NATO
OTAN

Joint Analysis & Lessons Learned Centre

NATO's Lead Agent for Joint Analysis

Joint Analysis & Lessons Learned Centre
JALLC

CYBER DEFENCE SITUATIONAL AWARENESS IN NATO

Report Published on 13 October 2014

PROJECT FACTSHEET

PROJECT OVERVIEW

Project Manager COL Gilles Castel (r) with JALLC analyst Art Sosa outside the Allied Joint Force Command HQ in Naples

In response to the rapidly growing cyber threat targeting both NATO and Allied networks, Heads of State and Government at the 2010 Lisbon Summit took the decision to bolster NATO's cyber defence efforts. Significant progress has since been made in this respect, but it is important to recognize the emerging challenges to cyber defence that NATO faces.

The Joint Analysis and Lessons Learned Centre (JALLC) was tasked by Supreme Allied Commander Transformation (SACT) to conduct a study analysing Cyber Defence Situational Awareness and Information Sharing within NATO in order to improve the ability of the NATO Command Structure (NCS) to respond to Cyber Threats and share Cyber Defence lessons.

The study focused on mapping the key Cyber Defence actors within NATO and their connections, identifying the key information exchange requirements to be shared within NATO for Cyber Defence in the NCS, and identifying any gaps and shortfalls in NATO's Cyber Defence Situational Awareness.

MAIN FINDINGS AND RECOMMENDATIONS

One of the main findings from the study is that, within the NCS there is a lack of clarity about who is actually responsible for Cyber Defence and what information should be shared and with whom. Currently, it appears that Cyber Defence related information is not being shared effectively among NCS Cyber Defence personnel, usually because personnel either do not know who has the information or who needs it. Where lines of communication regarding Cyber Defence information sharing do exist, these lines seem to be highly dependent on personal relationships—rather than on a standard process—implying that such lines of communication may be lost after personnel rotation.

To resolve many of these issues the Cyber Defence Working Group concept has been developed in a number of Allied Command Operations Standard Operating Procedures (SOP) and endorsed by SHAPE in the Cyber Defence Functional Planning Guide. Once these Working Groups are officially created, enshrined in SOPs, and recognised as the primary points of contact for Cyber Defence for their command, then it is expected that lines of communication and information sharing with regard to Cyber Defence will improve.

Many of the main-findings and recommendations from this study have since been addressed in the Enhanced Policy on Cyber Defence, Supreme Allied Commander Europe's Direction and Guidance on Cyber Defence, and SHAPE's Cyber Defence Functional Planning Guide. However, the report still provides a succinct overview of Cyber Defence in the NCS and sets out recommendations for the way ahead.

Cyber Defence is of growing concern within NATO (Source: NATO website)

Project Execution

In 2011 there were 403 million unique variants of malware, compared to 286 million in 2010. Source: Symantec Internet Security Threat Report, April 2012 (Photo courtesy of National Intelligence Criminal Resource Centre, NATO)

In order to conduct an analysis of the Cyber Defence environment within NATO, the project team first needed to increase their understanding of Cyber Defence in general and in particular NATO Cyber Defence policy and Cyber Defence information sharing within the NCS. The project team achieved this by first performing a thorough review of relevant documents followed by conducting interviews with almost 60 subject matter experts, including personnel from HQ SACT, SHAPE, NATO Communications and Information Agency, the Joint Force Commands, and the Single Service Commands, as well as NATO's International Staff and International Military Staff.

The project team then defined Cyber Defence situational awareness in terms of the ability to Detect, to Assess and to Inform on Cyber Threats, utilizing these terms to categorize the gaps and shortfalls uncovered during their research and analysis.

The scope of the study was limited to cyber defence situational awareness within the NCS and was not an analysis of NATO's technical capabilities or a study of cyber related security matters.

Project Team

Colonel Gilles Castel, French Army

COL Castel was posted to the JALLC as Legal Adviser (LEGAD) and military analyst in August 2013. He served initially as a Surface to Air Artillery officer until his graduation from the French War College in 2000. He then served as LEGAD in several Headquarters, either in France or in Operations as KFOR, SFOR or ISAF. His last deployment before joining the JALLC was chief of the Administrative Law Office by the French Ministry of Defence legal department .

Lieutenant.Colonel Claudio Toro, Italian Air Force

LTC Toro was posted to the JALLC as a military analyst in 2012. He has served in the Italian Air Force as an Air Defence Controller since 1991. Most of his career has been spent with Radar Squadrons as a Surveillance Coordinator, Ground Intercept Controller, Fighter Allocator and Weapons Manager. In 1998, he was assigned to the US Balkan Combined Air Operations Centre in Vicenza as Mission Director for the NATO Joint Operations in Bosnia and Kosovo. In 2007, he was assigned to the Italian Air Force HQ in Rome, where he had served until his current assignment to the JALLC.

Lieutenant Colonel Rafal Chmura, Polish Air Force

LTC Chmura has served in the Polish Air Force since 2000. After graduating from the Polish Military University of Technology (as an engineer), he served in a number of positions including as commander of a radar station and as a specialist in the Defence Planning Division of the Polish Air Force HQ. He completed the Operational-Tactical Postgraduate Studies at the Polish Academy of National Defence in Warsaw and holds masters degree in telecommunication in transport (from Warsaw Polytech). LTC Chmura joined the JALLC as a military analyst in 2013.

Mr. Art Sosa, Civilian Analyst

Mr. Sosa is a former US Army Officer with thirty years of experience holding command at all attained ranks. He graduated from the US Army Senior Service College/War College and Command and General Staff College. He holds a master's degree in education and has served with the JALLC since 2007.

JALLC

Joint Analysis and Lessons Learned Centre
Avenida Tenente Martins – Monsanto
1500-589 Lisbon
Portugal

Phone: +351 21 771 7007/8/9
Fax: +351 21 771 7098

NATO's Lead Agent for Joint Analysis

All JALLC Reports, the LL Portal, and NATO LL Items may be found in their entirety under the *Products* section on the NS WAN: **http://www.jallc.nato.int**

Non-classified reports and LL Items, Project FactSheets, the Joint Analysis Handbook and the Lessons Learned Handbook can be found on JALLC's Internet site at the same address.

A proud member of Allied Command Transformation