Carvalho CYDEF 2018

１　氏名及び役職名等（Name and Title）

ルイス・カルバルホ、NATO 多国間サイバー教育訓練プログラム
LTC Luis Carvalho, NATO Multinational Cyber Education and Training Program

２　略歴（CV）

通信部隊将校、指揮幕僚課程を修業。ルイス・サロマオ・カルバホ中佐は電子計算機科学の学士号、軍事電子工学の修士号を有している。かれは幾つかの研究プロジェクト、サイバー関連の作業部会、例えばリスボンにおける陸軍司令部の幕僚、ブリュッセルにおけるポルトガルの NATO 及び欧州連合軍事代表部の幕僚及び軍事支援員として勤務した。ルイス・サロマオ・カルバホ中佐は、軍事作戦、運用術、軍事技術の専門家である。2017 年に、かれは NATO スマート防衛「サイバー防衛教育訓練に関する多国間プロジェクト（MNCDE&T）」に参加するとともに、欧州連合軍事訓練集団－サイバー防衛熟練部の国家共同リーダーとなった。現在、かれはポルトガル防衛省国防資源部長の顧問としても勤務している。

Signal Corps Army Officer, qualified with the Staff Officer's Course. Lt Col Luis Salomão Carvalho has a degree in Electronics and Computer Science and a Master in Military Electronics Engineering. He has been involved in several research projects and Cyber related working groups namely as Staff Officer at Army Staff HQ, in Lisbon, and as Staff Officer and Military Assistant of the Portuguese Military Representative to NATO and EU, in Brussels. Lt Col Luis Salomão Carvalho is an expert on Military Operations and on Techniques and Military Technologies. In 2017 he was appointed Project Manager of the NATO Smart Defence "Multinational Project on Cyber Defence Education and Training (MNCDE&T)" and the National Co-Leader at the European Union Military Training Group - Cyber Defence Discipline.
He is now working for the Directorate-General for National Defence Resources of the Ministry of Defence, as advisor.

３　参加枠（Time Slot）

APR 5, 1305-1335 Key Note Speech

４　講義要約（Abstract）

「イノベーションと能力構築に向けた教育訓練」
サイバー空間はしばしば軍事作戦の第 5 のドメインであり、陸上、海上、航空及び宇宙のドメインと同じく国家防衛及び集団的防衛のため死活的に重要だと言われる。軍事任務を成功させるには、サイバー空間の利便性と活動の自由が益々重要になっている。堅牢でレジリアンスを確保したサイバー防衛能力は、現在、軍事構造、任務及び作戦の支援に必須となっている。
厳しい予算的制約と乏しい資源のもと、各国の指導者は、NATO 加盟国及び欧州連合諸国が将来課題に向き合うため、実践的で足並みを揃えたサイバー防衛能力構築の手法として、NATO の「スマート防衛」及び欧州連合の「プーリング＆シェアリング」構想に着目している。この動きはさらに進展する。サイバーは両義性をもつ領域で、サイバー防衛及びセキュリティを担保する相助作用を伸ばす多くの機会を提供するとともに、そのコンピテンスは研究開発を強調する。

“Education and Training towards Innovation and Capability”
Cyberspace is often described as the fifth domain of military operations, as equally critical to national and international defence as the domains of land, sea, air and space. The success of military missions increasingly depends on the availability of cyberspace and freedom of action in it. Robust and resilient cyber defence capabilities are now required to support military structures, missions and operations.
Because of severe budget constraints and scarce resources, leaders see NATO’s Smart Defence and the European Union’s (EU’s) Pooling and Sharing efforts as pragmatic and coherent ways to generate the cyber defence capabilities NATO member nations and EU member states need to face future challenges.
As this work moves forward, cyber remains a dual-use sector that offers many opportunities to develop synergies covering several aspects of cyber defence and security, from competence profiles to research and development.