



## 1 氏名及び役職名等 (Name and Title)

クリスチャン・リフランダ－、NATO エマ－ジグセキ－リテ－対策本部サイバ－防衛部長

Mr. Christian Lifländer, Head of the Cyber Defence Section, Emerging Security Challenges Division, NATO

## 2 略歴 (CV)

クリスチャン・マーク・リフランダ－は NATO エマ－ジグセキ－リテ－対策本部サイバ－防衛部長である。サイバ－防衛部は、NATO のサイバ－防衛政策の策定及び調整に責任を有する。リフランダ－氏の前職は、エマ－ジグセキ－リテ－対策本部サイバ－防衛部の政策顧問兼副部長 (政策) であった。国際スタッフとして NATO に参加する前は、リフランダ－氏はエストニア防衛省に勤務していた。かれは経歴の早期に幾つかの枢要な配置及び上級顧問職を経験しており、防衛大臣補 (代理)、政策局長、防衛大臣顧問の任についていた。リフランダ－氏は在米国エストニア共和国大使館の防衛審議官、エストニア共和国 NATO 派遣部の防衛審議官も経験している。リフランダ－氏はエストニア防衛軍 (歩兵) の将校待遇辞令を受け、エストニア防衛軍殊勲賞及びエストニア防衛省殊勲賞を受賞している。リフランダ－氏は米陸軍士官学校で科学学士号、また、エドモンド・A・ウォルシュ海外校において、ジョージタウン大学セキュリティ研究所のセキュリティ学修士号を授与されている。

Christian-Marc Lifländer is the Head of the Cyber Defence Section of the Emerging Security Challenges Division at the NATO Headquarters. Cyber Defence Section is responsible for cyber defence policy implementation and coordination across NATO. Prior to his current position Mr Lifländer served as a Policy Advisor and the Deputy Head (Policy) in the Cyber Defence Section of the Emerging Security Challenges Division.

Before joining NATO International Staff Mr Lifländer served a career in the Estonian Ministry of Defence. He held several executive and senior advisory level

positions early in his career, including serving as Acting Deputy Undersecretary for Defence Policy, a Director of Policy Planning, and an Adviser to the Minister of Defence. Mr Lifländer also served as a Defence Counselor at the Embassy of the Republic of Estonia in the United States and as a Defence Counselor at the Delegation of the Republic of Estonia to NATO.

Mr. Lifländer received a direct commission in the Estonian Defense Forces (Infantry) and has been awarded with the Estonian Defence Forces Distinguished Service Decoration as well as Distinguished Service Decorations of the Estonian Ministry of Defence.

Mr. Lifländer received his Bachelor of Science Degree in Engineering from the United States Military Academy, West Point. He received his Master of Arts in Security Studies from Georgetown University's Center for Security Studies (CSS) in the Edmund A. Walsh School of Foreign Service.

### 3 参加枠 (Time Slot)

APR 4, 1040-1110 Key Note Speech

### 4 講義要約 (Abstract)

「新しいドメイン、古き課題: NATO の直面するサイバー課題」  
将来のいかなる事件、紛争または危機において、サイバー的要素を含まないものは想像し難い。そして、これは現在すでに我々が直面している環境でもある。その意味は、能力開発の分野に「魔法の弾丸」はないということだ。実際のところ、サイバーに内在する技術的特徴は、勃興するサイバー脅威に対抗するソリューションを、希にウィジェット調達するようなものだ。この特殊なサイバーの課題に対処するためには、モノの要素から、より幅広く、より実践的な変革が求められている。つまり、それは人材登用、ドクトリン、訓練及び組織改編に関わる課題を意味する。NATO は共同作業により、より良い成果が得られることを発見した。サイバー空間を航空、陸上及び海上に並ぶ作戦ドメインとして認知する意志決定により、多くのものが生まれた。われわれは前に進み始めた、この仕事は前進の終点を意味するのではなく、むしろ始まりを意味する。

“New Domain, Old Challenges - NATO meeting the challenge of cyberspace”

It is difficult to imagine any future event, conflict or crisis that would not include a cyber component, given that this is the environment that we are all operating in already today. What this means for capability development is that there is no cyber ‘magic bullet’. In fact, the inherent technical characteristics of cyber mean that solutions to emerging cyber threat are rarely going to be about widget acquisition. If we are to respond to the unique challenges of cyber we will have to have a much wider and more practical change than

**addressing the material element alone. This means addressing challenges such as manning, doctrine, training and organizational issues. NATO is founded on the idea that we can achieve more when we work together. A lot is happening as a result of a decision to recognise cyberspace as an operational domain, alongside air, land and sea. While progress is being made, this work must be regarded as the beginning, rather than end, of progress.**