," *IEEE Std 1900.1-2008*, pp. c1-48.

[13] ITU, "'Cognitive radio systems in the land mobile service," *ITU-R M.2330*, Nov 2014.

[14] K. Koufos and et al., "'Deliverable D5. 4 Future spectrum system concept," *ICT-317669-METIS/D5.4*, 30 April 2015.

[15] Wireless Innovation Forum, "'Volume 1: Review of the 7 July Bombing of the London Underground," *SDRF-07-P-0019-V1.0.0*, 8.11.2007.

[16] Wireless Innovation Forum, "'Software Defined Radio Technology for Public Safety," *SDRF-06-P-0001-V1.0.0*, 14.4.2006.

[17] T. Tuukkanen and J. Anteroinen, "'Initial assessment of proposed cognitive radio features from a military perspective," *18ICCRTS*, 19-21.6.2013.

[18] US Department of Defense, "'Joint Publication 1 - Doctrine for the Armed Forces of the United States," *JP1*, 25 March 2013.

[19] UK MoD Development, Concepts and Doctrine Centre, "'Army Doctrine Publications - Operations,", 2010.

[20] US Department of Defense, "'Joint Publication 6-01 - Joint Electromagnetic Spectrum Management Operations ," *JP6-01*, 23.12.2012.

[21] T. Tuukkanen and J. Anteroinen, "'Framework to develop military operational understanding of cognitive radio," *ICMCIS2015*, 18-19.5.2015, pp. 1-9.

[22] UK Ministry of Defence, "'Defence Industrial Strategy," *Defence White Paper*, vol. CM997, Dec 2005.

[23] T. Vainio and et al., "'National Risk Assesment 2015," *Ministry of Interior Publications*, vol. 2016, no. 3, 26.1.2016.

[24] Wireless Innovation Forum, "'Elements of Context for Cognitive Radio Based Public Safety Communications Systems," *WINNF-16-P-0019 Version 1.0.0*, 15.4.2016.

[25] F. Hoffman, "'Conflict in the 21st century: The rise of hybrid wars,", 2007.

[26] C. Paul, "'Confessions of a Hybrid Warfare Skeptic," *Small Wars Journal*, 3 March 2016.

[27] R. Oliphant, "'Ukraine crisis: 'Polite people' leading the silent invasion of the Crimea," *The Telegraph*, 2.3.2014.

[28] P. Kuosmanen, "'Choosing routing protocol for military ad hoc networks based on network structure and dynamics," *Helsinki University of Technology*, 2002.

[29] ETSI, "'White Space Devices (WSD); Wireless Access Systems operating in the 470 MHz to 790 MHz TV broadcast band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive," *EN 301 598 V1.1.1 (2014-04)*, April 2014.

[30] CEPT, "'Licensed Shared Access," *ECC Report 205*, Feb 2014.

[31] FCC, "'Order on Reconsideration and Second Report and Order on rules governing the Citizens Broadband Radio Service in the 3550-3700 MHz band," *FCC 16-55*.

[32] A. Ahmed and J. Markendahl, "'Impact of the flexible spectrum aggregation schemes on the cost of future mobile network," *22nd ICT 2015*, 2015, pp. 96-101.

[33] M. Uusitalo, O. Tirkkonen, L. Campoy, K. Sung, H. Schotten and K. Balachandran, "'Spectrum," *5G Mobile and Wireless Communications Technology*, 2016, pp. 336-356.

[34] Wireless Innovation Forum, "'Dynamic Spectrum Sharing Annual Report - 2014," *WINNF-14-P-0001 V0.2.16*, 14.8.2014.

[35] Wireless Innovation Forum, "'Dynamic Spectrum Sharing Annual Report - 2015," *WINNF-16-P-0012 V0.6.0*, 4.3.2016.

[36] ETSI, "'Reconfigurable Radio Systems (RRS); System architecture and high level procedures for operation of Licensed Shared Access (LSA) in the 2 300 MHz - 2 400 MHz band - Technical Specification," *ETSI TS 103 235 V1.1.1 (2015 - 10)*, 2015.

[37] M.M. Sohul, M. Yao, T. Yang and J.H. Reed, "'Spectrum access system for the citizen broadband radio service," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 18-25.

[38] WINNF Spectrum Sharing Committee, "'SAS Functional Architecture," *WINNF-15-P-0047*, 7 Sept 2015.

[39] European Commission, "'Promoting the shared use of radio spectrum resources in the internal market," *COM(2012) 478*, 3.9.2012.

[40] ETSI, "'Reconfigurable Radio Systems (RRS); System requirements for operation of Mobile Broadband Systems in the 2 300 MHz - 2 400 MHz band under Licensed Shared Access (LSA)," *ETSI TS 103 154*, 2014.

[41] S. Yrjölä and et al., "'Licensed Shared Access (LSA) field trial using LTE network and Self Organized Network LSA controller," *WinnComm Europe 2015*, October 2015.

[42] L. Varukina, "'Новые подходы в использовании радиочастотного спектра, [New approaches in the use of radio frequency spectrum]," *Spektr Forum 2015*, 23.9.2015.

[43] CEPT, "'Operational guidelines for spectrum sharing to support the implementation of the current ECC framework in the 3600-3800 MHz range," *ECC Report 254*, 18.11.2016.

[44] President's Council of Advisors on Science and Technology, "'Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth," *PCAST*, July 2012.

[45] FCC, "'FCC Record, Vol. 30, Nr 5,", 13.4.2015, pp. 3494-4441.

[46] IEEE Standard, "'802.22-2011 Wireless Regional Area Networks Standard for Local and metropolitan area networks,", 2011.