2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011

Rationale and Blueprint for a Cyber Red Team Within NATO

An Essential Component of the Alliance's Cyber Forces

Luc Dandurand
Cyber Defence and Assured Information Sharing
NATO C3 Agency
The Hague, Netherlands
luc.dandurand@nc3a.nato.int

Abstract– **This paper provides the rationale and blueprint for a "cyber red team", a dedicated military capability whose objective is to improve the cyber defence of the Alliance through the controlled execution of cyber attacks. These cyber attacks would be specifically designed to achieve three goals. The first goal is to assess the effectiveness of the existing security measures in providing mission assurance, at both the technical and procedural levels. The second goal is to demonstrate the possible impact of these cyber attacks to senior management and key stakeholders. The third goal is to improve the cyber security staff's ability to detect and respond to cyber attacks by exposing them to realistic, unannounced attacks in their specific working environment. Details of the proposal cover governance, command and control, modus operandi, organizational structure, skills and experience required for team members as well as recommendations for personnel selection. It also identifies a number of controls that would address concerns related to its implementation.**

Keywords: NATO, cyber defence, cyber attack, cyber forces, red team, assessment, demonstration, training

This work was sponsored by NATO's Allied Command Transformation under the 2010 Cyber Defence Programme of Work. This document is a working paper that may not be cited as representing formally approved NC3A or NATO opinions, conclusions or recommendations, and represents only the views of the author.

I. INTRODUCTION

Given the immense complexity of large, modern communication and information systems (CIS), military organizations rely on risk management as the primary approach to achieve "adequate" security and protect the CIS from attack, each following the approach with a different degree of formality. Through risk management, military organizations identify security measures intended to bring the risk to a level thought acceptable without unduly limiting the usability of the protected CIS, an unfortunate side-effect of most security measures.

Many accelerating trends, such as convergence to IP networks, greater interconnectivity, and increased cyber threats, are resulting in greater uncertainty about the actual risks being taken. The cyber domain is simply changing too quickly for most military organizations to fully appreciate the impact of these changes on the security posture of their CIS. Best practices on risk management [1] are increasingly more difficult to follow under tighter constraints on time and budget, and the constant changes in operational requirements inherent to military missions. Finally, most of the security measures deployed in modern CIS require human involvement to function properly. Thus the effectiveness of security measures is dependent not only on the successful implementation of an underlying technical system, but also on the users' ability to operate it correctly and to follow specific processes.

The end result is that once a CIS is deployed, the senior decision makers responsible for its security and proper functioning, as well as those relying on it to execute their assigned mission, are sometimes left with a number of unanswered questions:

- Is the system sufficiently secure? Are some security measures unnecessary?
- Are the firewalls properly configured? Are the proper rules loaded into the intrusion detection system? Is the wireless network properly secured?
- Are the restrictions on the user workstations really necessary? Does it really help security to have new staff request access to each information resource independently? Does the single sign-on solution create a single point of failure?
- Will advanced, persistent threats be detected? Will potentially significant events be reported? Will all detected incidents be correctly analysed? Will staff know how to respond to an attack? Could security staff be overwhelmed by a cyber attack?
- What can an attacker do if he gains access to the CIS? How much information could be extracted before detection? If the attacker tried to modify operational information, would the users realize it before using the information? If the attacker destroys information, will it be possible to restore it from backups? How long will it take to restore each service?

Large military organizations require the capability to measure the actual effectiveness of the security measures deployed in operational CIS to provide mission assurance and reduce the uncertainty about the risks the CIS faces. As well, they require the capability to effectively demonstrate to senior decision makers the possible consequences of cyber attacks against specific military missions. Finally, given the significant degree of dependence of security measures on human processes, users and security staff require experience in how to respond to cyber attacks based on highly realistic scenarios conducted in their day-to-day environment, so that the cyber domain benefits from the same level of preparatory training as that being provided to the other domains of warfare.

Within NATO, the NATO Network Enabled Capability (NNEC) has begun shifting the traditional balance between security and ease of use and ease of access to information. "By improving collaboration in an open and dynamic information environment, NNEC enhances the efficiency and effectiveness of the Alliance." [2] For the International Security Assistance Force in Afghanistan, NATO's Afghanistan Mission Network is a significant step towards the NNEC. It reviews the balance between security risks and the benefits of an open and dynamic environment brought to overall mission effectiveness in a large coalition of military forces. More recently, the WikiLeaks incidents [3 and 4] have led some to question whether this new balance is the right one, and NATO's senior decision makers are trying to find the correct balance between sharing and protecting information given the realities of the modern cyber world.

This paper proposes the establishment of a "cyber red team" as a standing capability within NATO that would complement ongoing efforts aimed at addressing the above military requirements, as well as help NATO reap the full benefits of the NNEC with greater confidence that the actual risks being taken are in fact acceptable.

II. THE CYBER RED TEAM: AN ESSENTIAL MILITARY CAPABILITY

This paper considers a "cyber red team" (CRT) as a specific military cyber defence capability that provides a service to a requesting NATO organization. The capability and the service it provides to its "clients" are defined in some detail in order to provide a holistic and coherent view of how it could be properly managed, to dispel unfounded perceptions that it is a high-risk initiative, and to build confidence that, with the proposed control and accountability mechanisms, NATO can trust that the CRT will deliver the requested service in a proper fashion. Most if not all of the proposed implementation can be amended if necessary.

A. Mission of the Cyber Red Team

The mission of the proposed CRT is: "to assess the overall effectiveness of the security measures of an operational CIS in providing mission assurance through the controlled execution of no-notice, realistic cyber attacks, demonstrate their

mission impact to stakeholders and senior decision makers, and improve the cyber security staff's ability to detect and respond to these attacks".

As explained in Section I, the three activities identified in the mission statement (assess, demonstrate and improve) are the activities that could contribute the most to increasing the cyber security of NATO's CIS. The fact that the controlled execution of cyber attacks against operational CIS will generate factual evidence is the key value-added element for the assessment of security measures, at both the technical and procedural levels, and will enable credible demonstrations of the potential mission-level impact of these cyber attacks. As well, the fact that these controlled cyber attacks will be performed on operational CIS and without advising security staff in advance will allow for the best opportunity for improvement possible, short of an actual cyber attack.

It is important to note that the implementation of this capability will also provide insight into various aspects of cyber attacks, an element sometimes missing in the design and deployment of security measures. The rapid pace of change in the cyber domain requires defenders to remain abreast of the evolution of cyber attacks, and the CRT will provide critical information regarding the nature of cyber attacks to NATO and NATO Nations as a result of the execution of its mission.

1) Assessment of the Overall Effectiveness of Security Measures and Processes in Providing Mission Assurance

One of the three primary activities of the proposed CRT is to assess the actual effectiveness of security measures in an operational CIS and determine the extent to which they contribute to mission assurance. Such an assessment is performed only at the request of the head of a client organization, who will also define its scope and objectives. By their nature, these assessments will cover not only the technical and procedural aspects of security measures, but also how well they actually integrate together, a key aspect typically not verified by conventional security assessments. Given that human actions and processes play a fairly significant role in nearly all security measures, and given human nature, a realistic assessment of the overall integration of human processes and technical solutions can be achieved only if performed without notice, hence most staff members will not be advised of a CRT assessment. As well, the focus of the assessment is not the security measures themselves, but the impact of the cyber attacks on the mission given the effectiveness of the security measures.

A red team assessment is not a vulnerability assessment, nor is it penetration testing, as those terms are generally understood[1]. For most organizations, the former is generally undertaken in a collaborative fashion with the aim of listing all vulnerabilities in a network using automated tools. These tools typically show only the potential vulnerabilities of the systems assessed within the context and configuration of such systems, and do not indicate whether their exploitation is realistic given the system's configuration, the network's topology, its security

[1] The definitions of vulnerability assessment, penetration testing and red team assessment can vary from one organization to another, and thus there can be an overlap of the objectives and methodologies of these activities depending on which definition is used.

countermeasures, and the level of security monitoring. Nor do they provide any insight into what an attacker could do if he managed to exploit them. Penetration testing generally involves attempts to exploit possible vulnerabilities. It is a more comprehensive attempt at finding all vulnerabilities in a system, usually performed using highly specialized tools and custom scripts developed specifically for the targeted system. It is generally focused on a specific application or service, rather than an entire CIS, and is typically done collaboratively just prior to operational deployment. Thus the service provided by the proposed CRT is complementary to traditional vulnerability assessment and penetration testing activities.

Within NATO, the assessments to be performed by the proposed CRT would complement those already identified in the NATO Security Policy and Supporting Directives, with the additional advantage that the CRT activities would not be limited to assessing only vulnerabilities, but also the mission impact that can be achieved through their exploitation.

2) Demonstration of the Mission-Level Impact of Cyber Attacks

The second objective, demonstrating the impact of cyber attacks, will always be aimed at military operations or business processes at the mission level. The demonstration objectives will be determined by the head of the client organization, and will aim at showing the potential impact of specific cyber attacks to the organization's mission given the functionality provided by the operational CIS in support of that mission. Demonstration to stakeholders and senior decision makers is specifically mentioned as an objective because it is a key aspect typically not well addressed by most current security assessment activities, which are mostly focused on the technical functioning of CIS components. For example, a conventional assessment could determine that "it is conceivable that an attacker could exploit a newly discovered vulnerability in a cross-domain guard and gain access to an operational chat room and influence the command of military operations, but we think that we will detect that". Such a finding will never have as much value as "the CRT was able to force an infantry company to move from location A to location B during a training exercise by exploiting a vulnerability in a cross-domain guard, and did so without being detected". The fact that the activity is intended to remove uncertainty through actual demonstration of the possible impact allows senior decision makers to more objectively discharge their responsibility to balance security measures against competing CIS requirements such as ease of use, functionality, and the amount of investment and implementation time necessary for these security measures.

The only limitations on which effects can be demonstrated by the CRT are those brought by the necessity of maintaining control on these effects as well as on any second-degree effects resulting either directly from the CRT activities or from the reactions of staff not aware of such activities. Clearly, any improper manipulation of an operational military CIS can have serious consequences. While risks exist, they can be managed and maintained at an acceptable level at all times. This is the purpose of most of the controls described in Section IV.

3) Improving the Ability of Cyber Security Staff and Users in the Emerging Cyber Threat Environment

Proper functioning of most security measures depends to a large extent on their proper use by security staff and users. Users are given training on how to perform procedures that pose a risk to the security of CIS, such as transferring files using removable devices. Security-awareness programs educate users as to telltale signs of cyber attacks and advise them on how to handle them. Security staff are trained to detect and handle cyber attacks by operating specialized tools and following a number of processes that ensure detected attacks are correctly interpreted, stopped, and reported, and that necessary recovery actions are undertaken. Some of this training is given through dedicated courses, while some of it is achieved through cyber defence exercises. Courses are generally used to train security staff in the use of specialized tools, while exercises are generally used to train them in the execution of processes.

Although these training courses, awareness programmes and exercises are in place and definitely contribute to the overall security of NATO's CIS, they generally do not take place on the operational CIS, and they are not optimized for the day-to-day working environment of security staff. Finally, certain assumptions are often made regarding the outcome of business processes and/or whether security tools would have functioned properly, simply for efficient conduct of the training or exercise.

The controlled execution of cyber attacks against operational CIS will provide a clear opportunity for users and security staff to hone their skills with the tools they will use to handle real cyber attacks. Specific objectives can be defined to fill identified training gaps and to make sure that all staff are able to execute incident-handling processes correctly for the situations of concern. This is a key benefit provided by the CRT, since the quality of training obtained from courses and traditional exercises is very much limited by the level of reality of the training or exercise.

B. Cyber Red Team Tasks

The proposed CRT will fulfil its mission by undertaking each assignment within the context of a "task". A distinct task is created for each request for the CRT's services by a client organisation. The concept provides a logical framework that addresses key requirements for command and control, for defining the legal basis, and for information management. It also allows for the concurrent execution of multiple assignments by the CRT. To be effective, a CRT task needs to be executed over a period of between six and fifteen months. This is to ensure that the CRT has the opportunity to make a comprehensive assessment without substantial prior knowledge of the organization's CIS and internal processes and to properly demonstrate the impact of advanced, persistent threats.

1) Simulated Threats

For each task, the client will define in very general terms the threats the CRT must simulate. These can include a foreign intelligence service, a criminal organization,

an ideologically motivated hacker group, a malicious insider, and military forces with a computer network attack capability. Of course the reality of the simulated threats will be limited by the capabilities of the CRT, and the objective is simply to generally define the modus operandi of the CRT during the execution of the task and the types of activities it will perform.

2) Typical Activities

Each task will have a specific list of authorized activities, which could include:

- Gathering and taking advantage of public information from open sources
- Scanning and probing networks (wired and wireless) and telephone systems
- Performing social engineering
- Monitoring facilities, including "dumpster diving"
- Exploiting vulnerabilities and compromising client systems
- Exfiltrating information
- Conducting denial-of-service attacks against specific services or networks
- Modifying operational data
- Attempting physical access to facilities to gain access to CIS.

Clearly the above activities must be legally authorized, and they must be performed with sufficient controls to ensure that they will not cause unintended consequences.

III. GOVERNANCE, COMMAND AND CONTROL

Management of the capability has been divided into three levels: strategic, operational and tactical. The main reason for differentiating between the strategic and the operational levels is to create a clear delineation of responsibilities and thus contain liability in case an error or fault is committed by members of the CRT. The main reason for differentiating between the operational and the tactical levels is efficiency, as explained in Section III.D.

At the strategic level, a "Steering Committee" will direct the proposed CRT. The use of a Steering Committee addresses the requirement for having representation from both Strategic Commands and the civilian structure in order to support the CRT's NATO-wide remit and to ensure the CRT is independent of the CIS providers and their security staff. This is a key aspect of the capability, as a proper assessment cannot be provided by those responsible for the operation of a CIS or those responsible for the operation of its security measures.

At the operational level, control will be provided by a Task Control Team (TCT), defined specifically for each task. Since the CRT can execute multiple concurrent tasks, there can be several different TCT in existence at the same time. Finally, at the tactical level, "Attack Team Leaders" within the CRT will oversee actions taken by CRT staff members. An exact placement of the proposed CRT within the

overall NATO organizational structure has not yet been suggested. This is a secondary consideration given that regardless of its organizational location, it will report to a Steering Committee specifically established to support it.

A. Legal Framework

A full legal analysis of the implications of establishing and operating the proposed CRT is required, but is beyond the scope of this preliminary proposal. The two main issues identified at this point are the need to legitimize the CRT activities that could otherwise be construed as malicious or unauthorized use of computer systems, and the potential for invasion of privacy resulting from CRT activities. Since some NATO Nations are already performing red team activities in a similar manner as proposed herein, it is reasonable to expect that a suitable legal framework can be established.

B. Strategic Direction and Guidance

At the strategic level, a Steering Committee will be established to direct the CRT and guide its continuous evolution. It will have at least the following responsibilities:

- Maintaining mission and vision statements, defining key values and ethical behaviour for the CRT staff, setting the high-level objectives, priorities and milestones for the evolution of the capability over time
- Ensuring that a generic legal framework for the different types of activities to be performed by the CRT is established and maintained and that the CRT has the required set of processes and procedures in place for achieving its objectives without undue risk or liability
- Overseeing staffing of the CRT and ensuring it is properly resourced
- Securing continued funding for the capability
- Securing support required from external parties (facilities management, common services, etc.)
- Identifying possible clients and tasks, and promoting the capability in various forums
- Prioritizing, scheduling and authorizing tasks
- Defining the elements to be audited and the manner in which audits will be performed, and setting the performance standards against which the CRT will be assessed (see Section IV.E)
- Accepting the findings of audits performed on the CRT, and ensuring identified issues, if any, are resolved in a timely fashion.

C. *Operational Control*

Operational control of the proposed CRT will consist of authorizing and directing all activities performed on operational CIS during the execution of the CRT's mission. It is at this level that the responsibility for any mishap or unintended consequence lies. Operational control of the CRT will be performed by the TCTs. At minimum, a TCT will consist of the Head of the CRT and a representative from the client organization who has been delegated the required authority. Both of these individuals will have veto power on all decisions made by the TCT, and thus the CRT staff members will be able to perform only the activities that have been authorized by both.

Within the TCT, the key responsibility of the client representative will be to accept the risk posed by proposed CRT activities to the operational CIS on behalf of the head of the client organization. The key responsibility of the Head of the CRT will be to ensure that the CRT is capable of successfully executing the proposed activity, satisfying himself that the staff members are sufficiently trained, that the exploit tools have been properly tested, and that possible secondary effects have been properly identified to the client representative so that he has the appropriate information regarding the risk posed by the activity. If an unforeseen consequence occurs despite the CRT having full and accurate information from the client organization, it will be the responsibility of the Head of the CRT. If a consequence that was foreseen actually occurs and is not well received within the client organization, it will be the responsibility of the client representative.

D. *Tactical Control*

The activities authorized by the TCTs will be defined in a certain amount of detail. For example, "scan a range of IP addresses for services", "deploy to a site and identify wireless access points", "attempt compromise of the server at IP address A.B.C.D", or "perform a denial-of-service attack against IPs in the range A.B.x.y". The amount of detail provided will be at the discretion of the TCTs. In most cases however, there will remain latitude in the specific execution of the activity, if only because a TCT simply will not be able to oversee every detail of a task. This "tactical control" will be the responsibility of the Attack Team Leader (see Section V.A). The Attack Team Leader will control and oversee the staff within his team and ensure that activities are executed in accordance with the direction provided and all applicable procedures. He will also take part in most activities, and will be responsible for constant oversight of the operational activities. Finally, he will also be responsible for ensuring the targeted CIS can be restored to its original state at the end of the task.

IV. MANAGING THE OVERALL RISK

The activities to be performed by the proposed CRT pose certain risks, including:

- Actions on a target system could cause unintended effects, such as rebooting it, affecting the functioning of services, or causing the loss of data

- Actions on a target network could cause unforeseen, collateral consequences, such as affecting dependent systems that were not to be targeted, consuming a substantial amount of bandwidth, destroying data, or triggering alerts
- Staff from the client organization could detect the red team activities and react to them in a problematic manner
- A red team staff member could act maliciously during a task.

To properly address these significant risks, specific controls have been built into the proposed CRT. The following sections provide insight into the most important of these controls.

A. *Trusted Agents*

In order to ensure staff members within the client organization do not react in a problematic fashion to detected CRT activities, and to ensure that unforeseen consequences are detected in a timely fashion, it will be necessary to place "trusted agents" at key positions within the client organization. Trusted agents will be identified when a task is initiated and will be given 24/7 contact information for various members of the CRT. They will be provided with sufficient information to allow them to immediately identify activities that could potentially originate from the CRT. When such activities come to their attention, they will contact the CRT who will in turn advise them of how to properly handle the situation.

Trusted agents will be selected from key positions within the client organization along the incident-handling process from sensor to decision maker to operator. A sufficient number of agents will be required to ensure that the CRT will have enough "eyes and ears" at the client organization to detect in a timely fashion any potential problem that may result from its activities.

In some cases, the CRT may choose to inform trusted agents of a specific action in advance in order to adequately control the risk it poses. For example, if the CRT is tasked to modify information in an operational command and control application to verify whether its users or security staff would detect attacks against the integrity of the information, a sufficient number of trusted agents in the immediate vicinity of the targeted users would be kept in direct and constant contact during the activity to ensure none of the users reacts to the modified information in a problematic fashion.

B. *Authorized Activities*

The CRT will be able to perform only those activities that have been specifically authorized prior to execution. There are two levels of prior authorization. The first will occur in the development of the task plan, in which the types of activities to be performed are identified in general terms, reviewed by legal counsel and authorized by the head of the client organization. These become "sanctioned" activities.

The second level will occur in the actual execution of the task, when the TCT authorizes that one of the sanctioned activities be performed in a specific way. The TCT may or may not make use of all sanctioned activities, but under no circumstance will it be able to authorize an activity that has not been sanctioned in the task plan. This second level of authorization will ensure that the TCT agrees that the specific activities are aligned with the objectives of the task and do not pose an unacceptable risk.

These authorizations would be of no use if they were not backed up by a code of conduct that each team member must agree to follow in order to join the team, the means to detect attempts by a team member to perform unauthorized actions, and administrative regulations that would enable NATO to take the required actions against such an individual. These are also addressed within the proposed CRT.

C. *Sanctioned Targets List*

Another key control mechanism is the Sanctioned Targets List (STL). The STL is a controlled document, signed by the head of the client organization, that will identify the systems that can be targeted by the CRT during a task. The STL can also specifically list the types of activities that can be performed against each target, thus further limiting the scope of authorized activities. It will be the responsibility of the client organization to ensure that it has authority over all of the systems listed in the STL.

D. *Two-Person Rule*

To address the risk that a CRT staff member could act maliciously and abuse the access to systems and information achieved by the team during a task, a two-person rule will be put in place. The two-person rule requires that all actions taken on an operational CIS be performed by two staff members working together. The proposed CRT will make use of a dedicated facility for the conduct of operations specifically to accommodate this rule (see Section V.B). Any team member observing another member working alone in the dedicated facility will have the obligation to challenge that person and report any suspicious activity to the TCT. The two-person rule implies that at least two staff members would need to collude to perform malicious activities, thus significantly reducing this risk.

E. *Comprehensive Auditing*

Another mechanism to address the risk that a CRT staff member could act maliciously is the comprehensive use of automated auditing and a comprehensive review of all aspects of the CRT's activities by a Task Audit Team (TAT) appointed by the Steering Committee and the head of the client organization. All activities performed on operational CIS will be audited in a number of ways:

- All authentications to sensitive information stores and systems will be logged

- All custom-developed systems to support CRT operations will have significant auditing in place that monitors the access of CRT staff to sensitive information
- Keystroke loggers will be installed on key systems
- Full packet capture systems will record all traffic in and out of the CRT
- All input and output on shells on key workstations will be copied to log files
- Screenshots of key workstations will be taken at random intervals and recorded
- All logs will be centralized and available for the TAT's review.

Clearly, with this amount of comprehensive audit logging, there is a strong probability that malicious activity, if suspected, will be detected by reviewing the log material. While the depth of the review of the logged material will be left to the discretion of the TAT, the mere fact that so many of the staff members' activities will be logged will act as a significant deterrent to malicious activity.

F. Test Procedures

The CRT will be obliged to test all exploit tools and software it will use against or on the client's CIS. The testing must provide reasonable assurance that the software will not cause unintended consequences. It will be the responsibility of the Head of the CRT to ensure that minimum testing standards are clearly defined, and it will be the responsibility of the Attack Team Leader to ensure that all software used during a task has been properly tested according to these standards.

G. Management of Client Information

During the execution of a task, the CRT will obtain and generate a large amount of information about the client organization, some of it potentially highly sensitive. The CRT will ensure that this information is properly secured according to the applicable NATO and national policies. In addition, the CRT will limit the information it retains after a task to a "task record" used for the purposes of programme management, and general findings that can be re-used for cyber awareness programs within NATO, as specifically authorized by the client organization. All other information will be destroyed at the end of a task, and the destruction will be audited. Finally, in addition to keeping as little information as possible, the CRT will follow specific procedures to ensure that proper care is taken when handling personal information in order to protect the privacy of individuals.

V. ORGANIZATIONAL STRUCTURE AND SUPPORTING FACILITIES

A. Organizational Structure

Figure 1 shows the organizational structure of a red team suitable for the proposed mission. The two main components of such a team are the Attack Group and the Support Group, which are further described below.

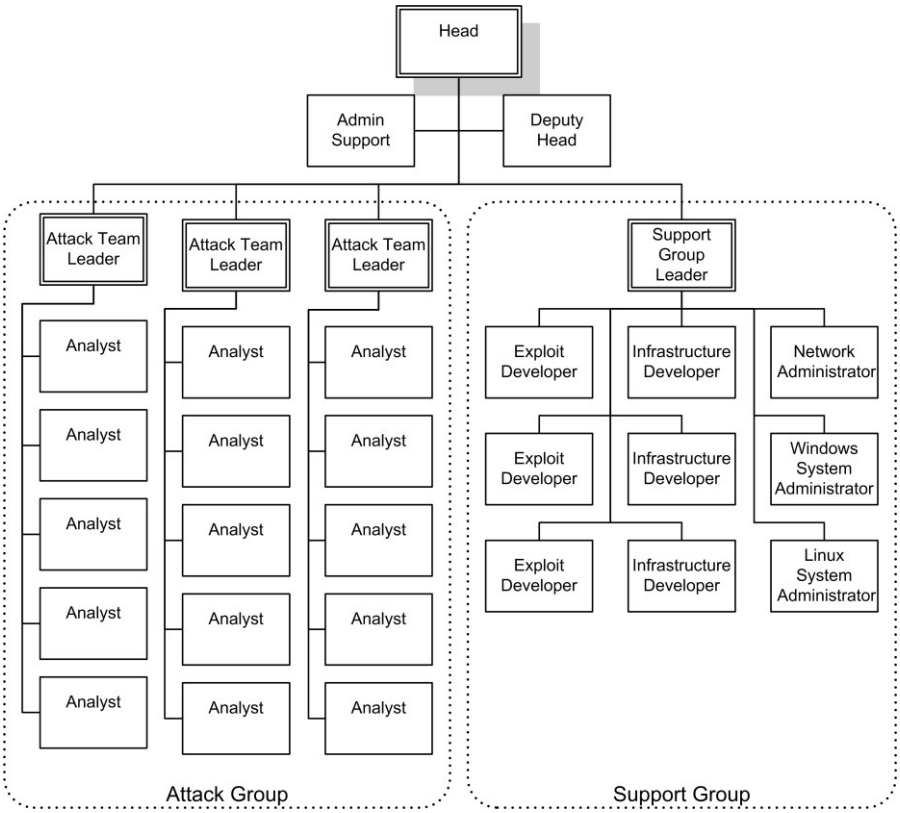

Figure 1. Organizational structure of a red team

The optimal size of a red team depends on a number of factors, such as:

- The size and complexity of the various CIS to be assessed
- The scope and depth of the assessment, the impacts to be demonstrated and staff improvement to be provided
- The frequency of the assessments
- The threat to be simulated and the level of desired reality.

While the size can vary according to these factors, the structure should remain the same as it is built around the different types of work and the skills and knowledge required in each area, as detailed below. There is however a bare minimum size below which it will not be possible to have the breadth and depth of knowledge required to provide realistic assessments, demonstrations and improvement. This bare minimum is 12 full-time members for the type of red team described herein. Even at 12 members, there remains a risk of mission failure, particularly if the staff selection process does not deliver the highest-calibre cyber security experts. It is important to note that mission failure in this case implies that the CRT would inaccurately assess the effectiveness of the security measures of an operational CIS, eventually leading senior decision makers and stakeholders to falsely believe that these measures are adequate.

The team size presented in Figure 1 represents the ideal size for the proposed CRT. The size of the team is based on the requirement to have a representative from each NATO Nation in addition to the three NATO civilians holding the positions of Head, Deputy Head and Admin Support. It is proposed that the national representative positions within the CRT be staffed through Voluntary National Contributions so that each Nation retains an agreed level of control and insight into the team's activities through a national chain of command.

1) Attack Group

The Attack Group is composed of three Attack Teams each consisting of an Attack Team Leader and five analysts. They are responsible for performing the required attacks against the targeted CIS and seeking ways of achieving the objectives of the task while staying within the defined boundaries. Analysts require a mixture of skills and experience:

- Expert knowledge of cyber security
- Strong knowledge of system and network management
- Strong experience in the Unix and Windows environments
- Strong knowledge of common Internet protocols
- Strong knowledge of wireless networks
- Military experience or at least a strong understanding of how military forces employ their CIS
- Ability to think "outside the box" and persevere.

2) Support Group

The Support Group is responsible for the development of the various tools needed by the Attack Group and the maintenance of the CRT systems. In addition to system and network administrators, the Support Group has two types of developers: Exploit and Infrastructure. Exploit Developers require:

- Expert knowledge of cyber security

- Software-development experience and reverse-engineering experience for both Windows and Unix systems
- Ability to search for vulnerabilities in software
- Ability to exploit buffer overflow and heap vulnerabilities
- Ability to code in assembly for different architectures.

Searching for vulnerability and developing exploit code is perhaps the most difficult work in cyber security. It requires a special "mindset" and extraordinary concentration, and these positions will likely be the most difficult to staff.
Given the requirement for custom software to provide a suitable exploitation infrastructure (e.g. "backdoors" and "covert channels"), efficient information management tools, and the required automated auditing and control mechanisms, the CRT requires an internal team of Infrastructure Developers who possess:

- Expert knowledge of cyber security
- Software-development experience for both Windows and Unix systems in several languages
- Experience in advanced version control and release management
- Experience in systems and network programming
- Experience in database development
- Experience in web development.

B. Physical Facilities

The conduct of red team tasks must be seen by all team members as a special activity. In addition to specialized systems, it requires concentration, focus and oversight. The proposed CRT would therefore perform its task from a purpose-built "Operations Room". This Operations Room would be designed specifically to address the human factors associated with the controlled execution of cyber attacks on operational CIS, accommodate the size of the team, and allow for proper demonstrations to senior-level decision makers.

C. Personnel Selection

A cyber red team is an elite team. To be successful, its members need to possess knowledge in a large number of highly technical areas. In addition, they need perseverance and an ability to think "outside the box". While all of these are the typical traits of a "hacker", the stereotypical hacker will also have the undesirable traits of disrespect for rules and desire for fame. Disrespect for rules and desire for fame are the most critical threats to the success of a professional red team. The leader of the CRT will play a critical role in establishing and maintaining the correct "mindset" among the staff, founded on meticulousness, rigour and discipline, in order to deliver a highly professional military capability. The CRT

also requires a strong team spirit, as it must achieve effects beyond those within the reach of individuals.

While common recruiting tools and methods can be used to screen applicants in terms of their education, experience and knowledge in technical areas, it is very difficult to evaluate whether candidates also possess the right attitude and "mindset". To create the best possible team, the following recommendations are made:

- The team's leader should have a few years' experience in managing a red team.
- The team should be built progressively so that the leader can instil the right values, attitude and team spirit in the members without being overwhelmed with new recruits.
- The selection process should allow for a multi-day competitive evaluation of a handful of potential candidates previously screened for their suitability in terms of education, experience and knowledge. The evaluation should be performed through a realistic simulation of a red team task and assess the candidates' abilities while under pressure for extended periods of time.

VI. CONCLUSION

The proposed cyber red team would provide a significant contribution to the improvement of NATO's cyber defence capability by identifying potential gaps and shortfalls in both technical solutions and incident-handling processes, demonstrating the mission-level impact of cyber attacks, and improving to the highest degree possible the skills and ability of security staff. Its implementation represents a significant, dedicated effort by NATO to perform an unbiased, highly realistic self-assessment of the effectiveness of security measures in providing mission assurance, and helps identify the most cost-effective way of improving NATO's cyber defence. Finally, it would also provide NATO Nations with insight into how cyber attacks can be successfully executed, and the mission-level impact these attacks can have against modern CIS.

REFERENCES

[1] G. Stoneburner, A. Goguen and A. Feringa, *Risk Management Guide for Information Technology Systems*, Special Publication SP 800-30, National Institute of Standards and Technology, 2002.

[2] "Allied Command Transformation NATO Network Enabled Capability Information Portal on TRANSNET", Internet: transnet.act.nato.int/WISE/Informatio, May 18, 2010 [Mar. 17, 2011].

[3] "The War Logs. An archive of classified military documents offers views of the wars in Iraq and Afghanistan", Internet: www.nytimes.com/interactive/world/war-logs.html [Mar. 17, 2011].

[4] Nick Davies and David Leigh, "Afghanistan war logs: Massive leak of secret files exposes truth of occupation", Internet: www.guardian.co.uk/world/2010/jul/25/ afghanistan-war-logs-military-leaks, Jul. 25, 2010 [Mar. 17, 2011].