Homeland Defence:
Arguments For
A Network Centric Approach

Brian Naudé (Pr Eng)
CSIR (DPSS)
bnaude@csir.co.za

Abstract

Arguments for a Network Centric Approach are considered in view of threat characteristics and a multitude of role-players within an international arena. The challenges to attain effective Command and Control are discussed in the context of Joint, Inter-agency, Inter-department and Multi-national Operations. The opportunities offered by modern technologies are examined in terms of information gathering and exchange. The practical issues of asset application touch on the realities of achieving effective results.

Perspective

Homeland Defence in Operations Other Than War (OOTW) is a challenging business with many facets that determine the manner in which such a defence is given effect. The legal framework within which Homeland Defence may take place is complex given the various threat types and the remedies available to deal with them. The complexity is exacerbated in an international arena by agreements, different cultures and political agendas to serve national interests. The allocation of resources is problematic as there are always shortages and the application thereof is hampered by organisational and technical interoperability issues. Several important factors that impact Homeland Defence are indicated in Figure 1.

Threats and Characteristics

The threats identified come in many guises and are categorised as follows for this discussion:

a) Refugees
b) Illegal immigrants
c) Cross-border criminal activity
d) Criminal activity in international territory/waters
e) Militia incursions across borders

Each threat type has unique characteristics and needs to be dealt with differently by the various government agencies in terms of country and international law. Consequently the government agency individuals directly involved need to know what may be done by whom. The perpetrators will also have knowledge of means to circumvent/ delay law enforcement to their advantage. Therefore there is a need for integrated teams of diverse specialists to handle each situation effectively.

Role-players

The key role-players in the RSA context consist of, but are not limited to, the following:

a) South African National Defence Force (SANDF)
b) Police services
c) Customs and Excise
d) National Intelligence
e) Foreign Affairs
f) Port Authorities
g) Civil Aviation
h) Social Services
i) Department of Justice

In the case where neighbouring countries are involved the equivalent counterparts, especially security agencies, also become role-players if co-operation agreements are in place. The presence of many role-players, each with its own function, and culture, which are not well structured and co-operate on a mutual basis only, presents many challenges for command and control efforts to achieve Homeland Defence objectives. These objectives can form a basis for common intent amongst role-players.

Command and Control

Command and Control (C&C) is an ancient issue and the effectiveness thereof depends on many factors.

Management or C&C functions in this case typically comprise:

a) Setting goals
b) Organising (roles, responsibilities)
c) Creating business rules (how to)
d) Allocating resources
e) Monitoring (assessing execution performance, implementing corrective action)

The above functions are generic in nature and are likely to be named differently depending on the environment and the level at which management functions are taking place i.e. Strategic, Operational or Tactical.

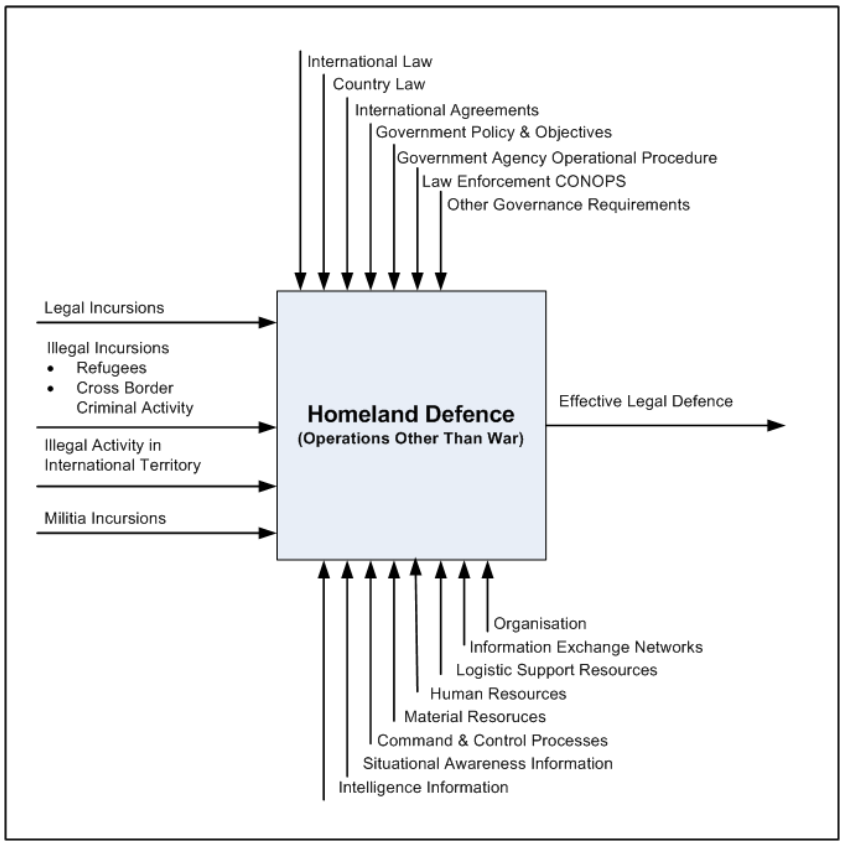

Figure 1: Homeland Defence Factors

Understanding C&C, for the purpose of this discussion, is facilitated by the conceptual frame by Alberts and Hayes [1] in Figure 2.

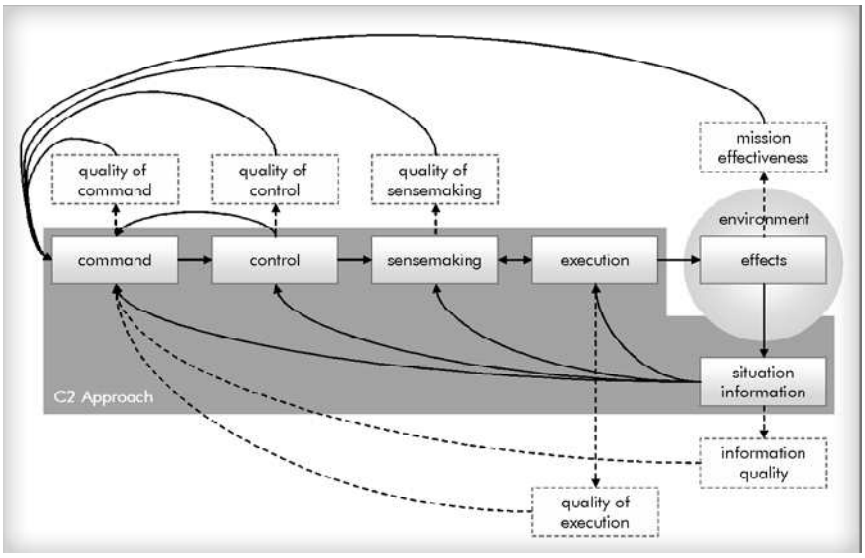

Figure 2: C&C Conceptual Framework

The traditional approach to C&C within the security environment is a centralised unitary hierarchical approach w.r.t. to decision-making. This approach is propagated down through the strategic, operational and tactical levels in terms of a hierarchical structure, facilitating very tight control. Organisationally it implies an individual is at the head of the entire organisation.

In the case where many role-players are involved in a loose or "round table" organisation co-

operation is based on mutual interest or common intent and structured C&C becomes interesting as there is no formal chain of command or rules amongst role-players as in the traditional case mentioned above. In such a loose arrangement a different approach to C&C is required to facilitate the achievement of common objectives.

Situational Awareness

Situational Awareness (SA) is the crux of any C&C effort, irrespective of the approach. The insight and knowledge obtained from SA is dependent on the assimilation of information and data obtained from multiple sources and the cross correlation thereof. Sense-making plays the key role in achieving situational awareness as cognitive processes are unique to each individual involved.

Homeland Defence, as indicated above, is characterised by many role-players who all have information sources and have information that needs to be shared to effect good, agile decision-making. The time value of the information is not to be neglected.

Information gathered on an entity needs to be analysed to characterise the entity in terms of attributes and behaviour for quick reference purposes to aid decision makers on a course of action.

Given the multiple sources of information and the many role-players involved in Homeland Defence it is logical that a shared SA is required to facilitate the achievement of Homeland Defence objectives. The issue will be about what constitutes shared SA, as role-players tend to jealously guard their information.

Performance Criteria

The effectiveness of the Homeland Defence effort needs to be reflected by performance criteria that reflect the success of all activities, including the application of resources and the inherent efficiencies thereof. This implies a management model and systems to assist in control functions.

Setting performance criteria is a challenge owing to the complexity of the Homeland Defence. The many possible parameters that can be of use require a high degree of correlation in a dynamic environment. The creation of a Homeland Defence Index (HDI) is of interest as this is a means to stochastically measure current performance against that of the past, using many different parameters. The means to measure the parameters must (of course) also be in place. The identification of these parameters is beyond the scope of this discussion.

Asset Employment

Assets include all the material and intellectual means to manage Homeland Defence, gather information, and effect defensive actions.

The employment of assets of various role-players needs to be co-ordinated in terms of decisions made in context of the common SA perspective; this implies a level of consensus amongst role-players that requires a high level of mutual confidence to achieve real success.

The availability of assets, within the means of each role-player and national priorities and objectives, presents a challenge in itself as there will always be a shortage.

Technology

The role of technology cannot be under-estimated. Total reliance on technology is not a solution either.

Perpetrators of criminal activity also use modern technology to ply their “trade” and consequently Homeland Defence requires modern technology for surveillance, detection and prosecution of offenders.

The use of modern Information and Communication Technology (ICT) and a plethora of sensors greatly enable the collection, assimilation, distribution and exchange of information in a secure, fast and efficient manner. This includes the sharing of appropriate information on a massive scale. The implication of modern ICT systems is that business processes are enhanced which enable organisations to become very agile. The mass of relevant information available to decision-makers is in itself, a force multiplier.

Concept of Operations- A Network Centric Approach

The Concept of Operations for Homeland Defence needs to be considered in terms of a Network Centric (or enabled) approach to effectively address some of the characteristics of Joint, Inter-agency, Inter-department and Multi-national (JI^2M) operations from a C&C perspective. Such an approach could go a long way to alleviate the problems that will be encountered with the traditional C&C approach (e.g. long decision lines).

The JI^2M operations are likely to be loosely structured, procedurally and organisationally, between main role-players who have more or less autonomy, which will hamper the execution of traditional C&C. Internal structures of role-players

may differ greatly w.r.t. to central and decentralised C&C. A conceptual framework for network-centric operations by DS Alberts and RE Hayes [1] is provided in Figure 3.

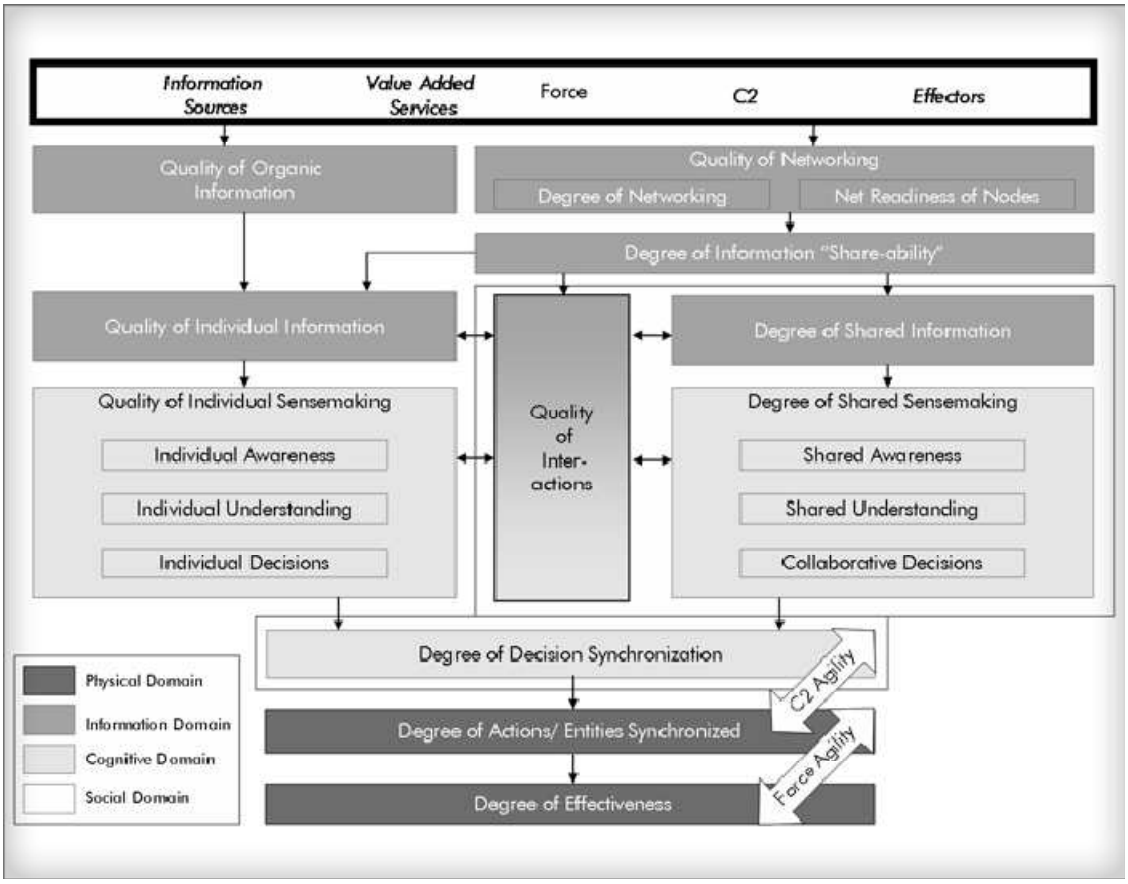

Figure 3: Network Centric Operations Conceptual Framework

A network-centric approach favours autonomous decentralised C&C as opposed to the central unitary C&C of the traditional approach. This implies the movement of C&C functions as far as possible to the outer reaches of the network facilitating force agility.

Technology permits the interoperability at the JI^{2}M level to share integrated information and establish relevant shared SA amongst role-players.

The success of such an approach will depend on the maturity of the JI^{2}M organisation role-players.

Cultural differences will be challenging irrespective of approach. Network-centric structures can actually help solve issues as a result of autonomous C&C. Considerable cross cultural awareness training may be required at all levels, certainly at the higher command levels where personal communication takes place.

Mutually agreed strategies and processes shall facilitate interoperability between JI^{2}M role-players.

Common Cognition

Irrespective of agreements between the JI2M organisations the concept of a "common cognition" within the JI2M role-players is of key importance to give effect to any objective. The concept implies a high degree of common understanding between individuals and groups of objectives and how these are going to be achieved, and the role of each individual.

Only once this state is achieved is effective collaborative action possible as the collective energy of the role-players can be successfully focused. Figure 4 highlights this relationship and its intangible human complexities.

The effectiveness will depend enormously on the skill and maturity of individual role-players and the extent to which they are able to collaborate.

Conclusion

The network-centric approach offers many advantages for Homeland Defence in a multi-cultural and international environment as it offers a

means to manage complex mutual defence efforts on a collaboration basis. The involvement of neighbouring states on a common intent base permits the displacement of threats away from physical, political and socio-economic borders by

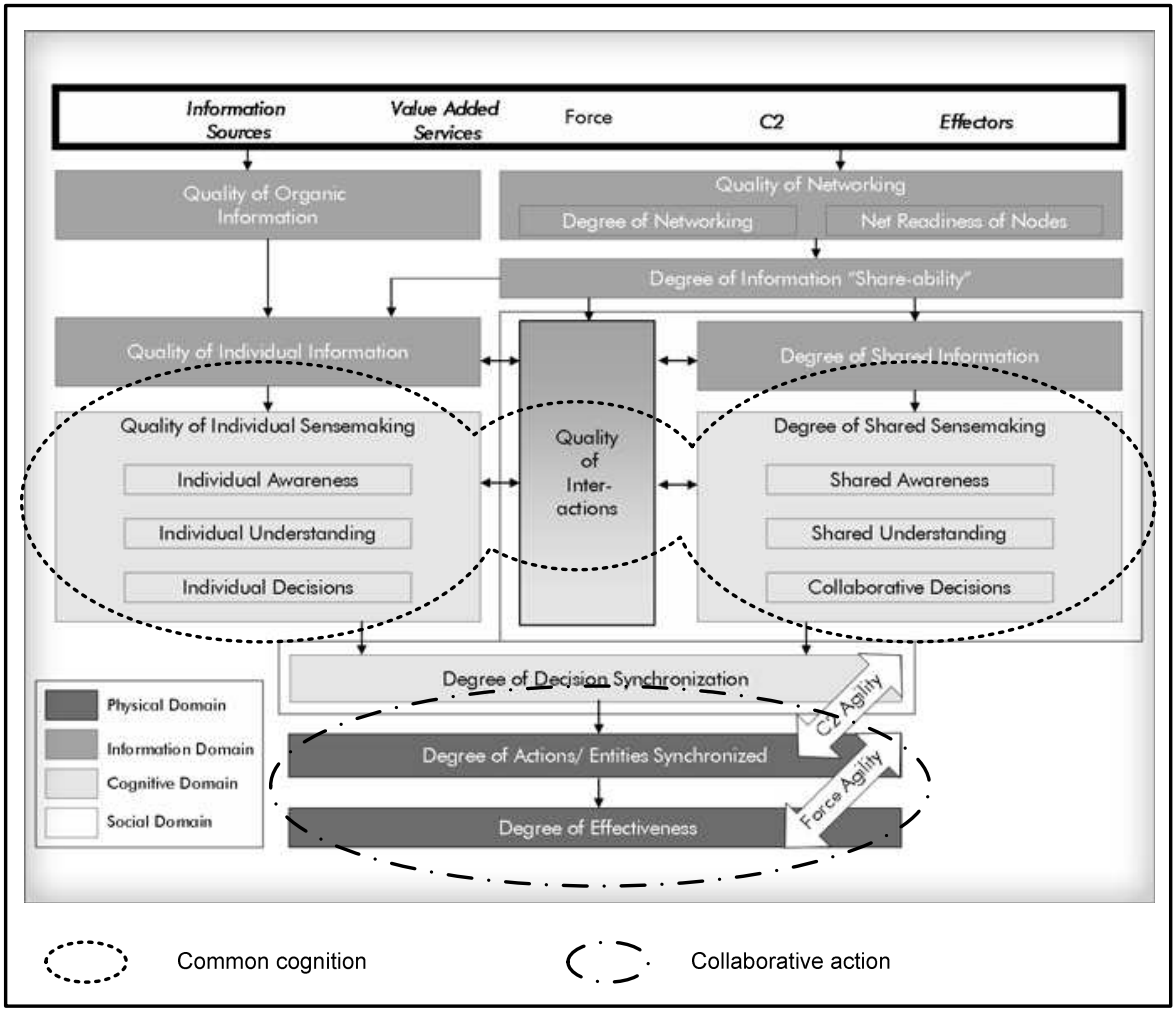

Figure 4: Cognition & Collaboration

means of a larger co-ordinated defence effort to the benefit of collaborating role-players. The visible beneficiation to the respective economies as a result of the effort will strengthen the collaboration efforts. The undermining of the collaborated efforts would no doubt constitute the most serious threat to Homeland Defence.

References

[1] DS Alberts, RE Hayes, 2006, *Understanding Command and Control*, Command and Control Research Program, USA DOD, ISBN 1-893723-17-8

Biography

Brian Naude (Pr Eng) has 30 years of engineering experience. He started his career in the Telkom laboratory developing micro-processor based test equipment and later held a communications network planning management post. During national service he performed a radio communication support function. He has been in the defence industry for the last 25 years where he has worked in a system and logistic engineering role on a diverse set of military projects ranging from IT to SAN, SAAF and SA Army systems. He holds a BSc (Eng) degree in electronics from the University of Pretoria.