Adapting the Current National Defence Doctrine to Cyber Domain

Topi Tuukkanen, Finnish Ministry of Defence, Helsinki, Finland

ABSTRACT

The current defence doctrine in Finland is analysed from a cyber perspective, and doctrinal tenets that adapt to the cyber domain as well as fundaments that do not, are pointed out. In most cases, current defence doctrine and fundaments can be adjusted to cyber domain. Some need more research and planning, but also new legislation and organisational arrangements would be needed. As such, a cyber defence doctrine has a sound basis but should be elaborated in more detail once national cyber security strategy has been completed.

Keywords: *Comprehensive Approach, Conscription, Cyber, Deterrence, Doctrine, Readiness, Sovereignty, Territoriality*

CYBER AS A NEW DOMAIN?

The emergence of internet and interconnected systems has created an altogether new ecosystem, a domain that significantly contributes to our daily lives. Having revolutionised many ways by which we conduct our everyday tasks, be it in companies or in private; also new threats and challenges have emerged. Forrest Hare (2010) has analysed societies' vulnerabilities to cyber threats using Buzan's (1991) framework of power versus socio-political cohesion. Finland has traditionally had relatively low budgetary expenditures on armed forces in general, a relatively homogenous population, a strong national identity and a well-established and functioning political system. Therefore, based on the work of Hare, it can be argued that Finland would be especially prone to military threats in the strategic-political sphere and to substantial cyber threats against critical infrastructure.

Alvin and Heidi Toffler (1993) have claimed that any period of civilization – be it iron age, bronze age, etc., up to present information age – have introduced new means of waging war appropriate to the technologies available at that time. The older means of war fighting still remain, but the new means are additions to the toolbox available. Already in the contemporary "Information Age" we have already witnessed state sponsored (if not necessarily authored) attacks and espionage campaigns as well as attacks to internet services or attacks through SCADA-networks to inflict physical harm, although it seems that the full potential of the cyber domain in warfare has not yet been utilised. Therefore, cyber domain has created

DOI: 10.4018/ijcwt.2011100103

impetus to alter and adjust military strategies that ultimately affect the very nature of war (Cebrowski & Gartska, 1998).

Entry to the information age in the way militaries think,plan and conduct warfare was already understood in the early 1980s in the Soviet Union as Military Technological Revolution (Krepinevich, 1992). After the Gulf War, this notion was captured in the western world under the title Revolution in Military Affairs. It was later followed and complemented by the concept of Effects Based Approach to Operations (EBAO), which, however, has now been suppressed (Mäesalu, 2010). Parallel to these developments, the emerging internet technologies contributed to the rise of new war fighting concepts like Information Operations (U.S. Department of Defense, 1998) and Network-Centric-Warfare (Cebrowski & Gartska, 1998).

In 2001, the US Department of Defence initiated the "*transformation*" in armed forces and by the establishment of the Allied Command Transformation, as the second strategic command within the NATO command structure, the Alliance is now formally following the suit. In addition to these, many nations have already identified the cyber domain as a 5th space of warfare after land, sea, air and space (Schreier, Weekes, & Winkler, 2010).

For example, the U.S. Department of Defense 2010 Quadrennial Defence Review Report outlines that: *"The global commons are domains or areas that no one state controls but on which all rely. Future adversaries will likely possess sophisticated capabilities designed to contest or deny command of the air, sea, space, and cyberspace domains"* (U.S. Department of Defense, 2010). This strategic view is further developed in the U.S. Department of Defense's Strategy for Operating in Cyberspace, where it is quite clearly stated that: *"DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential"* (U.S. Department of Defense, 2011).

On the other hand, doubts have been expressed that cyberspace could not be characterized as a domain. However, current thinking on the territoriality of cyberspace reflects that cyberspace is partly a human construct, partly natural and partly informational, but that the physical nature of its infrastructure permits territoriality to be exercised by the states. From this, legal norms concerning sovereignty, territoriality and jurisdiction apply to those elements which on their part constitute the cyberspace (Robinson et al., 2012).

The rapid emergence and continuous change of underlying and underpinning technologies on cyberspace have presented armed forces with a number of challenges:

- The late 90s dogma of Revolution in Military Affairs (RMA) and complementing Network-Centric-Warfare have, by focusing on robotics and automation, rendered militaries vulnerable to cyber attacks.
- Militaries have become reliant and dependent on cyberspace both for national defence as well as for expeditionary operations.
- Cyber has been used in warfare (Georgia, 2008) and also demonstrated in one-off incidents below the threshold of an act of war, but massive demonstration of cyber-power is still yet to come.
- At nation-state-strategic level, the military is often poorly positioned to take the holistic responsibility of national cyber defence; in many instances the armed forces simply do not have the mandate or the authority to do so and often they also lack the resources and access to the very systems they might be expected to protect. Public-private partnerships and more agile administrative arrangements are needed (Joubert, 2010).
- Cyber capabilities present the small-to-mid-sized nations a possibility to alter present military status-quo in relative terms (Schreier & Weekes & Winkler, 2010).

The USA as well as Russia and NATO all recognise various forms of Information Warfare technologies as critical. These have also been identified as critical technologies to be closely monitored in the Finnish Defence Forces (Ko-