



Fig.1. General Taxonomy of cyber attacks for the operational level.

Cyber defence is a serious threat facing NATO and its information systems. But, to remain cyber secure, this effort cannot be accomplished alone.

Serious Threats Take Serious Action

Cyber attacks on the NATO Communication and Information System (CIS) are becoming more frequent, more organised and more influential to the NATO mission. These attacks may affect critical infrastructure supporting NATO CIS. It is possible that they may reach a threshold which threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised crime, terrorist and/or extremist groups and even insiders can all be at the source of a cyber attack.

Maintenance of cyber security is a shared NATO responsibility and every one of us has a cyber defence role to play. Effective NATO cyber defence must be a collective effort; it is not a game that can be played alone.

Cyber training and the integration of cyber-relevant injects within exercises are the means to test and validate consultation, command and control (C2) and the decision-making processes required to establish and maintain effective cyber defences in a complex, multi-national and coalition environment.

Change of the Operational Mindset

The main defence against cyber attacks are user awareness and prompt reporting of suspicious activity.

The initial effort in Allied Command Operations (ACO) for cyber defence training is to change the mindset of the staff regarding the topic. This mindset change will assist the operational staff on how to respond to cyber threats. The training aims to enforce that managing cyber incidents is an operational issue and not just a CIS issue. Moreover, cyber incidents have to be handled operationally across the ACO commands and beyond.

The Need for Cyber Defence within NATO Exercises

"When you move from "policy" level to "do it" level, you realize that only a few people are around with expertise and experience to effectively translate into practical terms for the operational staff what the high level policy wants to say", as mentioned by Lieutenant Colonel Luc Lafreniere

[SHAPE CIS INFOSEC](#)

former Section Head.

You may be familiar with the Cyber Defence Policy, [CDMB CONOPS](#) and other documents from the strategic NATO HQ level. While helpful, these documents do not provide operational staff answers to the principal question

"What do I have to do when a cyber attack occurs?"

Here is where ACO can provide a tight linkage between the operations and strategic side of cyber defence therefore providing answers to the above question.

ACO maintains a focus in planning and executing cyber defence scenarios into existing NATO exercises which will be on creating cyber security awareness for training audiences. This awareness will be exercised on preemptive measures, such as contingency planning, and reactive actions, such as consequence management.

Cyber defence training scenarios should be incorporated into the overall exercise scenario in such a way that they do not interrupt the execution and/or evolution of the exercise and do not hinder the fulfilment of the set training objectives. This links back to enforcing a mindset change. The efforts should be focused on linking cyber security issues with operational incidents. This will bring realization to the forefront of individual's minds that cyber attacks may be detrimental to operations and lead to wider comprehensive issues.

Think Beyond Technology

Figure 1 describes the final result of a cyber attack. The key takeaway is the "Exfiltration" and how to respond. The technical aspects of cyber defence ([IDS](#) configuration and exploitation, malware analysis, forensics, etc.) are assumed to be carried out by other bodies and the operational staff starts training from that point forward.

Some types of cyber attack like Denial of Service (DoS) are easy to be observed. Some other types like data exfiltration and modification can not be easily revealed and effective fusion of information is critical in order to come to the right conclusion. It is very important to be able to analyze, correlate and synthesize information. The key element is the capability for fusion of information through varied sources (INTEL, SIGINT, Media reports, INFOSEC reports etc) in order to recognise the Cyber Attack (for example a document exfiltration) as the root cause of other operational/kinetic attack events.

Cyber defence incidents should not be reviewed in isolation. They should require the engagement of all operational staff and not be treated as CIS technical issue.

ACO is focused on implementing a comprehensive approach which integrates cyber technology with policy, processes, people and management. By adopting this approach we expect to train staff in an appropriate way during exercises in order to achieve uninterrupted operations and mission fulfillment.

[Back to Cover](#)

[Next Article](#)